SAND98-1557
Unlimited Release
Printed July 1998

High Consequence Operations Safety Symposium II

July 29–31, 1997

Sandia National Laboratories
Albuquerque, New Mexico

Daryl Isbell, Editor
High Consequence Surety Engineering Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0490

Abstract

From July 29 to 31, 1997, the Surety Assessment Center at Sandia National Laboratories hosted the second international symposium on High Consequence Operations Safety, HCOSSII. The two and one-half day symposium allowed participants to share strategies, methodologies, and experiences in high consequence engineering and system design. The symposium addressed organizational influences on high consequence safety, assessment and analysis processes, lessons-learned from high consequence events, human factors in safety, and software safety. A special session at the end of the symposium featured a presentation by Federal Nuclear Center—All Russian Research Institute of Experimental Physics and Sandia National Laboratories personnel on their joint efforts to establish the International Surety Center for Energy Intensive and High Consequence Systems and Infrastructures.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401, FTS 626-8401

Available to the public from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161

NTIS price codes
Printed copy: A20
Microfiche copy: A01

SAND98-1557
Unlimited Release
Printed July 1998

High Consequence Operations Safety Symposium II

July 29–31, 1997

Sandia National Laboratories
Albuquerque, New Mexico

Daryl Isbell, Editor
High Consequence Surety Engineering Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0490

Abstract

From July 29 to 31, 1997, the Surety Assessment Center at Sandia National Laboratories hosted the second international symposium on High Consequence Operations Safety, HCOSSII. The two and one-half day symposium allowed participants to share strategies, methodologies, and experiences in high consequence engineering and system design. The symposium addressed organizational influences on high consequence safety, assessment and analysis processes, lessons-learned from high consequence events, human factors in safety, and software safety. A special session at the end of the symposium featured a presentation by Federal Nuclear Center—All Russian Research Institute of Experimental Physics and Sandia National Laboratories personnel on their joint efforts to establish the International Surety Center for Energy Intensive and High Consequence Systems and Infrastructures.

Intentionally left blank

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Table of Contents

Software Safety **357**

International Surety Center... **437**

Intentionally left blank

OPENING SESSION

Intentionally left blank

A Safety Culture: The Welcoming Address to the Second High Consequence Operations Safety Symposium

W. C. Nickell
Director, Surety Assessment Center, 12300
Sandia National Laboratories*
Albuquerque, New Mexico

Welcome

On behalf of Sandia National Laboratories and the Surety Assessment Center, welcome to the Second High Consequence Operations Safety Symposium.

I will attempt to provide some context for this symposium by addressing the subject of safety culture.

A Summary of Nuclear Weapon Safety History

Nuclear weapon safety has progressed through three stages. The first stage related to early weapons where safety was assured by physically separating the nuclear material from the explosive. This provided a first principle assurance that nuclear yield was impossible in an accident. Additionally, it provided assurance that an accidental detonation would not scatter nuclear material if the explosive and the nuclear material were sufficiently separated.

This safety theme served us well. Of the 32 nuclear weapon accidents, about half involved this separable design and none resulted in accidental nuclear detonation.

The second stage of nuclear weapon safety was characterized by the so-called 'wooden bomb'– a weapon that did not have to be assembled, tested, or exercised prior to its use. It was ever ready for employment. The advantage of this concept was significant to operational flexibility and use. But we lost the safety inherent in the separable design.

The safety theme of these weapons was based on meticulous design, careful analysis, thorough testing, and reliable components – similar to the safety theme used by much of the industry even today. Of the 32 nuclear weapon accidents, about half were of this safety theme and none resulted in nuclear detonation. Altogether, nine of the accidents

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

resulted in the high explosive burning, 11 resulted in detonation of the high explosive, and 10 resulted in nuclear contamination. Five of the accidents resulted in both an explosion and contamination.

The third and current stage of nuclear weapon safety resulted from concerted attempts to improve safety and was motivated by the accident history. Added safety emphasis was precipitated by the Palomares accident in January of 1966, that, while it did not result in nuclear detonation, did result in a massive plutonium clean-up operation. This accident, together with the Thule, Greenland accident, caused the termination of flying weapons on alert. Ground alert was substituted.

Tests and analyses to determine or demonstrate the degree of weapons invulnerability to accidents were unsatisfying and difficult to quantify and finally resulted in an entirely new approach. The major problem was how to design a fail-safe system, based on fundamental principles, that would not need to be justified on the basis of analysis, or the probability of the accident.

The new design was simple in concept, but difficult in implementation. First, reduce the number of safety critical components to the minimum set, then enclose those components in an exclusion region to isolate and protect them from the critical aspects of the accident environment. Second, protect all input signals such that only those that are known to be intended by *humans* could be used to arm the system by using a code that Mother Nature does not know. Finally, design the safety critical components such that the accident environment would irreversibly destroy them, but at lower levels, and earlier times than those at which the protective components were destroyed.

This development has been underwritten by a safety culture that I will say more about later.

Our Mission

Our principal mission has been to provide the nation with 'a safe deterrent' not just nuclear weapons.

Our principal customer is the public.

The military is the custodian of the product.

The military is well represented – they provide the requirements and we work with them continuously.

But, the public is not well represented. Thus we need to be the stewards of the public trust as well as funds. This is a fundamental concept.

Why Am I Talking About Nuclear Weapons?

Because there are some strong commonalties among us.

Our mission – the 'safe' part – is similar to yours, whether your business is transportation, production and distribution of electric power, food, water, medical products, chemicals, or other important industries. For these the public is the ultimate customer although there are many intermediaries, custodians, sponsors, brokers, regulators, investors, intervenors, and so forth. Sometimes the ultimate customer, the public, is represented well and at other times they are not.

Responsibility

We all have an awesome and daunting responsibility to the ultimate customer – the public.

- 'We,' the technical community that develops and manufactures products.
- 'We,' the operators that use our products to produce goods.

We have a difficult task because the focus is usually on other aspects of the product (*e.g.* effective deterrence, affordable power, fast or inexpensive transportation, *etc*) and not on the adjective – "safe."

We are producers and stewards at the same time – but we must be stewards first and producers second.

We should think of *safe* nuclear power, of *safe* air transportation, *safe* nuclear weapons, *etc.* The adjective "safe" should be inseparable from the product or service.

We – all of us in the high consequence engineering business – are partners in stewardship of the public trust.

It is not our job to play God by judging the acceptability of risk.

It is not our job to merely do what we are told – just meeting requirements and designing to specific limits – and taking umbrage by accepting our sponsor's definition of acceptable risk.

So Why We Are Here This Week?

We are here to broaden our collaborative view of our awesome and daunting responsibilities and to share our experience with each other – whether our products are deterrence, electric power, medical equipment, food, chemicals, transportation, or any others that contain the element of high consequences. Some of us are teachers, writers, representers of the public, but all of us have the same general interest.

We are here to learn what works well and what doesn't and perhaps more importantly, why.

We are here to share technology and information and learn from one another.

We are here to develop a coalition for future mutual information dissemination.

We are here to participate in a spirit of collaboration, bound by the mutual stewardship of making this world a better and safer world to live in while providing our customers with the products they need.

A Safety Culture

I said I was going to say more about safety culture.

A common thread in successful high consequence engineering is an enduring and pervasive safety culture.

Culture is necessary for endurance.

Culture – Webster's View

"The total pattern of human behavior and its products embodied in thought, speech, action, and artifacts and dependent upon man's capacity for learning and transmitting knowledge to succeeding generations through the use of tools, language, and systems of abstract thought.

"The body of customary beliefs, social forms, and material traits, constituting a distinct complex of tradition of racial, religious, or social group.

"A complex of typical behavior or standardized social characteristics peculiar to a specific group, occupation or profession, sex, age, grade or social class."

What is a Safety Culture?

It is behavior in ways where safety is held premium in its products embodied in thought, speech, action, and artifacts.

There are some fundamentals:

- There must be a complete and pervasive intolerance to compromising safety principles.
- The burden must always be to prove it safe – not to prove it unsafe.

- There must be a willingness to make unpopular decisions when necessary – and take the heat for them.
- There must be an attitude of pursuing the resolution of safety issues with vigor and determination, preferably founded on technical facts rather than opinion.
- There must be pride of work, yet with the maturity to seek and respect independent assessment.
- Those responsible for product must also be responsible for product safety. The role of independent assessment is necessary to support this concept. But independent assessment organizations should not be responsible for the product, lest they lose their independence.

Why is a Safety Culture Necessary?

- Products are flawed (hardware breaks and software has bugs).
- People make mistakes.
- Environments resulting from an accident are beyond those expected or specified.
- Sequences get out of whack.
- Faults propagate unintentionally and unpredictably.
- Products fail because of unknown or unexpected common mode failures.
- Products are used for times exceeding the design lifetimes

These factors cannot be adequately described in requirements or specifications.

How Do You Recognize a Safety Culture When You See One?

You wake up in the middle of the night wondering if you did everything you could and did it right. But you find that you are not alone – others wake up also. This is known as designer's paranoia. The concern for safety is pervasive and fractal.

There is a spirit of openness and communication in all directions.

There is a productive and professional tension.

There is a respect for others' opinion – everyone has the right to understand, explore, debate, and disagree.

There is no reliance on the fact that "nothing bad has happened yet."

There is a willingness to learn from the past or from the errors of others.

There is truth and reality above all.

The standard for judgment is the positive measures employed to ensure safety, as opposed to probabilistic estimates of risk or failure.

There is no reliance on the specific definition of accident environments but rather reliance on the thorough understanding of what really could happen. Use of the 'worst case accident' is to provide a baseline only and not for acceptance or completeness.

Probability-based models are regarded as excellent tools, but they are recognized as models and not necessarily reality.

How Do You Recognize the Absence of a Safety Culture?

In an ineffective safety culture there will be emotional rather than technical arguments. There are pontifications rather than technically based decisions.

There are arguments such as "prove that it is unsafe."

There is a willingness to make just a simple change without thorough revalidation.

There is reliance on probability assessments alone to prove acceptability. That is not to say that there is anything wrong with probability assessments, but rather they should be one of the tools to provide understanding and insight, for it's profound knowledge of the high consequence *system* that we seek.

There is an inconsistent value system – people are told that their responsibility includes safety, but they don't get paid if they shut down an operation.

There is a willingness to accept the argument that it's good enough or we don't have time to fix it. Or it met the requirements when we delivered it, so therefore its ok.

There is a willingness to believe numbers less than 10^{-6} or even 10^{-3} for single events.

Schedule and budget issues over-ride safety decisions.

Three Foundations for a Safety Culture

1. Accountability
   One of the foundations of a safety culture is that all must be accountable for their performance and the performance of their products – not just the management. Decisions should be made on the basis of what should be done with the long-term systems view in mind, not the short-term view.

2. Fractalism
   Fractalism means that everywhere you look you see the same patterns. Corporate management develops strategic directions with the concept of 'safe x' (where x is your product). If you zoom in to middle management you see them developing plans to carry out the strategic directions for 'safe x.' If you zoom in on the work being performed, you see the staff focused on 'safe x.' The parameters are different but the fractal nature is preserved at all levels, including suppliers.

3. Awareness
   Awareness is key to all activities. Self-assessment and independent assessment provide awareness. Education and training provide awareness. Symposia like this one provide awareness. Communications – free and open – laterally, vertically, and diagonally are essential. Awareness is the precursor to understanding.

Steps to Safety Design and Operation

1. Develop a profound knowledge and understanding of the functionality of the *system* under consideration and its failure modes – understand how things fail as well as how things work.

2. Develop a safety theme – an orienting principle that is dominant and effective in guiding action. For nuclear weapons, the safety theme has been to isolate the critical components from threatening environments for as long as they are operable.

3. Develop positive measures to prevent or mitigate undesired consequences *when* failures occur. Positive measures are a device, procedure or process with the primary purpose of preventing undesired consequences.

4. Establish configuration control of positive measures and critical features. Configuration control is to ensure that the positive measures and critical components or features are operative and do not get replaced or nullified without being subjected to the original engineering scrutiny in design and review, and that those critical features are proper and not defective or counterfeit.

5. Establish effective conduct of operations consistent with the design of the product, including inspection and surveillance.

Conclusion

Those of us working in high consequence engineering have a responsibility to our customers, but most of all we have a stewardship responsibility to the public.

To execute this responsibility we must go far beyond the concept of acceptable risk.

As engineers and scientists we must all apply our talents on behalf of the unrepresented customers – the public. We must be their technical representatives.

As the world increases in complexity this job becomes more difficult and more important as well. Our litigious propensities preclude honesty and integrity for fear of being challenged in the courts. Our angry subcultures provide additional threats with devastating results. Natural disasters will be with us forever, but the increasing complexity of our products may cause greater consequences.

We – all of us no matter what our role is – need to perpetrate a safety culture; a climate in which true improvements can be made, not because they are demanded or legislated, but because they are the right thing to do in executing our stewardship for the public.

It is in this spirit of collaborative synergy that I welcome you to this symposium.

Working Together Toward an Improved Safety Culture

Keynote Address

Robert T. Francis II
Vice-Chairman, National Transportation Safety Board
Washington, DC

Intentionally left blank

ORGANIZATIONAL INFLUENCES

Tuesday, July 29, 1997
10:30 a.m. – 12:00 p.m.

Intentionally left blank

Unreliable Organizations and Reliable Operations?

Scott D. Sagan
Stanford University
Stanford, California

Intentionally left blank

Independent Assessment and High Consequence Incidents

Orval E. Jones
Sandia National Laboratories, Retired
Albuquerque, New Mexico

Abstract

Independent surety assessment of high consequence operations and development activities, if truly independent and rigorously conducted, has the potential for identifying problems **before** a catastrophic failure occurs, rather than afterwards. It serves as a primary support function for executive management and the board of directors.

Introduction and Definitions

Speaking on the subject of "independent assessment and high consequence incidents" is much akin to a preacher delivering a sermon. Everything that he says is common sense and already known to all. The congregation listens politely to his admonitions to "do right," but usually forgets what it has heard as it exits the pews. And, of course, often the preacher himself may fall prey to the very transgressions against which he rails. Thus, I must be the first to admit to you that I have not always followed the advice that I will be giving.

What I will do is share with you some of my observations resulting from some twenty-five years of experience at Sandia National Laboratories, lastly as executive vice-president, in managing a variety of high consequence programs.

First, I need to define what the term "high-consequence incident" means to me. I will not try to be exhaustive. A high consequence incident is a catastrophic, high-visibility disaster that (1). might result in great injury to the population, such as the Chernobyl reactor accident and the Bhopal, India chemical plant release; (2) might inflict great harm on the environment, such as the Valdez oil spill; (3) might restrict national defense options, such as the Palomares and Thule accidents involving airborne nuclear bombs; (4) might cause the withering of a national industry or technology option, such as the Three-Mile Island reactor accident; (5) might severely damage national prestige, such as the Challenger space shuttle loss; (6) might impair public confidence in an institution, such as the Navy's Iowa gun turret explosion and the recent FBI forensic laboratory revelations; or, (7) might cause significant or irreparable damage to a major business, such as the ValuJet and TWA Flight 800 aircraft crashes. A high consequence incident may involve combinations of these. In addition, your own definition of a high consequence incident may well depend on the degree of your personal involvement.

A high-consequence incident might be initiated by a natural catastrophe, such as an earthquake, tornado, lightning, and so on. It might result from an external accident, such as an aircraft crash into an ongoing operation, or from an internal accident associated with the operation itself, beginning, perhaps, with a hardware, software or procedural failure, which then expands out-of-control. These are the types of initiating events that most commonly come to mind. However, high-consequence incidents might also be deliberately caused. In the case of an outside malefactor(s) the incident might range from a terrorist attack to sabotage. An inside malefactor(s) might overtly or covertly sabotage an operation.

Unfortunately, and often overlooked, several initiating events may occur simultaneously. Further compounding any initiating event(s) is the possibility of a "common-mode failure" in which supposedly independent backup safety and/or security protection systems fail together, thus allowing the initial failure to go on to a disastrous conclusion. In all these regards, for example, the financial industry could be as vulnerable as the nuclear power industry.

Focusing on an organization, the typical list of players concerned about and responsible for preventing high-consequence incidents are the (1) process operators and/or the design and development engineers; (2) surety, that is, safety and/or security, groups; (3) line management; (4) executive management; and (5) board of directors. The everyday responsibility for evaluating the risk associated with a high-consequence operation rests with the concerned line management and its staff, and with the surety groups.

To talk about independent assessment, I first must establish a context by discussing organizational surety dynamics and issues and then surety support for operations and/or development groups.

Organizational Surety Issues

An organization needs to periodically inventory and evaluate its operations to determine which, if any, are high consequence in nature and what those consequences might be. Then, estimates of the likelihood of occurrences of initiating events are required, followed by evaluations of the probability, given that the initiating events occur, that the protection systems fail to operate as designed. Risk, in simplistic terms, is the product of these three. A common and very serious difficulty is that while the risk of a high consequence incident may be deemed to be very low because of multiple protection systems, the possibility of a common-mode failure among those systems may not be recognized or understood. Edwin Zebroski[1], in analyzing several high consequence engineering failures of the 1980s, pointed out that those responsible in an organization for understanding and making such assessments may themselves suffer from a "common-mode failure of risk perception." Being a closed community they may develop a form of "tunnel-vision" that prevents them from recognizing and acknowledging actual and potential problems. From his analyses Zebroski[2] later declared that "*. . . major engineering catastrophes are rarely if ever accidental!*"

Hopefully, the safety or security group charged with reviewing the operation or the design and development will be sufficiently insightful and independent to flag any such problems. However, at their best, these oversight groups, working daily with the operators or designers, are naturally required to make certain accommodations and compromises if they are to continue to have full access to, and influence on, what is happening. This can lead to what Irving Janis[3] has called "groupthink," in which an insulated group of controlling individuals, often with common backgrounds, make flawed decisions due to arrogance, either intellectual or motivated by a "can-do" desire to succeed, and/or to stress resulting from budget pressures or external criticism.

Further, all parties generally desire, if possible, to resolve any problems in order not to draw the attention of executive management. Getting tangled-up with executive management is usually viewed as disadvantageous and an impediment to progress. For its part, executive management, including the board of directors, is usually only too delighted to hear that there are no problems, and normally is not inclined to inquire further.

I observed this process repeatedly in connection with the annual surety reports to the President of the United States on the status of nuclear weapons and operations. These reports, representing the joint views of the DoD and the DOE, involved substantial accommodations between the views of the two agencies in contentious areas. The result, I believe, was that the reports sometimes reflected a rosier state of affairs than I felt was justified at the time.

This is not to insinuate that these processes cannot work properly; indeed, with enlightened staff and management they can be fully effective. However, when a high-consequence incident occurs, any process failings are mercilessly exposed. It is then that executive management, be it of a company, institution, or a government, may be blind-sided and represented as irresponsible, negligent, stupid, equivocating—and in some cases the representation may be correct. Thus, executive management must actively work to be directly involved and to prevent organizational *arrogance* ("We're too smart to make a mistake."), *complacency* ("Everything's OK, don't worry."), *apathy* ("Who cares, it's not my concern."), and *ignorance* ("I didn't know anything about it."). Earlier[4], I noted that the quantity, quality, and integrity of interactions between managers and staff, at all levels, could be a powerful tool for countering these four apocalyptic horsemen of catastrophe. In addition, appropriate independent assessment of high consequence activities can be a powerful antidote to organizational tunnel vision.

I must admit that before 1986 I didn't give much thought to Sandia's processes, but simply assumed that they were effective because we had not been directly involved in any high-consequence incidents. But the catastrophic Space Shuttle Challenger accident on January 28, 1986, which resulted in an intensive investigation by the Rogers Presidential Commission, changed my outlook permanently.

As I read the Commission's report[5], especially the large blocks of verbatim testimony by both industry and government managers, I was forced to question whether I and other Sandia managers responsible for high consequence activities were sufficiently informed and involved in critical decisions. Subsequently, I prepared a summary of the report and gave it as a talk several dozen times throughout the DOE nuclear weapons complex. For those of you who are responsible for high consequence operations, I recommend emphatically that the Rogers Commission Report, or a similar report including actual testimony, should be required reading. I guarantee that it will at least raise your level of discomfort and, perhaps, even generate some fear. Fear can be a useful prod to action.

Surety Support: Organizational Outreach

It has been proven many times over, following catastrophic accidents, that the safety or security groups must report up a management chain different from that of the operations or development groups. In my view, they should report directly to the highest levels of executive management, as they do at Sandia. This signals to all the importance that executive management assigns to the function and provides an unimpeded channel for communication of issues and problems. There should be frequent, regularly scheduled meetings between the designated executive and the manager of the surety group, as well as whenever the manager desires. The executive must take responsibility for ensuring the adequacy of staffing and funding, even in times when resources are limited. This cannot be left to the management of operations and development groups; even with the best of intentions, they will gradually impoverish the surety function.

Also, I believe that there probably needs to be two parts to the surety activity. One part, the larger, works regularly and directly with operations or development groups, serving as a surety resource for special knowledge and insights provided by its safety and security specialists. Such an outreach relationship is extremely valuable. As noted earlier, when the groups are working well together, it is natural that accommodations and compromises will evolve in order to facilitate progress. Only the most hotly disputed issues are expected to surface formally; however, the surety manager should keep the designated executive apprised of anything noteworthy at their regular meetings.

The operations or development groups need to conduct themselves according to a written set of operations or engineering procedures. These procedures should be formal, rigorous and comprehensive. They should constitute a living document, being modified whenever required. They should be readily available throughout the organization, and the new intranets facilitate this. They should specify overall operation or design philosophy, prescribed practices, priorities, required operations or design reviews, and essential participants, required approvals, and so on. They should also specify the role of the surety group and its responsibilities. Collectively, these procedures provide the overall discipline that governs the operations or design groups, whether they are in the nature of engineering or conduct-of-operations guides.

For high-consequence activities there may be additional documents that guide the surety group. For example, at Sandia I implemented thorough specifications, among others, for the conduct of surety reviews, for required documentation, for identification of action items, and for procedures for ensuring the closure of action items.

Independent Assessment: Upward Oriented

In the foregoing context, we can now discuss independent assessment—the second part of the overall surety activity.

Independent assessment of high-consequence safety and security matters primarily supports the needs of executive management and the board of directors. It insures that high-consequence operations and development groups, while working with the surety support groups, have not developed tunnel vision so that they are unable to see problems. By independent assessment I mean that individuals who have no connection to the operators or developers make evaluations of the adequacy of high consequence surety measures. Their findings are reported to executive management. This, then, is clearly an executive staff function that reports through a management chain totally distinct from the operations or development groups. For day-to-day administrative purposes it may be situated in the larger surety support group, but it is independent and exists primarily to serve executive management. Further, it must be assigned bright, vigorous, and thoughtful staff and adequate resources.

The independent assessment group assists executive management in (1) identifying contentious potentially high-consequence surety issues that require executive review or intervention; (2) organizing and supporting *ad-hoc* assessment teams of internal or external experts; (3) ensuring that executive management actually discharges its responsibilities regarding high-consequence activities; (4) reporting on whether review functions are performed; (5) verifying that surety-related action items are properly documented and closed; and (6) preparing timely annual surety reports for internal and/or external distribution. At Sandia, the last of these items included an annual formal letter to DOE that put Sandia's assessment of nuclear weapons surety on record.

In my experience, I found that documentation of action items arising from design reviews was often lacking. Even more troubling, closure of action items was often neglected. It became the duty of executive management, assisted by the independent assessment group, to monitor and review these areas. For some system-level surety reviews it was also appropriate to involve executive management as either observer or participant.

The independent assessment group is almost guaranteed to become a source of resentment for operations or development groups. Typical objections are that it is staffed by zealots, enjoys too much access to, and creates problems with, executive management, etc. It is executive management's responsibility to manage this tension constructively and to protect and guide the independent assessment group. Executive management must take seriously the findings of its independent assessment group and choose appropriate responses, if any. If it does not, then the function will soon wither and become ineffectual.

Certain high-consequence activities may be of sufficient gravity that executive management may wish to appoint a select ad-hoc group, consisting of internal experts and/or outside consultants, to review a design or an operation. In some cases these teams may be referred to as "murder boards," "black-hatters," "adversary testers," and so on. Unfortunately, this is too often only done after an incident. For example, post hoc review teams assessed the Challenger accident (Rogers Commission), the Iowa explosion (Sandia), and the FBI forensic laboratory. In all of these cases, obvious problems were identified that had been overlooked or ignored by the respective operating groups. It is unfortunate that the problems, identified clearly through independent assessment, were not identified and remedied **before** failure, rather than afterwards.

Considering the variety of assessments and information that it receives during the year, executive management has a responsibility to inform its board of directors, or its governing body, about those high consequence activities that are on going in the organization or for which it is responsible. Unfortunately, executive management often has a tendency similar to that of the operators and developers. Namely, the less the board knows, the less it will interfere. This tendency must be resisted.

The board, in turn, must provide guidance on how, what and when it wishes to be informed. In fulfilling its stewardship obligations, the board may, in addition to its reviews, wish to examine each year those key documents that demonstrate to its satisfaction that executive management is properly fulfilling its responsibilities.

Finally, if the organization works for a sponsor, such as the government, then the board must be sure that the organization is measuring up to its responsibilities, rather than simply "saying what the sponsor wants to hear."

References

[1] E. L. Zebroski, "Common Risk-Management Attributes of Four Man-Made Catastrophes," unpublished manuscript, 1987.

[2] E. L. Zebroski, "Lessons Learned from Man-Made Catastrophes," Risk Management (Hemisphere Publishing Corporation, New York, 1991), pp. 51-65.

[3] See, for example, I. L. Janis and L. Mann, Decision Making (The Free Press, New York, 1977), pp. 129-133.

[4] O. E. Jones, "Managing Safety Through Interpersonal Interactions," Proceedings of the High Consequence Operations Safety Symposium, Sandia National Laboratories Report, SAND94-2364, 1994, pp. 29-33.

[5] W. P. Rogers, Report to the President By the Presidential Commission on the Space Shuttle Challenger Accident, Vol. I, June 6, 1986 (Superintendent of Documents, U.S. Government Printing Office, Washington, D.C., Stock no. 040-000-00496-3, 1986).

Biography

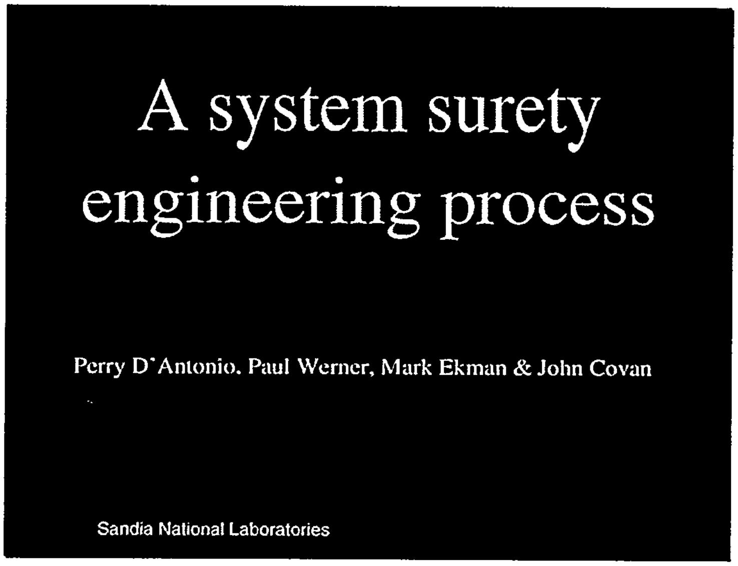
Dr. Orval Jones, now a consultant to Sandia National Laboratories, retired in 1993 from Sandia where he was the Executive Vice-President. Dr. Jones is a Fellow of the American Society of Mechanical Engineers and received the Department of Energy Distinguished Associate Award for his contributions to nuclear weapons safety and security.

Intentionally left blank

A System Surety Engineering Process

Perry D'Antonio
Paul Werner
Mark Ekman
John Covan
Sandia National Laboratories*
Albuquerque, New Mexico

Slide 1

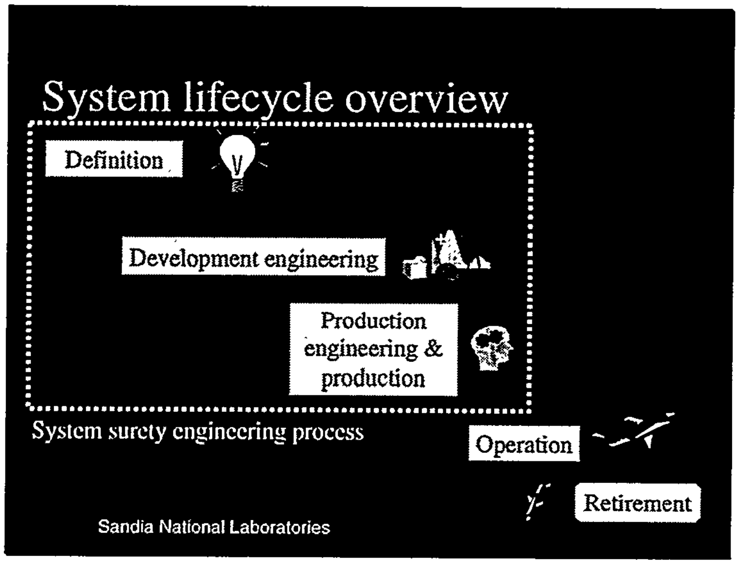


A system surety engineering process

Perry D'Antonio, Paul Werner, Mark Ekman & John Covan

Sandia National Laboratories

Slide 2



System lifecycle overview

Definition

Development engineering

Production engineering & production

System surety engineering process

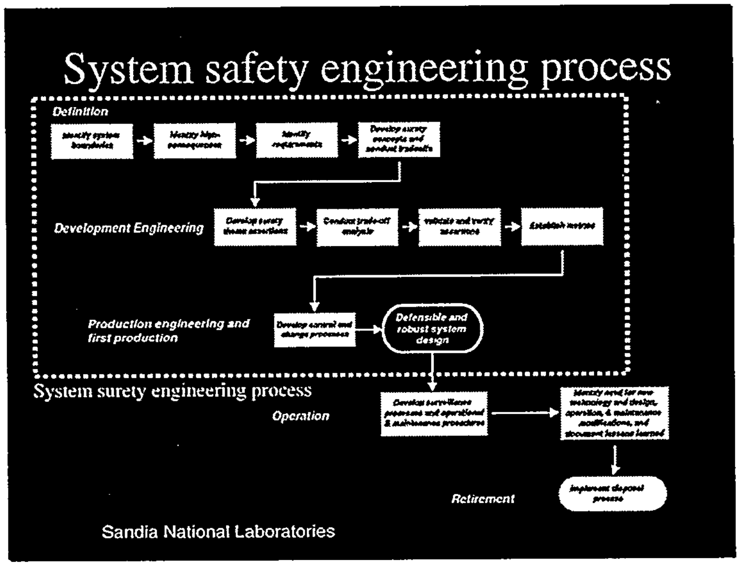
Operation

Retirement

Sandia National Laboratories

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

Slide 3



System safety engineering process

Definition

Identify system boundaries → Identify high-consequences → Identify requirements → Develop surety concepts and conduct tradeoffs

Development Engineering

Develop surety theme assertions → Conduct trade-off analysis → Validate and verify assurance → Establish metrics

Production engineering and first production

Develop control and change processes → Defensible and robust system design

System surety engineering process

Operation

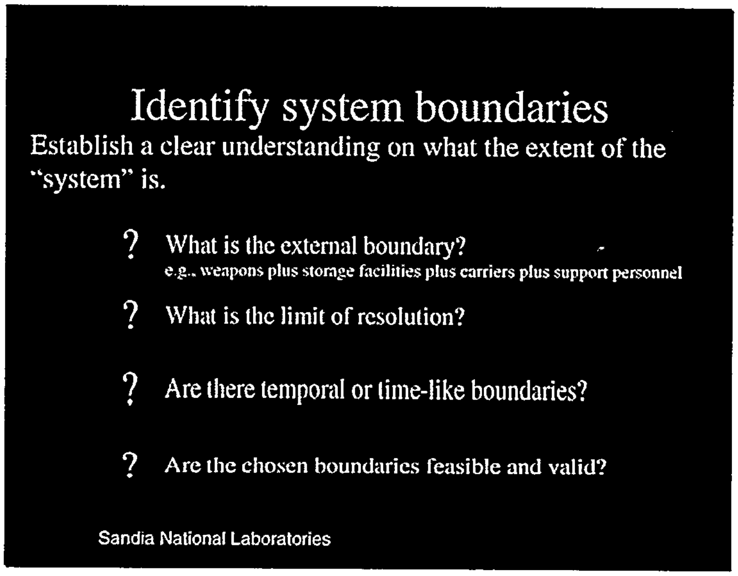
Develop surveillance programs and operational & maintenance procedures → Identify need for new technology and design, operation, & maintenance modifications, and document lessons learned

Retirement

Implement disposal process

Sandia National Laboratories

Slide 4



Identify system boundaries

Establish a clear understanding on what the extent of the "system" is.

? What is the external boundary?
e.g., weapons plus storage facilities plus carriers plus support personnel

? What is the limit of resolution?

? Are there temporal or time-like boundaries?

? Are the chosen boundaries feasible and valid?

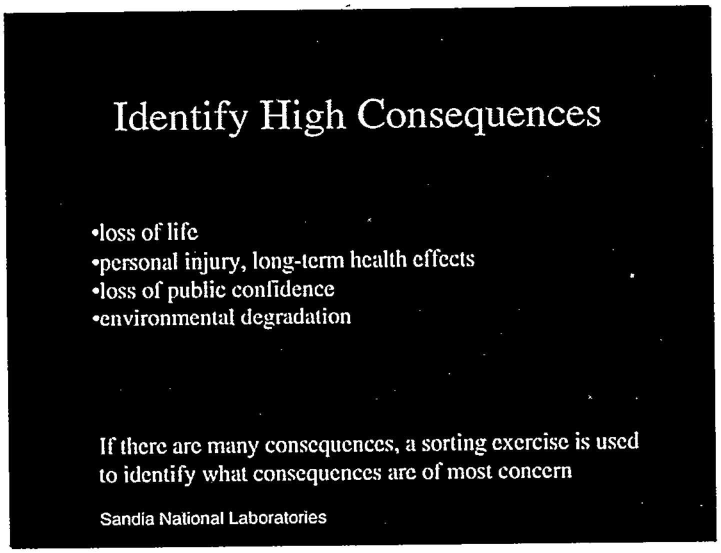
Sandia National Laboratories

Identify System Boundaries

A clear understanding on what the extent of the "system" is. A system is an identifiable entity comprised of discrete, interacting elements. It includes the integrated set of people, procedures, equipment, and facilities that perform a specific operational task within a specific environment. The system boundaries include the interaction of this set that may contribute to the formation of hazards during the life cycle of a system. System boundaries and interfaces will be specific to the individual system and its life cycle states. Of special importance are normal and off-normal flows of energy and information across boundaries.

This is analogous to similar processes in classical physics, such as thermodynamics. The establishment of appropriate boundaries is of utmost importance to the system surety engineering process.

Slide 5



Identify High Consequences

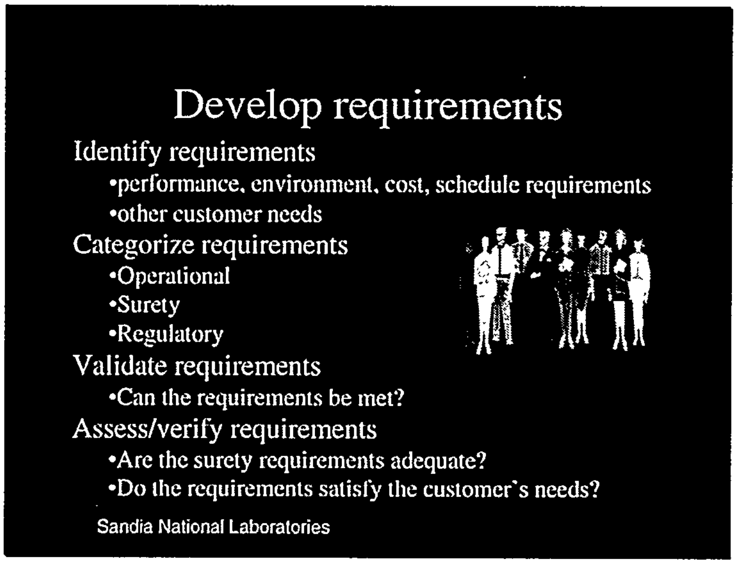
- loss of life
- personal injury, long-term health effects
- loss of public confidence
- environmental degradation

If there are many consequences, a sorting exercise is used to identify what consequences are of most concern

Sandia National Laboratories

Varies with the operation and the customer, but is judged to be severe, for example, resulting in significant loss of investment or loss of life. This is what the design must inherently avoid.

Slide 6



Develop requirements

Identify requirements
- performance, environment, cost, schedule requirements
- other customer needs

Categorize requirements
- Operational
- Surety
- Regulatory

Validate requirements
- Can the requirements be met?

Assess/verify requirements
- Are the surety requirements adequate?
- Do the requirements satisfy the customer's needs?

Sandia National Laboratories

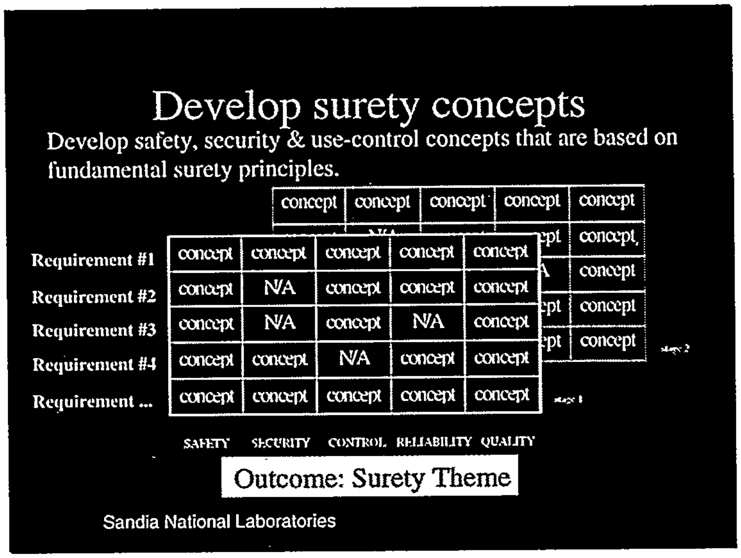
Using a team with design and surety expertise, identify, validate, and integrate traceable requirements of how the system is to perform with respect to its operation, surety elements, regulations and orders, and consequences. Major surety requirements include:

- safety
- security
- use control

System safety requirements are developed for both operating (normal) as well as accident (off-normal) environments. Requirements define hazards to be avoided, credible operating and accident environments, and span of operations covered. It may be necessary to revisit or redefine the system boundaries and high consequences.

Every requirement defined must be testable.

Slide 7



Develop surety concepts

Develop safety, security & use-control concepts that are based on fundamental surety principles.

	SAFETY	SECURITY	CONTROL	RELIABILITY	QUALITY
Requirement #1	concept	concept	concept	concept	concept
Requirement #2	concept	N/A	concept	concept	concept
Requirement #3	concept	N/A	concept	N/A	concept
Requirement #4	concept	concept	N/A	concept	concept
Requirement ...	concept	concept	concept	concept	concept

Outcome: Surety Theme

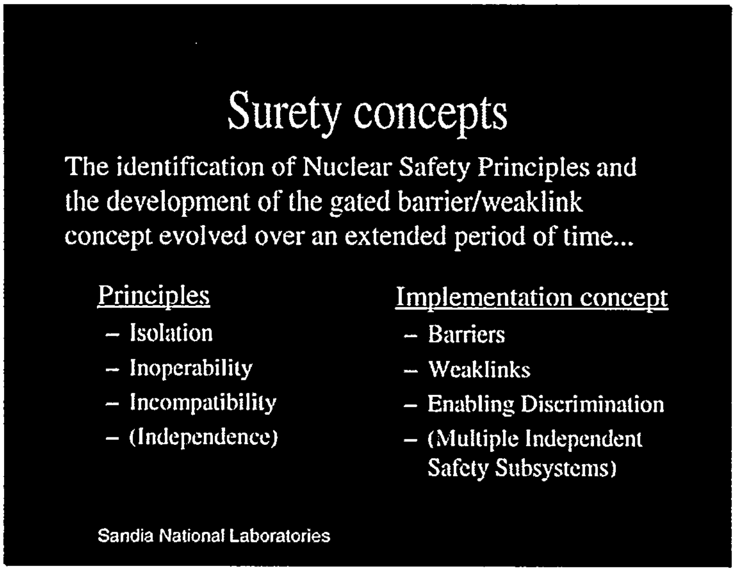
Sandia National Laboratories

Identify and integrate surety elements that are important in the system, resulting in a surety theme. A safety theme describes in a unified fashion the principles that will be used to assure safety under all expected environments.

The value of the theme is it directs design/development efforts towards meeting major requirements and provides a framework in which to communicate the various implementations (some of which, such as safety and security measures, may come into conflict) to surety review groups such as the NESSG. Realizing a safety theme through selection and implementation of first principles may depend on decades of engineering experience and judgment.

The safety theme focuses on those elements of system design that, by association with first principles, become safety critical. These elements must utilize engineered features that are identifiable, analyzable, and controllable. The goal is to minimize the number of system components that are safety-critical in abnormal environments. Because the safety assurance then hinges on a relatively small subset of overall system design, limited design and verification resources can be better focused to improve confidence that predictable safety will result.

Slide 8



Surety concepts

The identification of Nuclear Safety Principles and the development of the gated barrier/weaklink concept evolved over an extended period of time...

<u>Principles</u>

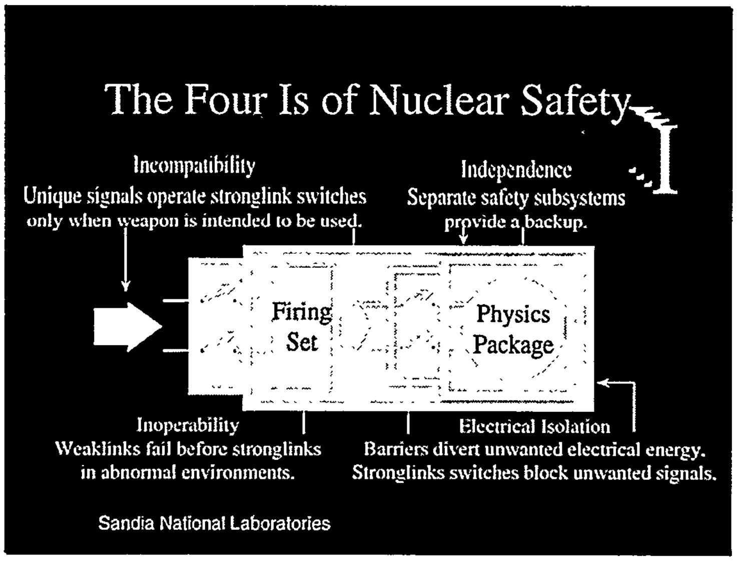
- Isolation
- Inoperability
- Incompatibility
- (Independence)

<u>Implementation concept</u>

- Barriers
- Weaklinks
- Enabling Discrimination
- (Multiple Independent Safety Subsystems)

Sandia National Laboratories

Slide 9



The Four Is of Nuclear Safety

Incompatibility
Unique signals operate stronglink switches only when weapon is intended to be used.

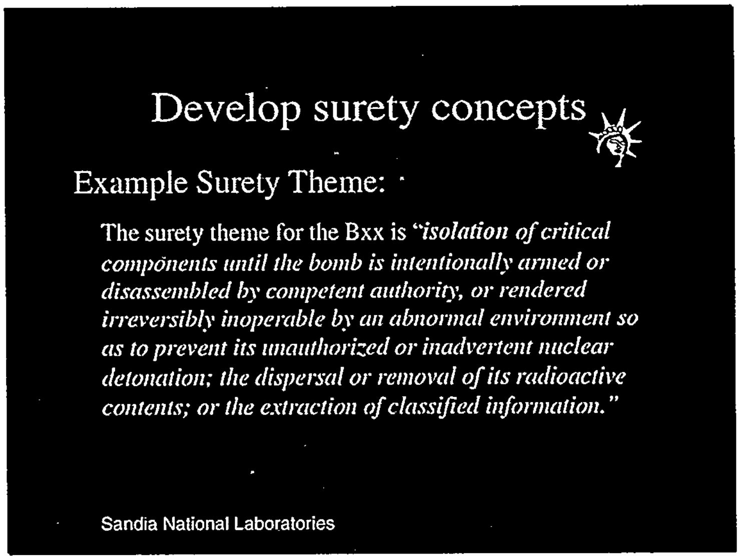
Independence
Separate safety subsystems provide a backup.

Inoperability
Weaklinks fail before stronglinks in abnormal environments.

Electrical Isolation
Barriers divert unwanted electrical energy.
Stronglinks switches block unwanted signals.

Sandia National Laboratories

Slide 10



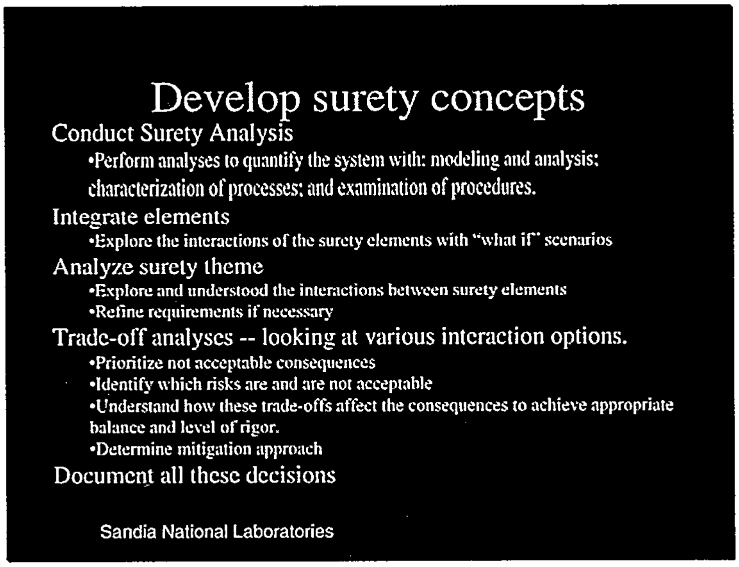
Develop surety concepts

Example Surety Theme:

The surety theme for the Bxx is "*isolation of critical components until the bomb is intentionally armed or disassembled by competent authority, or rendered irreversibly inoperable by an abnormal environment so as to prevent its unauthorized or inadvertent nuclear detonation; the dispersal or removal of its radioactive contents; or the extraction of classified information.*"

Sandia National Laboratories

Slide 11



Develop surety concepts

Conduct Surety Analysis

- •Perform analyses to quantify the system with: modeling and analysis: characterization of processes: and examination of procedures.

Integrate elements

- •Explore the interactions of the surety elements with "what if" scenarios

Analyze surety theme

- •Explore and understood the interactions between surety elements
- •Refine requirements if necessary

Trade-off analyses -- looking at various interaction options.

- •Prioritize not acceptable consequences
- •Identify which risks are and are not acceptable
- •Understand how these trade-offs affect the consequences to achieve appropriate balance and level of rigor.
- •Determine mitigation approach

Document all these decisions

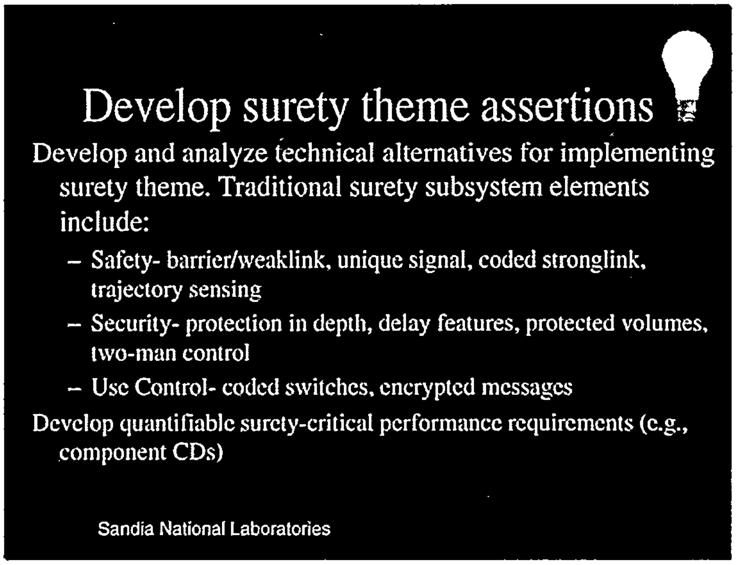
Sandia National Laboratories

Example interactions among surety elements are:

Use control hardware built into the weapon may pose an unintended penetration of a safety barrier

That design information for security/use control typically is classified, but for safety is not, confounds integration efforts

Slide 12



Develop surety theme assertions

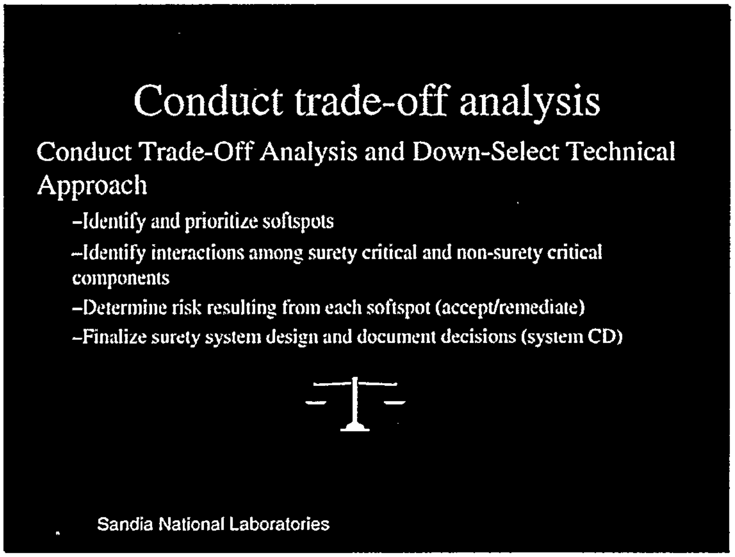
Develop and analyze technical alternatives for implementing surety theme. Traditional surety subsystem elements include:

- Safety- barrier/weaklink, unique signal, coded stronglink, trajectory sensing
- Security- protection in depth, delay features, protected volumes, two-man control
- Use Control- coded switches, encrypted messages

Develop quantifiable surety-critical performance requirements (e.g., component CDs)

Sandia National Laboratories

Slide 13



Conduct trade-off analysis

Conduct Trade-Off Analysis and Down-Select Technical Approach

-Identify and prioritize softspots

-Identify interactions among surety critical and non-surety critical components

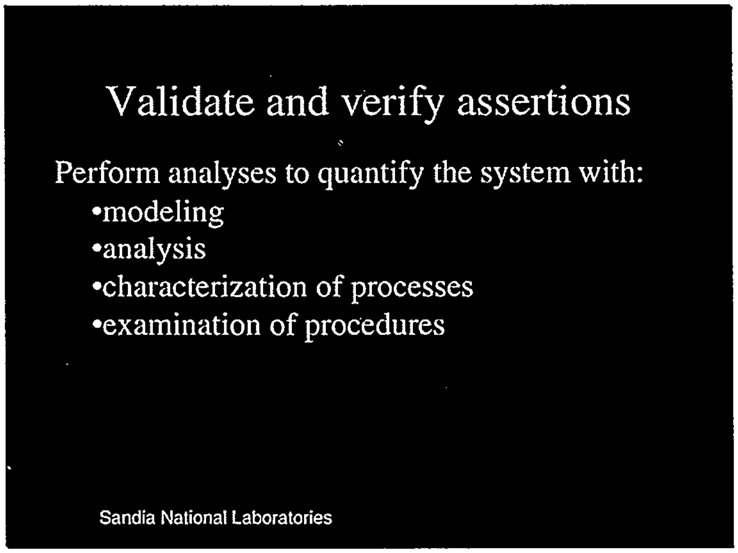
-Determine risk resulting from each softspot (accept/remediate)

-Finalize surety system design and document decisions (system CD)

Sandia National Laboratories

Because other systems requirements must be met (e.g., volume, weight, reliability in operating environments, security, use control, etc.) tradeoffs or compromises in design may be inevitable. Analyses of implications must be done to identify and evaluate associated vulnerabilities. In case of conflict, Sandia policy favors safety.

Slide 14



Validate and verify assertions

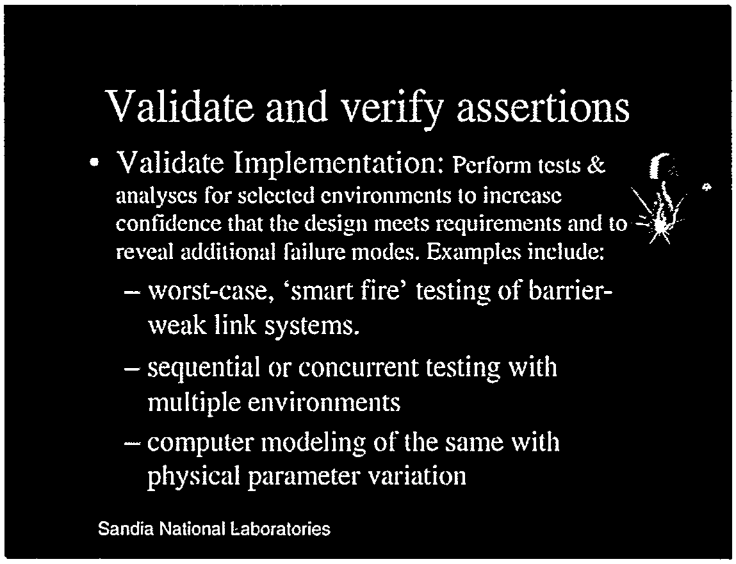
Perform analyses to quantify the system with:

- •modeling
- •analysis
- •characterization of processes
- •examination of procedures

Sandia National Laboratories

The notion of predictability is rooted in the inability to exhaustively test the safety performance of *ad hoc* designs (that may or may not be safe) to countless accident scenarios. Predictable safety is a robust philosophy, backed up by limited testing, that asserts a correctly implemented safety principles-based design will perform as expected under a broad range of accident environments. The interactions between the surety elements must be explored and understood.

Slide 15

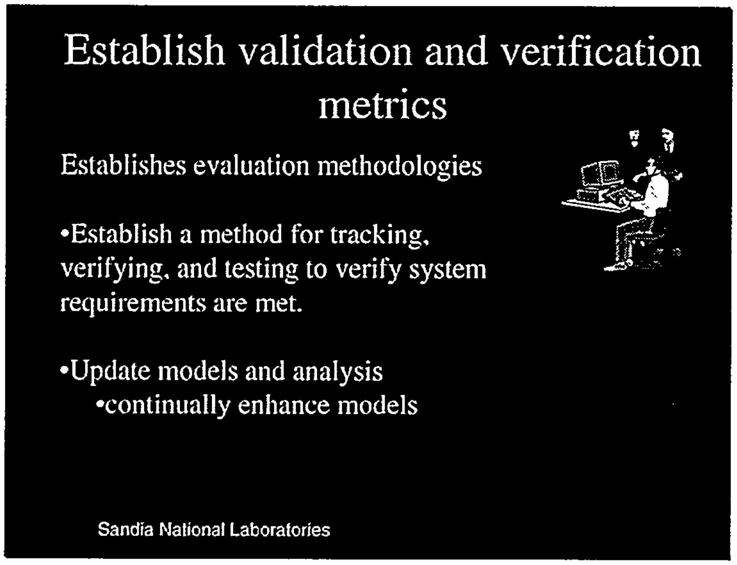


Validate and verify assertions

- Validate Implementation: Perform tests & analyses for selected environments to increase confidence that the design meets requirements and to reveal additional failure modes. Examples include:
  - – worst-case, 'smart fire' testing of barrier-weak link systems.
  - – sequential or concurrent testing with multiple environments
  - – computer modeling of the same with physical parameter variation

Sandia National Laboratories

Slide 16



Establish validation and verification metrics

Establishes evaluation methodologies

- Establish a method for tracking, verifying, and testing to verify system requirements are met.
- Update models and analysis
  - continually enhance models

Sandia National Laboratories

Develop Surety Theme Assertions

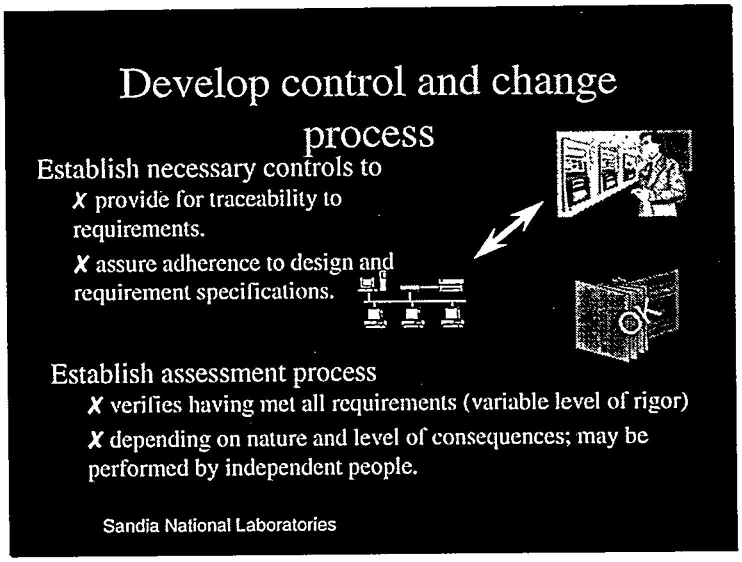
Develop surety performance assertions that are measurable and quantifiable. The implementation of safety critical elements must provide predictable, acceptably safe responses for a component or assembly subjected to specified stimuli such as accident conditions. The design must be 'first principles'-based, that is it must include some characteristic inherent in the physics and/or chemistry of a material--the permanent decomposition of an explosive material subjected to sufficiently high temperature is an example.

Validate and Verify Assertions

Perform analyses to quantify the system with modeling and analysis; characterization of processes; and examination of procedures.

The notion of predictability is rooted in the inability to exhaustively test the safety performance of *ad hoc* designs (that may or may not be safe) to countless accident scenarios. Predictable safety is a robust philosophy, backed up by limited testing, that asserts a correctly implemented safety principles-based design will perform as expected under a broad range of accident environments. The interactions between the surety elements must be explored and understood.

Slide 17



Develop control and change process

Establish necessary controls to

✗ provide for traceability to requirements.

✗ assure adherence to design and requirement specifications.

Establish assessment process

✗ verifies having met all requirements (variable level of rigor)

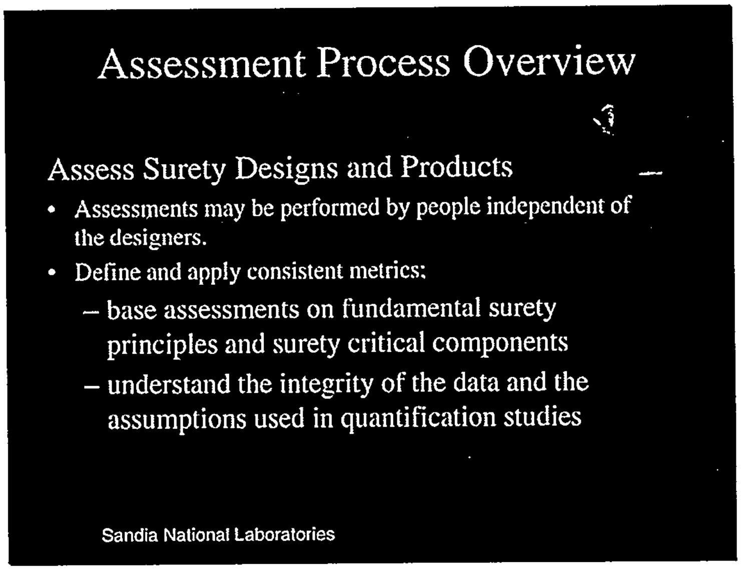
✗ depending on nature and level of consequences; may be performed by independent people.

Sandia National Laboratories

Define, Develop, Implement and Maintain Controls: Surety controls assure adherence to design specifications by tracking, controlling, and testing to verify system requirements are met. Examples of surety controls include:

- production controls such as Pentagon /S/ (for safety)
- emplacement (field assembly) controls for weapon storage vault
- stockpile surveillance, sampling and testing

Slide 18



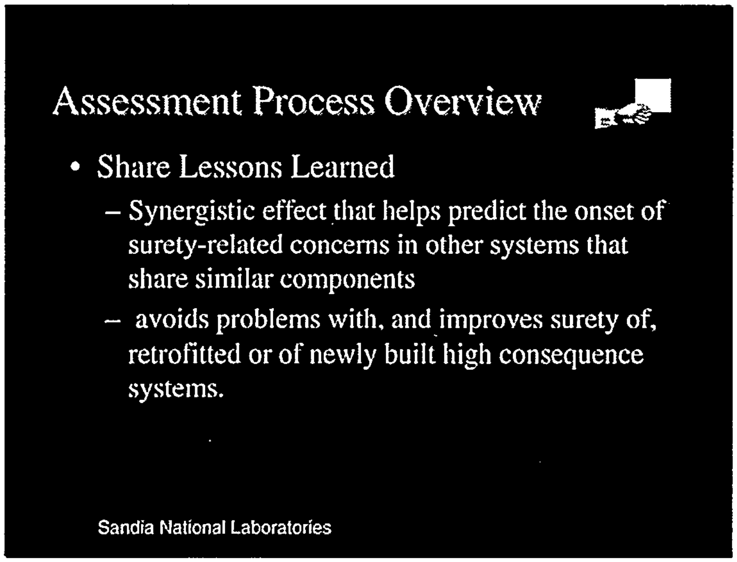
Assessment Process Overview

Assess Surety Designs and Products

- Assessments may be performed by people independent of the designers.
- Define and apply consistent metrics:
  - base assessments on fundamental surety principles and surety critical components
  - understand the integrity of the data and the assumptions used in quantification studies

Sandia National Laboratories

Slide 19



Assessment Process Overview

- Share Lessons Learned
  - Synergistic effect that helps predict the onset of surety-related concerns in other systems that share similar components
  - avoids problems with, and improves surety of, retrofitted or of newly built high consequence systems.

Sandia National Laboratories

Biography

Mr. Perry E. D'Antonio is currently on a special one-year assignment at the Department of Energy's (DOE) Office of Weapons Surety. Prior to this assignment, he managed the System Surety Engineering department at Sandia National Laboratories (SNL). The department develops system safety engineering solutions for nuclear weapons and other industrial high-consequence operations. He holds a Masters Degree in Electrical Engineering from Stanford University. In seventeen years at SNL he has held staff and management positions in weapon systems engineering design and safety assessment, and managed a research program to improve safety technology. He is the SNL representative to the Lockheed-Martin Engineering Process Improvement Center's System Safety Subcouncil. He is a weapons safety expert in the DOE Accident Response Group. Mr. D'Antonio is currently serving as President of the System Safety Society.

Dr. Mark E. Ekman is a Senior Member of the Technical Staff at Sandia National Laboratories. He holds a Ph.D. in Chemical Engineering from Iowa State University. He has led the incorporation of the Pentagon-S process for most of the nuclear weapon safety components in production at multiple DOE production agencies since 1992. He led a DOE multi-agency team to ensure consistency in process implementation throughout the Nuclear Weapons Complex (NWC) and is a co-author of the NWC Technical Business Practices defining the Pentagon-S process. Dr. Ekman is a member of the American Institute of Chemical Engineers and the American Chemical Society.

Dr. John M. Covan is a Senior Member of the Technical Staff at Sandia National Laboratories. He holds a Ph.D. in Nuclear Physics from the University of Arizona and an ME in Industrial Engineering from Texas A&M University. He has held a number of positions cutting across surety engineering at Sandia Laboratories. In the use-control arena, he has evaluated related weapon subsystems and has developed new concepts involving use control. In the detonation safety arena he has modeled new safety concepts, done experiments on electromagnetic sensitivities to premature detonation, and proposed procedures for investing detonation safety directly into new systems. He has also been involved in efforts to transport detonation safety-based concepts beyond this arena to more general commercial applications. He is a member of the System Safety Society and is currently serving on its Standards Committee.

Role as a Consideration of Design Direction for Hazard Mitigation

Robert N. Bettis
Harmon Industries, Inc.
Grain Valley, Missouri

Abstract

This paper proposes a consideration of the role a system, subsystem, device, or component plays in the potential realization of hazards previously identified and classified by well-known traditional methods. A classification system is outlined and application to hazard mitigation is discussed. Examples are supplied and system design techniques suggested.

Introduction

With decreasing development schedules and cost consciousness, hazard mitigation is accounting for an increasing percentage of the development effort. New tools and methods are required to make to most efficient possible use of development resources. A classification system for considering the role a system, subsystem, or device plays in the potential realization of hazards can be of use toward this goal.

In this paper, examples from industry are used to illustrate application to real world systems. Also discussed are some types of design techniques appropriate for differing combinations of hazard levels and role classifications.

The term ***element*** is used to denote a system, a subsystem, or a device or component within a system or subsystem.

Prior Processes

Role Classification does not involve new methods of identifying hazards, categorizing hazard severity, or of identifying contributing elements. Before role classification can be of use, standard safety analysis techniques must have been applied to identify all system level hazards, classify hazard severities, and identify contributing elements.

Hazard Identification

Definition *- Hazard*: Any real or potential condition or event that can cause or contribute to an accident.

The first stage of a safety process is identifying hazards that may be present in or be presented by a system. This is done by such methods as Preliminary Hazard Analysis (PHA) or Subsystem Hazard Analysis (SSHA).

Hazard Classification

Once the hazards have been identified, they must be classified according to severity and, optionally, probability, to determine which must be mitigated. Industry accepted severity classifications are well established. [1]

> Category 1 - Catastrophic: The worst case effects are death and and/or destruction of equipment or property.
>
> Category 2 - Critical: The worst case effects are severe personnel injury and/or major damage to equipment or property.
>
> Category 3 - Marginal: The worst case effects are minor personnel injury and/or minor damage to equipment or property.
>
> Category 4 - Negligible: The worst case effects are less than minor personnel injury and/or minor damage to equipment or property.

Source Identification

After the hazards have been identified and classified, the potential source elements of the hazard must be identified. This may be done through Fault Tree Analysis (FTA) [2], Failure Mode, Effects and Criticality Analysis (FMECA) [3], or any of the other methods in common industry use.

The Dilemma

A particular hazard may have numerous elements that can cause or allow a hazard to manifest by single failure or by failure in combination with other element failures.

Hazards can be mitigated at different levels, using a variety of techniques, with different costs in resources.

For a particular hazard, the severity is the same regardless of which potentially contributing element actually failed.

Making all subsystems, modules, etc. fail-safe, redundant, and so on, can always increase safety. However, the law of diminishing return applies to a safety effort as much as to the rest of engineering. The end result can be extended development schedules, increased costs and complexity, and sometimes-reduced functionality.

The design question then becomes "Where should design efforts be concentrated to get the greatest safety improvement for the resources expended?" When design prioritization is done, it is often on an 'ad hoc' or intuitive approach based on the ability and experience of the design team, thus leading to inconsistent results.

Role Classification

An approach to resolving this is to classify the contributing devices according to the type of involvement in the potential realization of the hazard. The resulting classification can be used to help determine appropriate mitigation techniques for each of the potential contributors.

Type of involvement

The first consideration is "How can the element under consideration contribute to the hazard?" Type of involvement can be broken down into the following five categories:

- Type A, Active Direct - The element can, by its inappropriate action or inaction, directly cause the hazard to manifest.
- Type B, Active Indirect - The element can, by its inappropriate action or inaction, allow the hazard to manifest. It cannot cause the hazard to manifest, but has the responsibility of preventing the hazard from occurring.
- Type C, Passive Direct - The element can, by misinformation of value or status, lead to inappropriate action causing the hazard to manifest. It cannot directly cause the hazard to manifest, and does not have responsibility for directly preventing the hazard from occurring. The element has the responsibility of providing status or values to guide the actions of operators or other devices.
- Type D, Passive Indirect - The element can, by misinformation of value or status, lead to inappropriate inaction allowing the hazard to manifest. It cannot directly cause the hazard to manifest, and does not have responsibility for directly preventing the hazard from occurring. The element has the responsibility of providing status or values, thus alerting operators or other devices of a potentially hazardous condition requiring action.
- Type E, Uninvolved - No action or inaction by the element can contribute to causing or allowing the hazard to manifest.

Level of Involvement

Level of involvement must also be considered. Can failure of the element alone cause or allow the hazard to manifest, or must other failures be present also? Two levels of involvement derive:

- Singular - A failure of the element is sufficient in and of itself to cause or allow the hazard to manifest.

- Grouped - A failure of the element must be combined with another failure of equipment and/or procedure for the hazard to manifest.

Role Classification

Combining Type and Level of involvement results in the following Role Classifications:

Table 1. Role Classification

	Singular	Grouped
Active Direct	AS	AG
Active Indirect	BS	BG
Passive Direct	CS	CG
Passive Indirect	DS	DG
Uninvolved	E	

Recursive Classification

Once an element has been categorized by role, it may be further subdivided and the process repeated on its parts. No part can have a higher role classification than the higher-level assembly or system to which it belongs.

Appropriate Mitigation

Definition *- Fail Operational*: A characteristic of systems that rely on redundancy, back-up facilities, and operators to minimize the probability of catastrophic failures and maintain it's primary function to the extent possible.

Definition *- Fail Safe*: No single failure or no single failure combined with latent failures will result in a catastrophic failure. The failure must lead to no effect upon the safety of the system, or must lead to a known safe state. The system must have a defined safe state for this to be possible.

Elements with differing role classifications require differing levels of engineering efforts and techniques to give adequate protection.

Roles AS and BS

For this classification, one of the following should occur:

- Analysis should show the element to be fail safe.
- Design efforts should be initiated to make the design fail safe.
- Design efforts should be initiated to reduce the role classification through alternative designs, addition of redundancy to ensure fail operational capability, addition of interlocking devices, and so on.

Roles CS and DS

For devices presenting status or value, fail-safe design or interlockings are not generally viable options. Therefore, for this classification, one of the following should occur:

- Analysis should show the element being presented the information to be fail safe.
- Design efforts should be initiated to reduce the role classification through alternative designs, addition of redundancy, and so on.
- Institute periodic testing to ensure that failures will not be latent. Failures must be capable of being detected and fixed in a period of time sufficiently short to minimize the probability of the hazard occurring simultaneously with the failure of the element under consideration.

Roles AG through DG

For elements with a Grouped level of involvement, design efforts should:

- Ensure through analysis and testing that no common-mode failures exist between the involved elements.
- Ensure that failures will not be latent. Failures must be capable of being detected and fixed in a period of time sufficiently short to minimize the probability of a second failure occurring simultaneously.

Role E - Uninvolved

No further mitigation effort is required.

Design Precedence

Note that when it is determined that a system or device requires further mitigation efforts, those efforts should follow established Design Control Precedence: [4]

(1) Design for acceptable hazard (design the hazard out).
(2) Safety devices (protect against the hazard).
(3) Warning devices (warn of the hazard when it occurs).
(4) Procedures and training (take corrective action for the hazard).

Examples

Some examples will serve to illustrate the points made here. The first will be a general example starting with a known hazard, a train derailment. The second will be a look at some elements involved in a well-documented [5][6] accident, the Union Carbide Bhopal disaster.

Train Derailment

A train derailment is classified as Hazard Category 1 - Catastrophic. Following are several devices for which failures have been identified as potentially contributing to this hazard.

Track switch machine: A device that moves a track switch to direct train movement between two sets of rails. If this device fails in a manner that moves the switch under a train, a derailment is the likely result.

Since inappropriate action directly causes the hazard, and since this single failure is sufficient to cause the hazard, the Role Classification is AS. Its nature prevents fail operational design through redundancy. It should be:

- Shown by analysis to be fail safe OR
- Must have a safety device, such as an interlock OR
- Be covered by procedure, such as "Remove power when a train is present."

If no such mitigation is present, design or procedure changes are indicated.

Note that the same device may be a contributor to other hazards, such as train collision if it misroutes a train. It should be classified separately for each hazard in which it is a consideration.

Train Speed Limiter: A device that monitors train speed and limits it to a safe value. If this device fails, the operator would be allowed to exceed the safe operating speed, potentially resulting in a derailment.

Since failure allows the hazard to manifest, the type of involvement is Active Indirect. Since the single failure is sufficient to allow the hazard, the Role Classification is **BS**.

If this device is subdivided into a Brake output, Speed Sensor, and Controller, these elements can be evaluated.

The Brake Output would be **BS**. The Controller portion is also **BS**. For both of these elements, an appropriate technique would be fail-safe design.

The Speed Sensor which provides speed information to the Controller is **DS**. An appropriate mitigation would be redundant Speed Sensors, which would change the classification to **DG**.

Note that should the Speed Limiter be in control of the throttle instead of or in addition to the brake, so that a failure could *cause* the overspeed condition, it would be classified **AS**.

Train Speed Limit Display: A device that monitors train speed limits and displays them to the operator to inform the operator of the maximum safe operating speed. If this device fails, the operator might be misled and exceed the safe operating speed, potentially resulting in a derailment.

Failure does not directly cause the hazard to manifest, and the device does not have responsibility for preventing the hazard. If this is the only control on train speed, the Role Classification is Type **CS**. If the train also has a Train Speed Limiter, the Role Classification is CG.

Bhopal

The worst industrial accident recorded occurred in December 1984 when a Union Carbide plant released large amounts of methyl isocyanate (MIC) gas into the city of Bhopal, India. This resulted in 3000 to 4000 persons dead and more than 200,000 seriously injured.

As background, the proximate cause of the release was the introduction of a large amount of water into MIC storage tank #610. This resulted in an exothermic reaction reaching a temperature of 120° Celsius. Since the boiling point of MIC is 37° Celsius, the resulting pressure exploded the tank, releasing the MIC in the form of heavier-than-air vapor.

While much has been written about the causes of the disaster, it might be instructive to apply Role Classification to some of the various devices and subsystems identified as contributors.

Inlet Pipe: The inlet pipe, by introducing water, directly initiated the hazard. It would be classified as Type A - Active Direct. As such, it should be fail-safe (no capability of introducing water) or have a Grouped level of involvement.

In point of fact, since it was necessary to periodically introduce water to wash the pipe, a safety device was designed in case the pipe valves leaked. A safety disk called a 'slip-blind' was supposed to be inserted to back up the valves during pipe washing.

Slip-Blind: The slip-blind had the responsibility of preventing the hazard. With no water present, its function would be irrelevant to the hazard. It would be classified as Type B - Active Indirect.

While it required failure of both the inlet pipe valves and absence of the slip-bind to introduce the water, they cannot together be truly classified as 'Grouped.' Neither had any failure detection designed in. Failure of the valves or absence of the slip-bind was latent, giving ample window of opportunity for failure of the other.

Pressure/Temperature Gauges: The tank had temperature and pressure gauges that gave warning of the reaction in terms of increased pressure and temperature. As their task was to alert the operators of needed action, they would be classified as Type D - Passive Indirect. They were however, so unreliable as to be disbelieved and alarms were no longer even logged. Type D devices, while not required to be fail-safe, must be of sufficient reliability as to be credible.

Refrigeration System: A refrigeration system was in place to keep the MIC at 0° Celsius to limit reactivity in the presence of water. As a Type B subsystem it should have been redundant, to be Fail Operational, or backed up by an alarm to indicate non-functionality. It had in fact been turned off five months earlier as a cost-cutting measure. The related temperature gauge has been examined above.

Overflow Tank: The 'first line of defense' in the event of a reaction in Tank #610 was an interconnected overflow Tank #619. Bleeding chemical into Tank #619 could relieve overpressure in Tank #610. This would be a Type B device. Fail-safe design might have employed a rupture disk to automatically initiate transfer at a set overpressure. Instead, it was required that the operator open valves between the two tanks after being alerted. This was not done.

Water Curtain/Gas Scrubber/Flare Tower: These were all "last ditch" containment devices designed to neutralize already generated MIC gas by acting in concert. The gas scrubber was to chemically neutralize escaping MIC gas. The Flare Tower was to burn MIC escaping from the scrubber. The water curtain was to neutralize any remaining gas by spraying the flare tower output.

These would all be classified as Type B - Active Indirect. Properly designed, they could be labeled as "Grouped." On the night of the accident however, only the Water Curtain was operational, and its designed operating height would not reach the top of the Flare Tower unless the water jets were operated individually.

At Bhopal, the latent failures of numerous Type B independent safety devices contributed greatly to the disaster.

Conclusion

While not a panacea, Role Classification can play an important part in the engineering decision making process. It can help identify those parts of a system where design efforts will give the biggest increase in system safety for the relative effort involved. It can also help determine the type of mitigation required. Adequate mitigation still requires careful attention to design precedence and especially failure detection of safety devices.

References

[1] U.S. Department of Defense. *MIL-STD-882C, System Safety Program Requirements.* 19 January 1993.

[2] U.S. Nuclear Regulatory Commission. *NUREG-0492, Fault Tree Handbook.* January 1981.

[3] U.S. Department of Defense. *MIL-STD-1629A, Procedures For Performing a Failure Mode, Effects and Criticality Analysis.* 24 November 1980.

[4] Roland, Harold & Moriarty, Brian. *System Safety Engineering and Management.* pp 188-190. ISBN 0-471-09695-4. John Wiley & Sons, Inc. New York 1983.

[5] Leveson, Nancy G. *Safeware - System Safety and Computers.* ISBN 0-201-11972-2. Addison-Wesley Publishing Company, 1995.

[6] Kurzman, Dan. *A Killing Wind: Inside Union Carbide and The Bhopal Catastrophe.* McGraw Hill, 1987.

Biography

Robert N. Bettis, BSEE, P.E.
Harmon Industries, Inc.
31003 E. Argo Rd.
Grain Valley, MO 64029

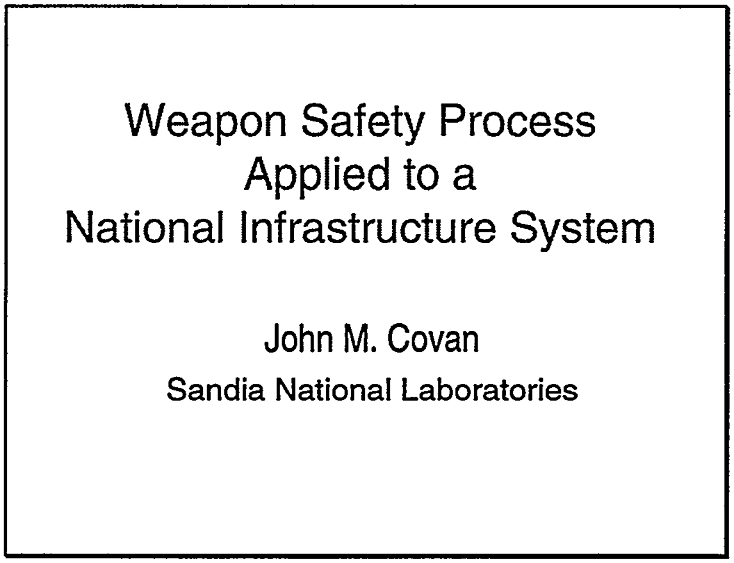
Mr. Bettis is a Senior Safety Engineer for Harmon Industries, a major railroad supplier. His degree in Electrical Engineering is from the University of Missouri. He is a member of Triangle Fraternity and IEEE. Before becoming involved in safety analysis, he designed hardware and software for embedded systems in several industries. He is a registered professional engineer in Missouri.

Intentionally left blank

Weapon Safety Process Applied to a National Infrastructure System

John M. Covan
Sandia National Laboratories*
Albuquerque, New Mexico

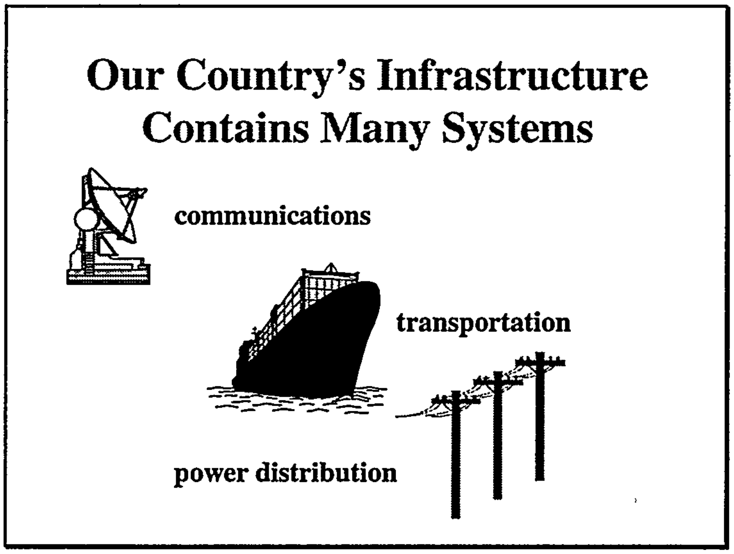
Slide 1



Weapon Safety Process
Applied to a
National Infrastructure System

John M. Covan
Sandia National Laboratories

Slide 2



Our Country's Infrastructure Contains Many Systems

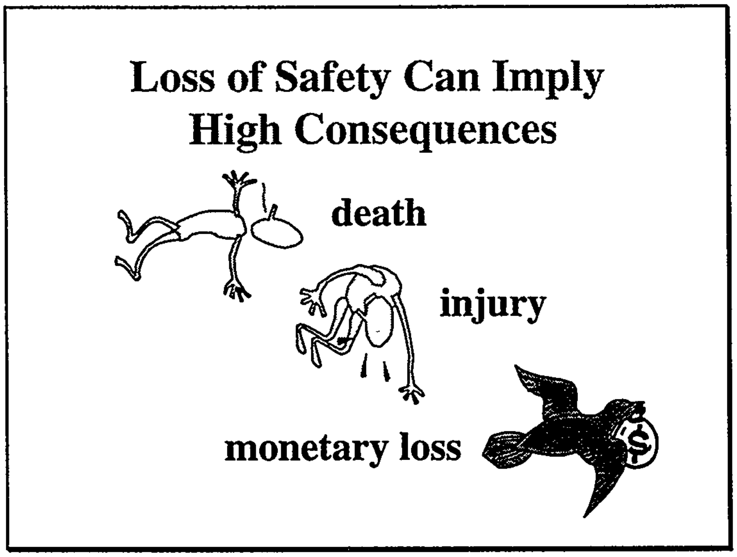
communications

transportation

power distribution

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

Slide 3



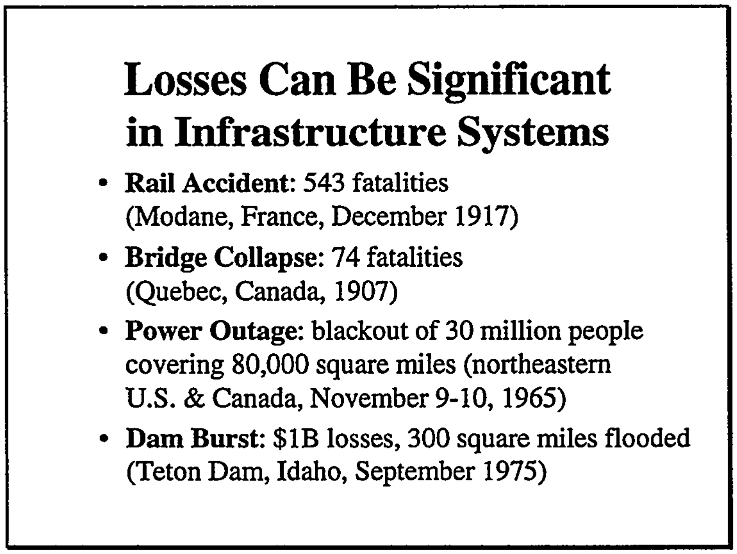
Loss of Safety Can Imply High Consequences

death

injury

monetary loss

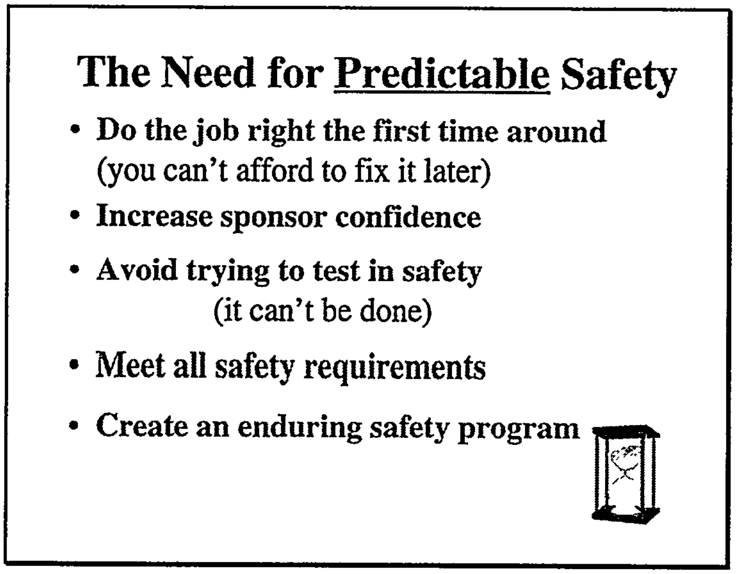
Slide 4



Losses Can Be Significant in Infrastructure Systems

- **Rail Accident**: 543 fatalities (Modane, France, December 1917)
- **Bridge Collapse**: 74 fatalities (Quebec, Canada, 1907)
- **Power Outage**: blackout of 30 million people covering 80,000 square miles (northeastern U.S. & Canada, November 9-10, 1965)
- **Dam Burst**: $1B losses, 300 square miles flooded (Teton Dam, Idaho, September 1975)

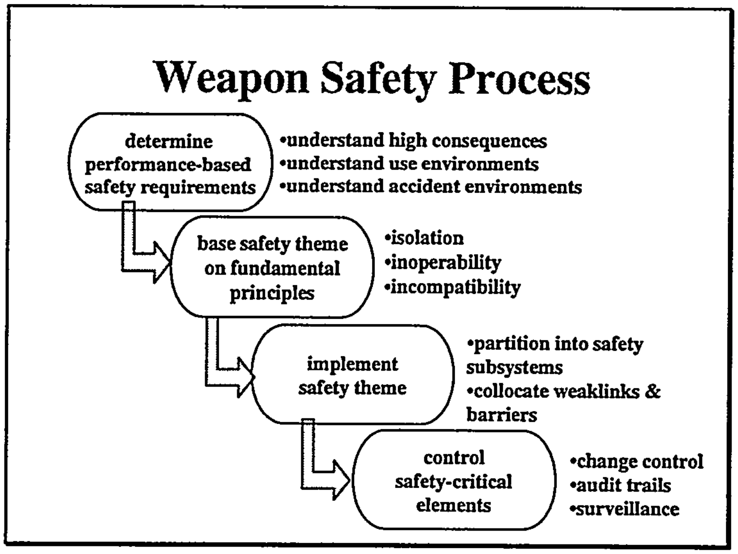
Slide 5



The Need for Predictable Safety

- Do the job right the first time around (you can't afford to fix it later)
- Increase sponsor confidence
- Avoid trying to test in safety (it can't be done)
- Meet all safety requirements
- Create an enduring safety program

Slide 6



Weapon Safety Process

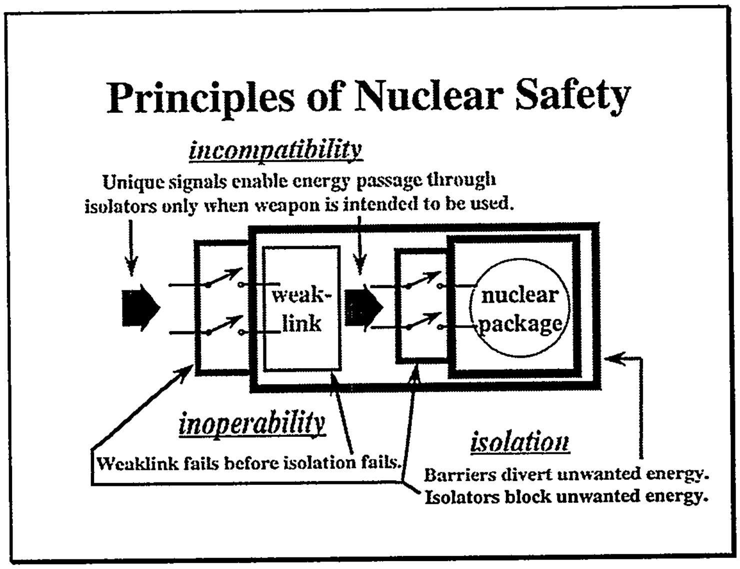
determine performance-based safety requirements
- •understand high consequences
- •understand use environments
- •understand accident environments

base safety theme on fundamental principles
- •isolation
- •inoperability
- •incompatibility

implement safety theme
- •partition into safety subsystems
- •collocate weaklinks & barriers

control safety-critical elements
- •change control
- •audit trails
- •surveillance

Slide 7



Principles of Nuclear Safety

incompatibility

Unique signals enable energy passage through isolators only when weapon is intended to be used.

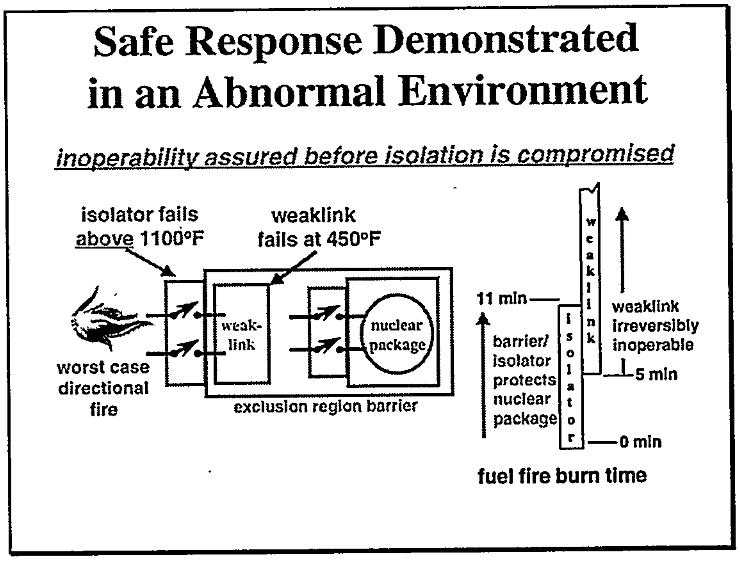
inoperability

Weaklink fails before isolation fails.

isolation

Barriers divert unwanted energy.
Isolators block unwanted energy.

Slide 8

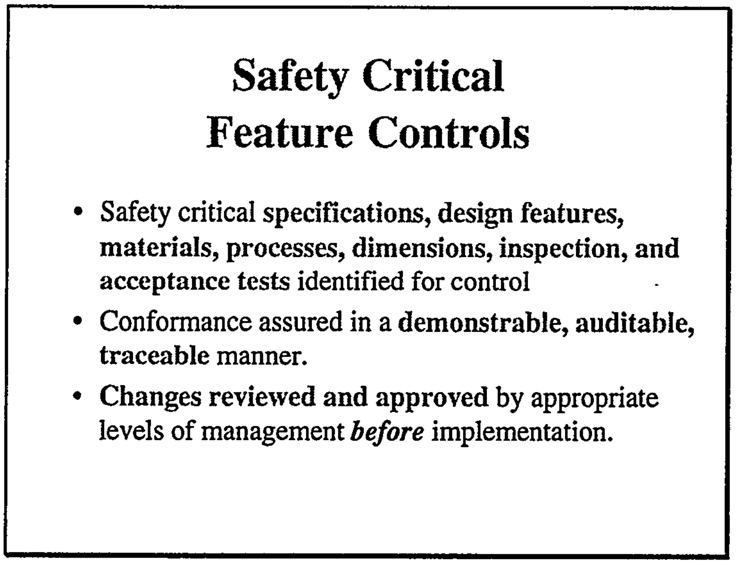


Safe Response Demonstrated in an Abnormal Environment

inoperability assured before isolation is compromised

isolator fails above 1100°F
weaklink fails at 450°F
worst case directional fire
weak-link
nuclear package
exclusion region barrier
11 min
barrier/ isolator protects nuclear package
isolator
weaklink
weaklink irreversibly inoperable
5 min
0 min
fuel fire burn time

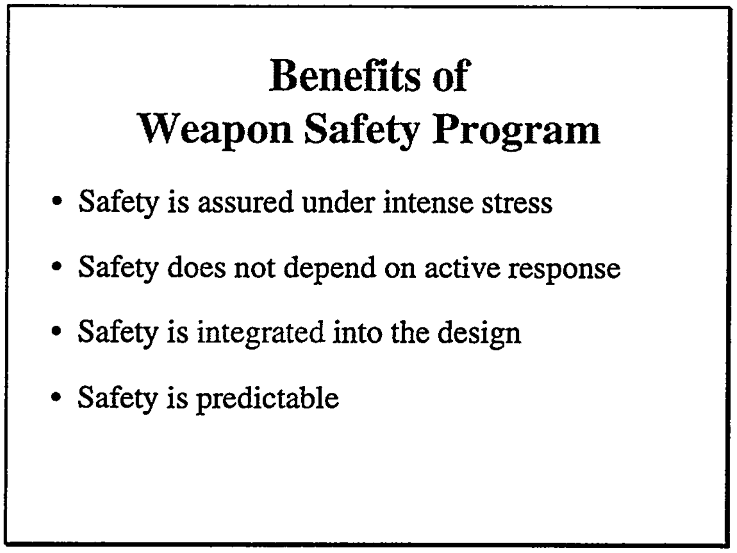
Slide 9



Safety Critical Feature Controls

- Safety critical specifications, design features, materials, processes, dimensions, inspection, and acceptance tests identified for control
- Conformance assured in a demonstrable, auditable, traceable manner.
- Changes reviewed and approved by appropriate levels of management ***before*** implementation.

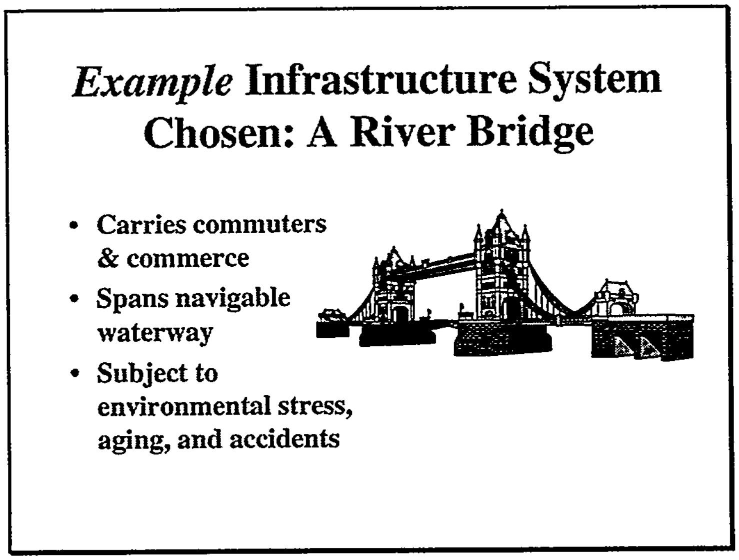
Slide 10



Benefits of Weapon Safety Program

- Safety is assured under intense stress
- Safety does not depend on active response
- Safety is integrated into the design
- Safety is predictable

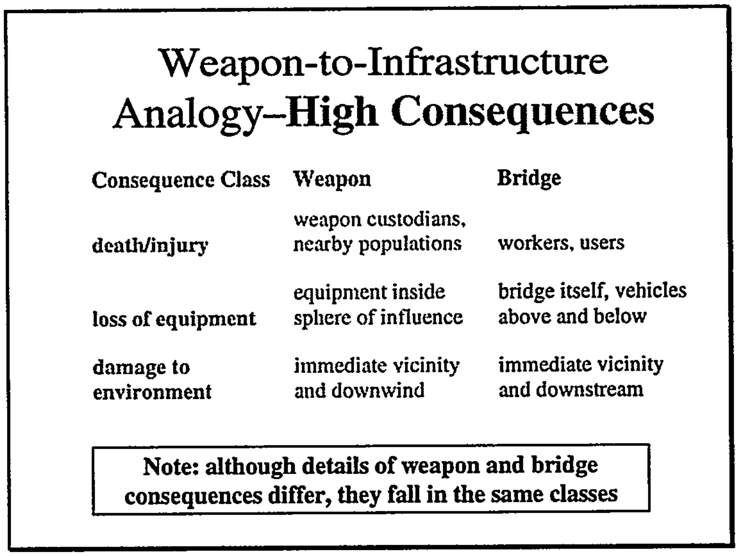
Slide 11



Example Infrastructure System Chosen: A River Bridge

- Carries commuters & commerce
- Spans navigable waterway
- Subject to environmental stress, aging, and accidents

Slide 12

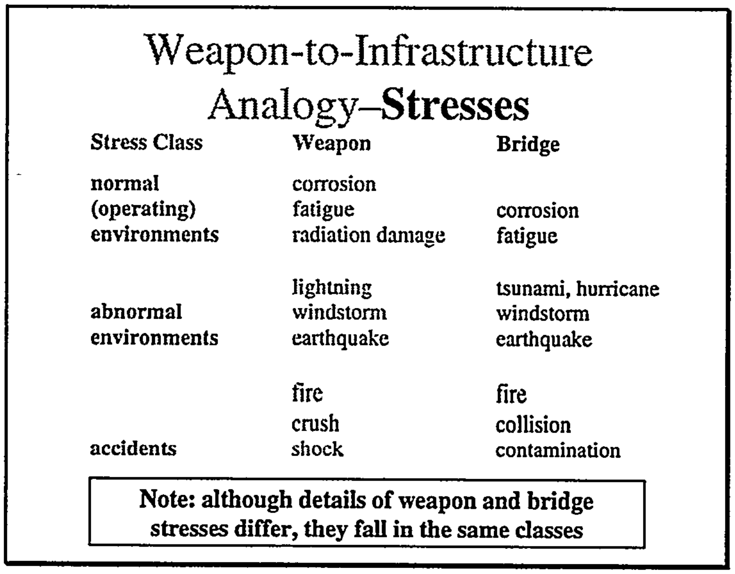


Weapon-to-Infrastructure Analogy–**High Consequences**

Consequence Class	Weapon	Bridge
death/injury	weapon custodians, nearby populations	workers, users
loss of equipment	equipment inside sphere of influence	bridge itself, vehicles above and below
damage to environment	immediate vicinity and downwind	immediate vicinity and downstream

Note: although details of weapon and bridge consequences differ, they fall in the same classes

Slide 13

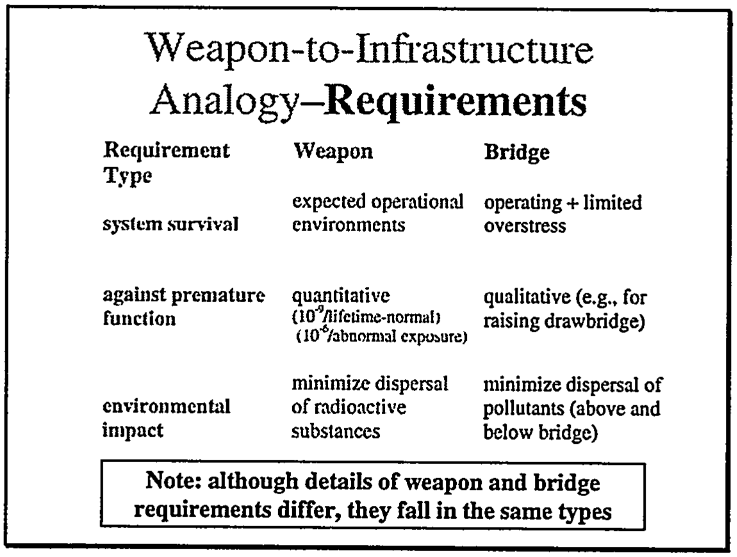


Weapon-to-Infrastructure Analogy–**Stresses**

Stress Class	**Weapon**	**Bridge**
normal (operating) environments	corrosion fatigue radiation damage	corrosion fatigue
abnormal environments	lightning windstorm earthquake	tsunami, hurricane windstorm earthquake
accidents	fire crush shock	fire collision contamination

Note: although details of weapon and bridge stresses differ, they fall in the same classes

Slide 14

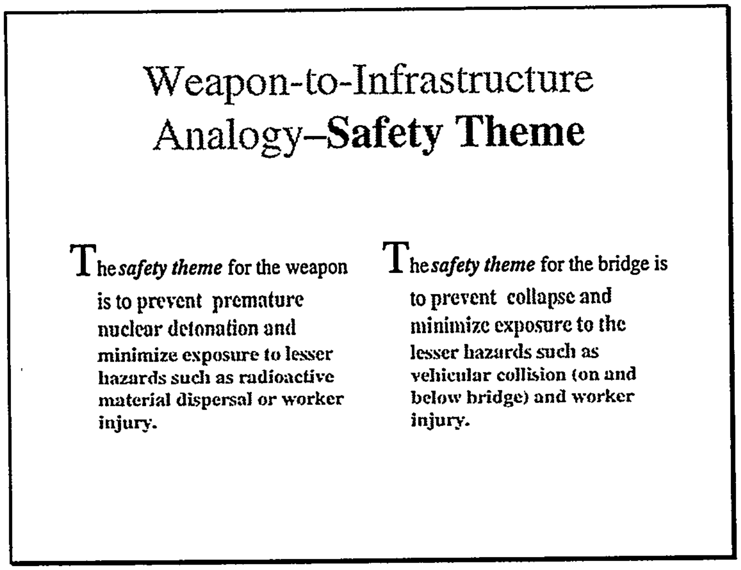


Weapon-to-Infrastructure Analogy–**Requirements**

Requirement Type	**Weapon**	**Bridge**
system survival	expected operational environments	operating + limited overstress
against premature function	quantitative (10^{-9}/lifetime-normal) (10^{-6}/abnormal exposure)	qualitative (e.g., for raising drawbridge)
environmental impact	minimize dispersal of radioactive substances	minimize dispersal of pollutants (above and below bridge)

Note: although details of weapon and bridge requirements differ, they fall in the same types

Slide 15

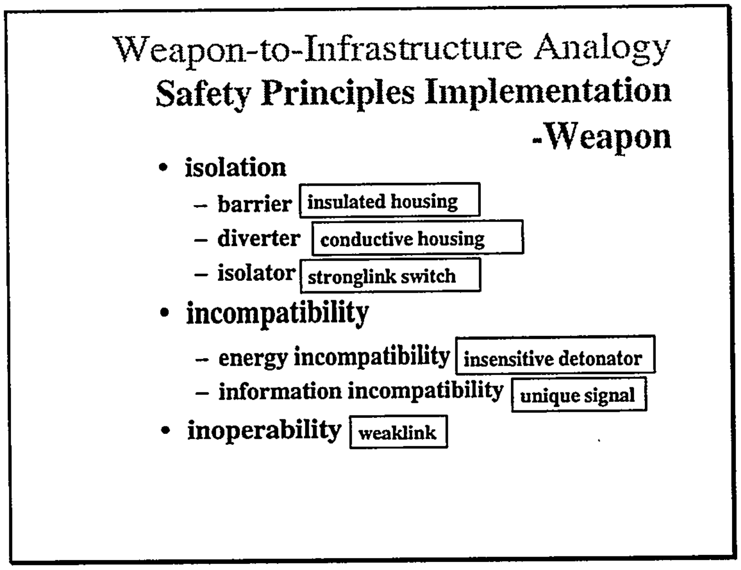


Weapon-to-Infrastructure Analogy–**Safety Theme**

The *safety theme* for the weapon is to prevent premature nuclear detonation and minimize exposure to lesser hazards such as radioactive material dispersal or worker injury.

The *safety theme* for the bridge is to prevent collapse and minimize exposure to the lesser hazards such as vehicular collision (on and below bridge) and worker injury.

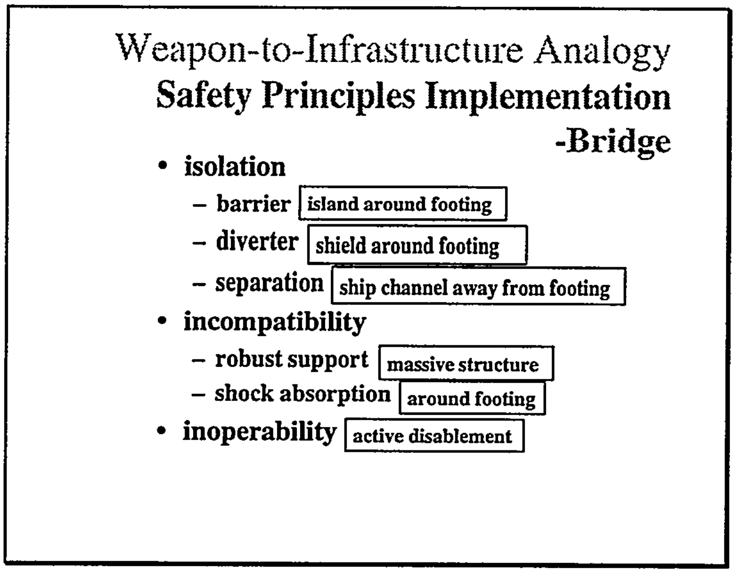
Slide 16



Weapon-to-Infrastructure Analogy **Safety Principles Implementation -Weapon**

- **isolation**
  - **barrier** insulated housing
  - **diverter** conductive housing
  - **isolator** stronglink switch
- **incompatibility**
  - **energy incompatibility** insensitive detonator
  - **information incompatibility** unique signal
- **inoperability** weaklink

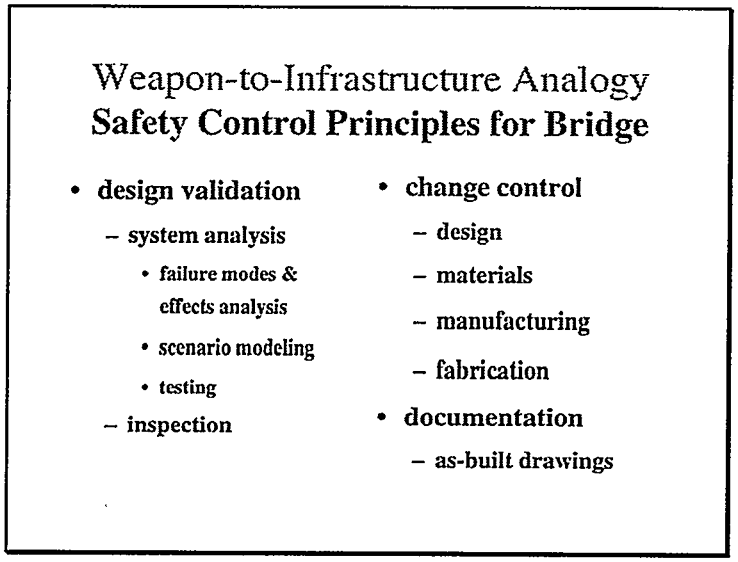
Slide 17



Weapon-to-Infrastructure Analogy
Safety Principles Implementation -Bridge

- **isolation**
  - **barrier** **island around footing**
  - **diverter** **shield around footing**
  - **separation** **ship channel away from footing**
- **incompatibility**
  - **robust support** **massive structure**
  - **shock absorption** **around footing**
- **inoperability** **active disablement**

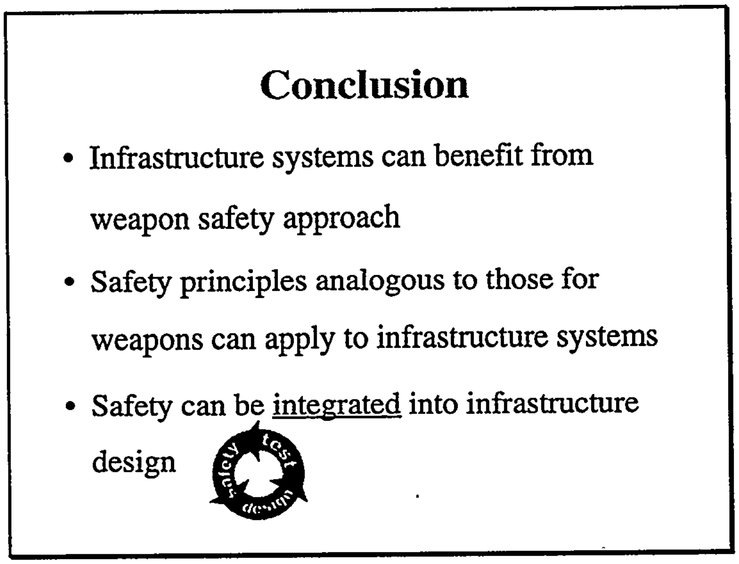
Slide 18



Weapon-to-Infrastructure Analogy
Safety Control Principles for Bridge

- **design validation**
  - system analysis
    - failure modes & effects analysis
    - scenario modeling
    - testing
  - inspection
- **change control**
  - design
  - materials
  - manufacturing
  - fabrication
- **documentation**
  - as-built drawings

Slide 19



Conclusion

- Infrastructure systems can benefit from weapon safety approach
- Safety principles analogous to those for weapons can apply to infrastructure systems
- Safety can be <u>integrated</u> into infrastructure design

safety
test
design

An Approach to Systems Safety

Frank F. Dean
Keith Ortiz
Sandia National Laboratories*
Albuquerque, New Mexico

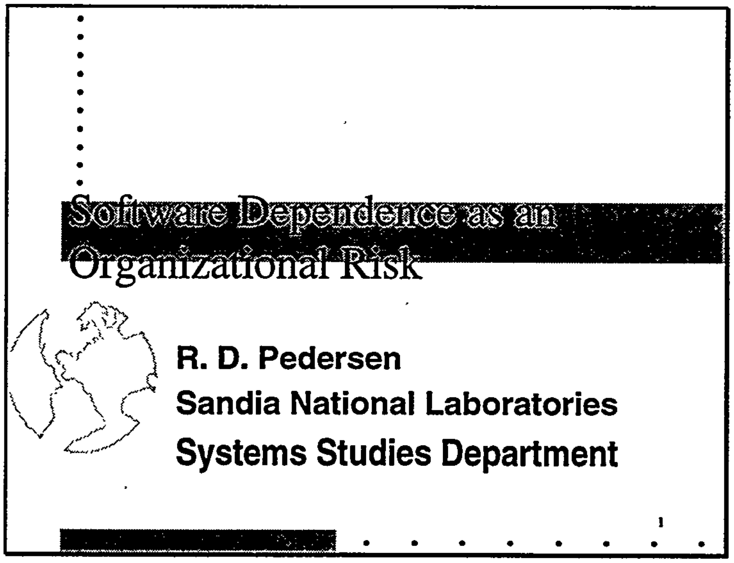
* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

Intentionally left blank

Software Dependence as an Organizational Risk

R. D. Pedersen
Sandia National Laboratories*
Albuquerque, New Mexico

Slide 1

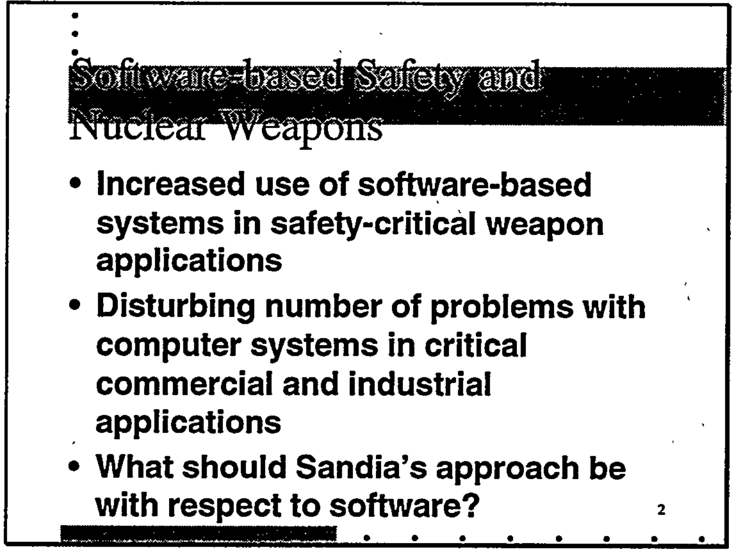


Software Dependence as an Organizational Risk

R. D. Pedersen
Sandia National Laboratories
Systems Studies Department

1

Slide 2



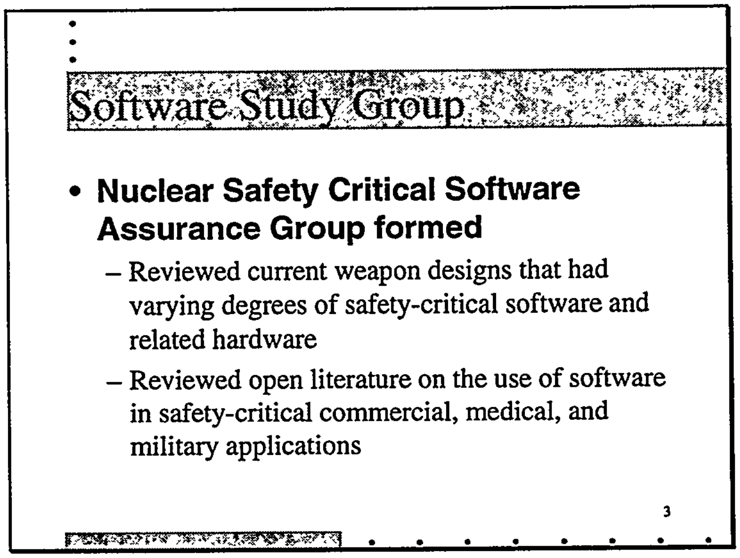
Software-based Safety and Nuclear Weapons

- **Increased use of software-based systems in safety-critical weapon applications**
- **Disturbing number of problems with computer systems in critical commercial and industrial applications**
- **What should Sandia's approach be with respect to software?**

2

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

Slide 3

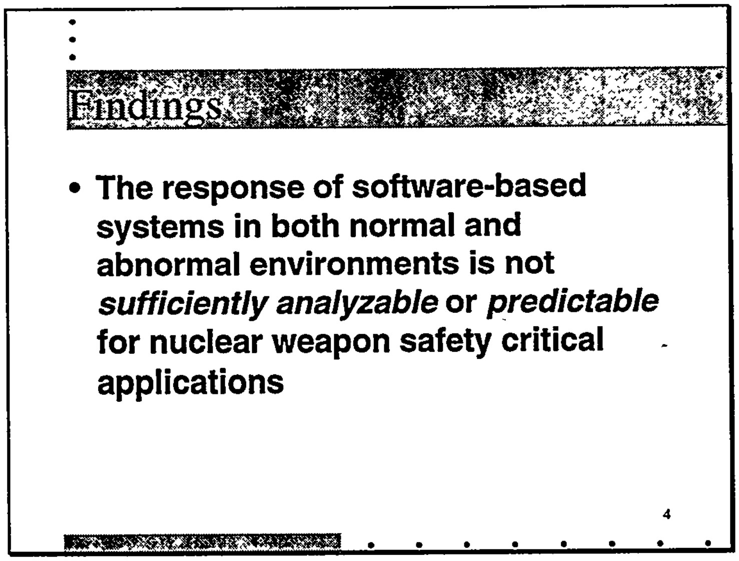


Software Study Group

- **Nuclear Safety Critical Software Assurance Group formed**
  - Reviewed current weapon designs that had varying degrees of safety-critical software and related hardware
  - Reviewed open literature on the use of software in safety-critical commercial, medical, and military applications

3

Slide 4

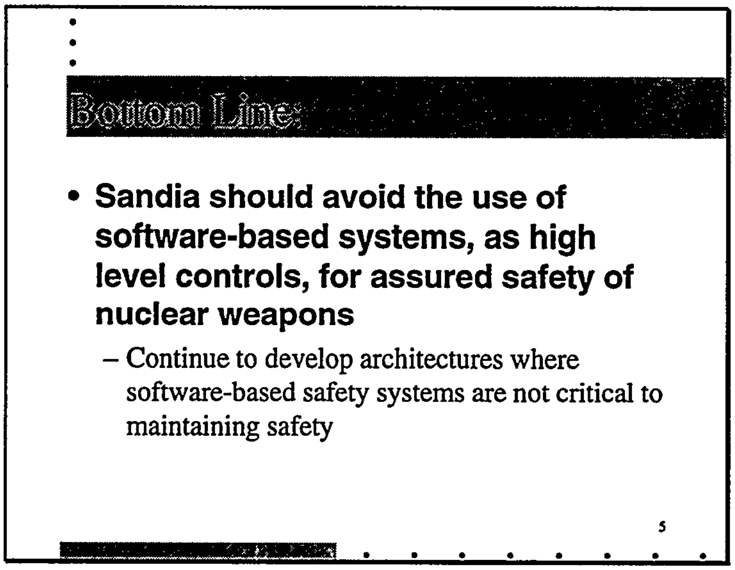


Findings

- **The response of software-based systems in both normal and abnormal environments is not *sufficiently analyzable* or *predictable* for nuclear weapon safety critical applications**

4

Slide 5

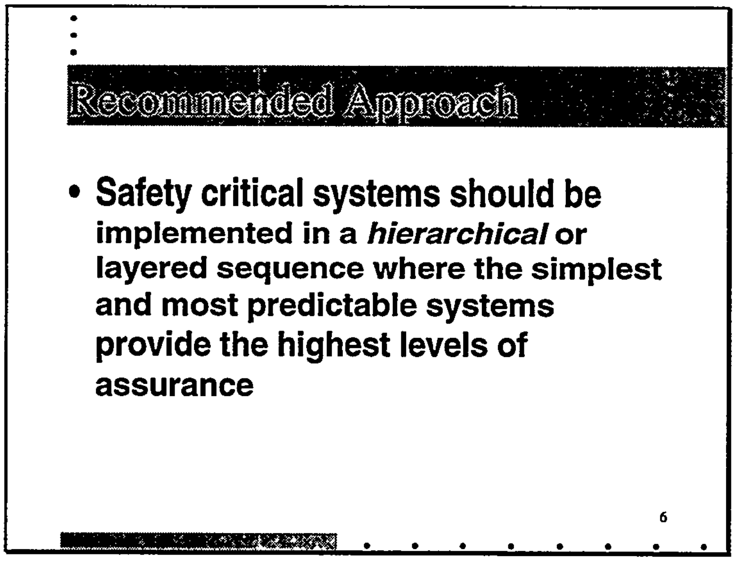


Bottom Line:

- **Sandia should avoid the use of software-based systems, as high level controls, for assured safety of nuclear weapons**
  - Continue to develop architectures where software-based safety systems are not critical to maintaining safety

5

Slide 6

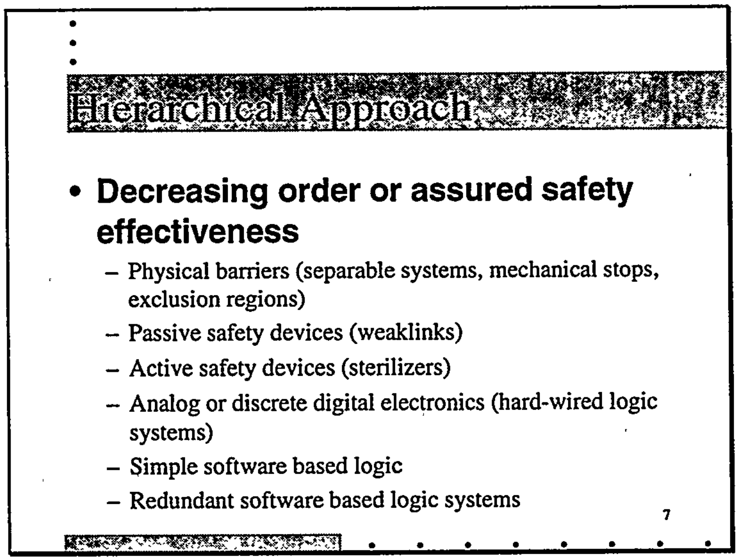


Recommended Approach

- **Safety critical systems should be implemented in a *hierarchical* or layered sequence where the simplest and most predictable systems provide the highest levels of assurance**

6

Slide 7

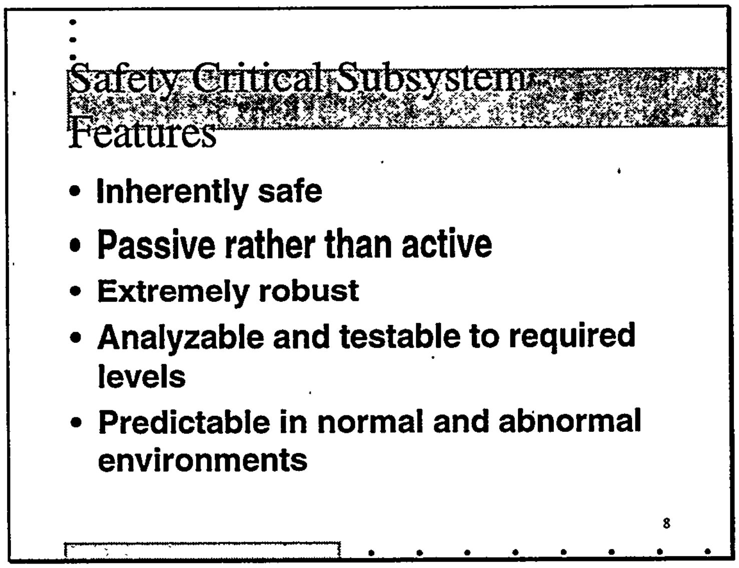


Hierarchical Approach

- **Decreasing order or assured safety effectiveness**
  - Physical barriers (separable systems, mechanical stops, exclusion regions)
  - Passive safety devices (weaklinks)
  - Active safety devices (sterilizers)
  - Analog or discrete digital electronics (hard-wired logic systems)
  - Simple software based logic
  - Redundant software based logic systems

7

Slide 8

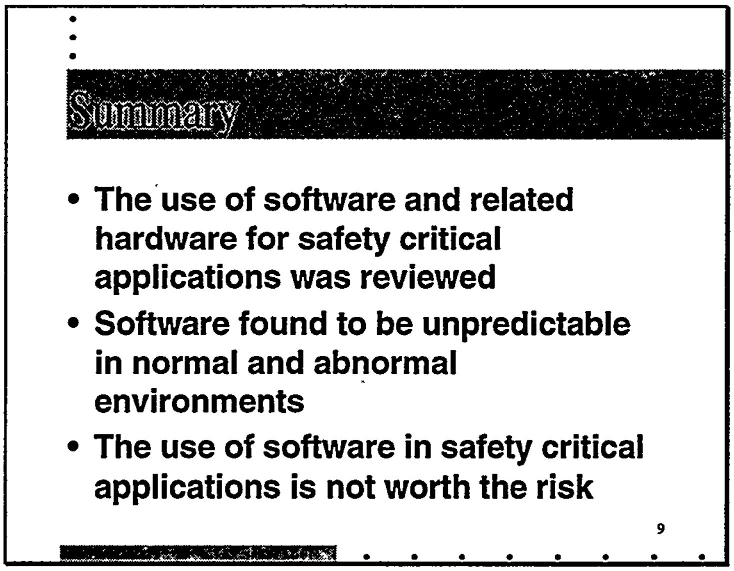


Safety Critical Subsystem Features

- **Inherently safe**
- **Passive rather than active**
- **Extremely robust**
- **Analyzable and testable to required levels**
- **Predictable in normal and abnormal environments**

8

Slide 9

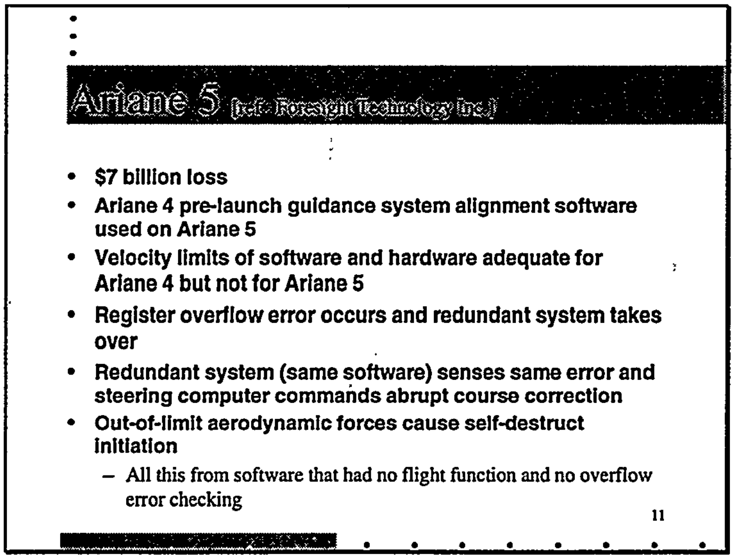


Summary

- The use of software and related hardware for safety critical applications was reviewed
- Software found to be unpredictable in normal and abnormal environments
- The use of software in safety critical applications is not worth the risk

9

Slide 10

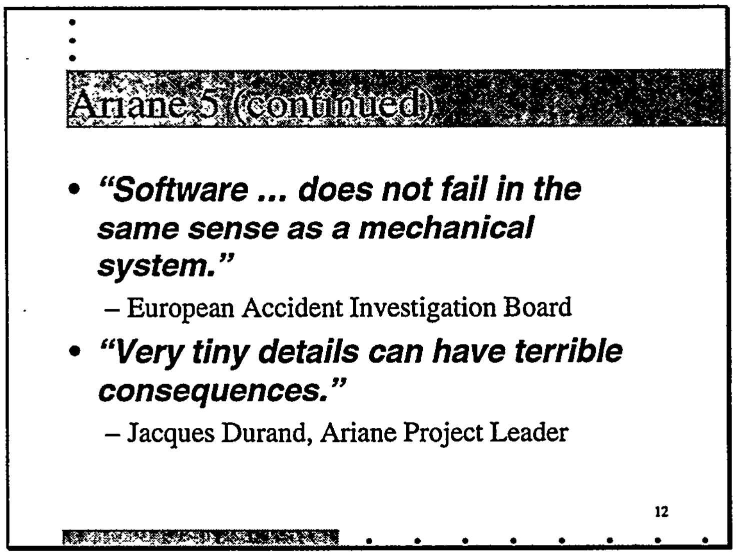


Ariane 5 [ref: Foresight Technology Inc.]

- $7 billion loss
- Ariane 4 pre-launch guidance system alignment software used on Ariane 5
- Velocity limits of software and hardware adequate for Ariane 4 but not for Ariane 5
- Register overflow error occurs and redundant system takes over
- Redundant system (same software) senses same error and steering computer commands abrupt course correction
- Out-of-limit aerodynamic forces cause self-destruct initiation
  - – All this from software that had no flight function and no overflow error checking

11

Slide 11



Ariane 5 (continued)

- ***"Software ... does not fail in the same sense as a mechanical system."***
  - European Accident Investigation Board
- ***"Very tiny details can have terrible consequences."***
  - Jacques Durand, Ariane Project Leader

12

Incidents History and Lessons Learned

Tuesday, July 29, 1998
1:00 p.m. – 5:00 p.m.

Intentionally left blank

The Role of Data Systems

Christopher A. Hart
Federal Aviation Administration
Washington, DC

Intentionally left blank

Investigation of the High Consequence Incident: Techniques and Lessons

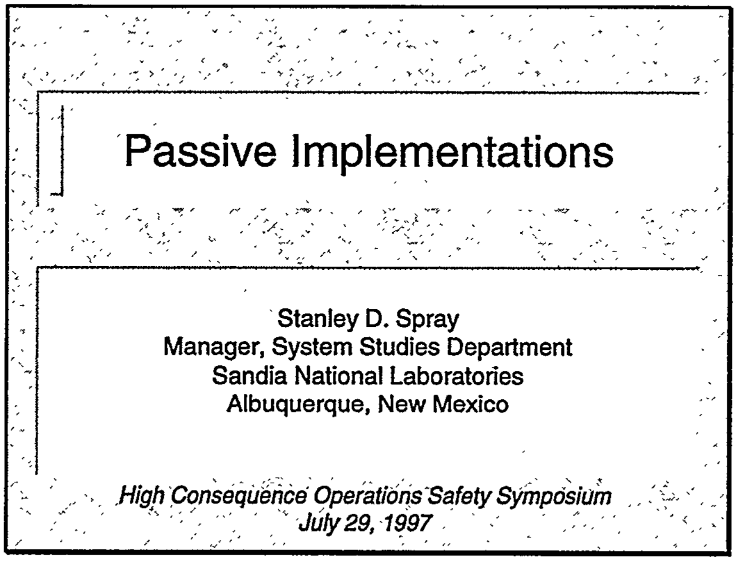
Roger L. McCarthy
Failure Analysis, Incorporated
Menlo Park, California

Intentionally left blank

Passive Implementations

Stanley D. Spray
Sandia National Laboratories*
Albuquerque, New Mexico

Slide 1

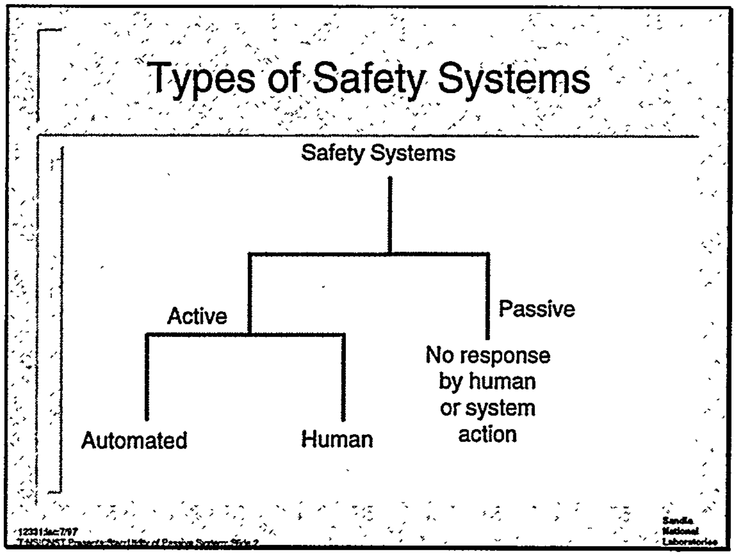


Passive Implementations

Stanley D. Spray
Manager, System Studies Department
Sandia National Laboratories
Albuquerque, New Mexico

High Consequence Operations Safety Symposium
July 29, 1997

Slide 2

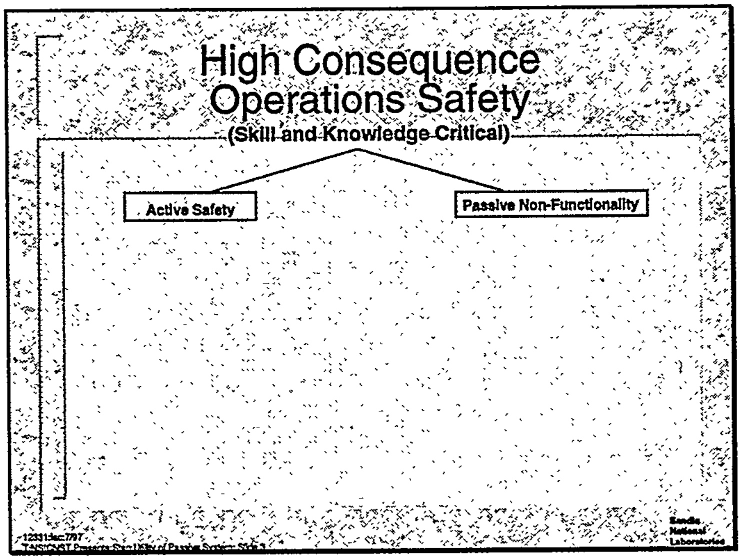


Types of Safety Systems

Safety Systems
Active
Passive
Automated
Human
No response by human or system action
12331/sac 7/97
T:NS/CNST Presents/Start Utility of Passive System: Slide 2
Sandia National Laboratories

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

Slide 3



High Consequence Operations Safety

(Skill and Knowledge Critical)

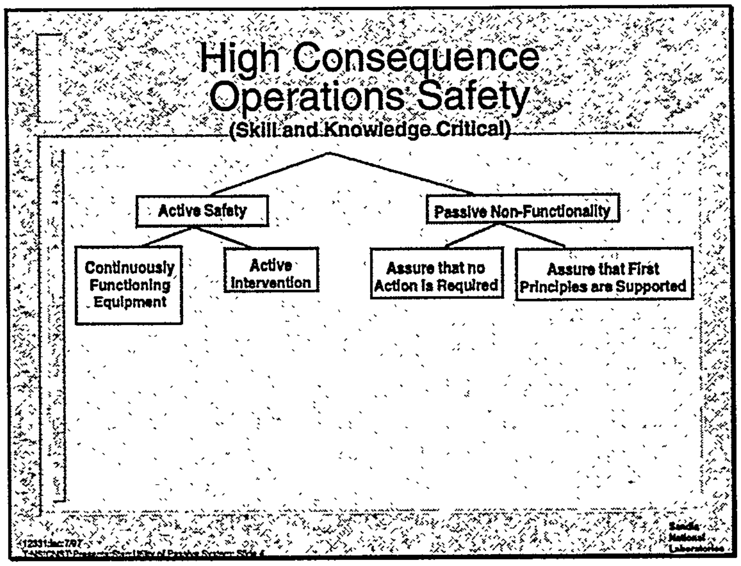
- Active Safety
- Passive Non-Functionality

12331:lac 7/97

[illegible] Utility of Passive Systems Slide 3

Sandia National Laboratories

Slide 4



High Consequence Operations Safety

(Skill and Knowledge Critical)

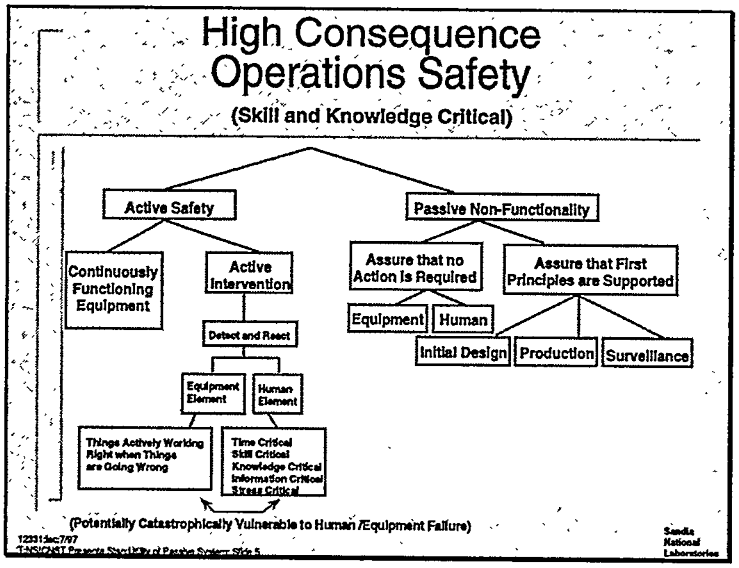
- Active Safety
  - Continuously Functioning Equipment
  - Active Intervention
- Passive Non-Functionality
  - Assure that no Action is Required
  - Assure that First Principles are Supported

12331:lac 7/97

[illegible] Utility of Passive Systems Slide 4

Sandia National Laboratories

Slide 5



High Consequence Operations Safety

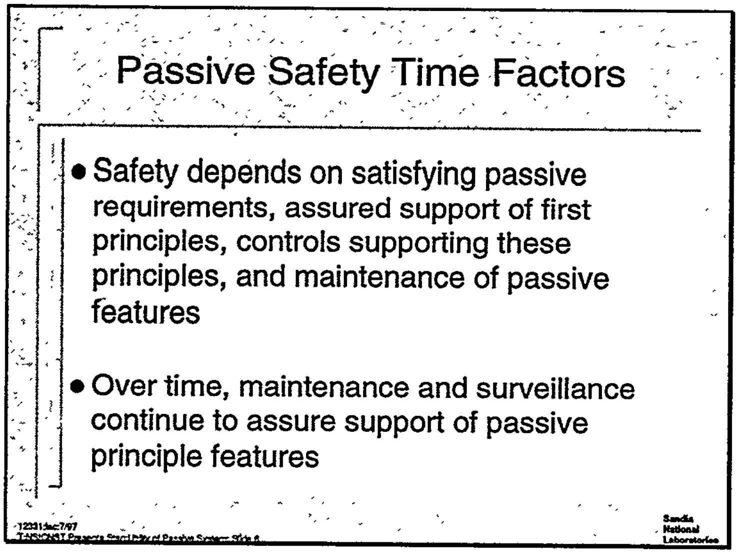
(Skill and Knowledge Critical)

(Potentially Catastrophically Vulnerable to Human /Equipment Failure)

12331:lac:7/97
T:NSICNST Projects Star\Utility of Passive System Slide 5

Sandia National Laboratories

Slide 6



Passive Safety Time Factors

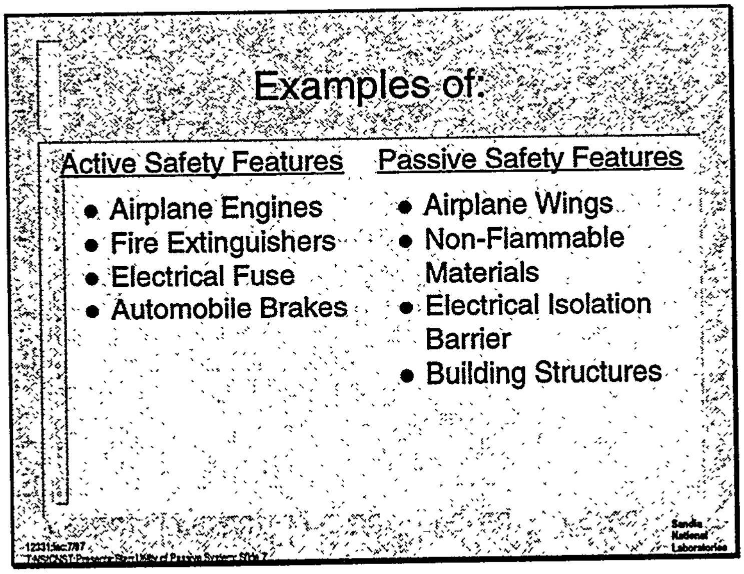
- Safety depends on satisfying passive requirements, assured support of first principles, controls supporting these principles, and maintenance of passive features

- Over time, maintenance and surveillance continue to assure support of passive principle features

12331:lac:7/97
T:NSICNST Projects Star\Utility of Passive System Slide 6

Sandia National Laboratories

Slide 7



Examples of:

Active Safety Features

- Airplane Engines
- Fire Extinguishers
- Electrical Fuse
- Automobile Brakes

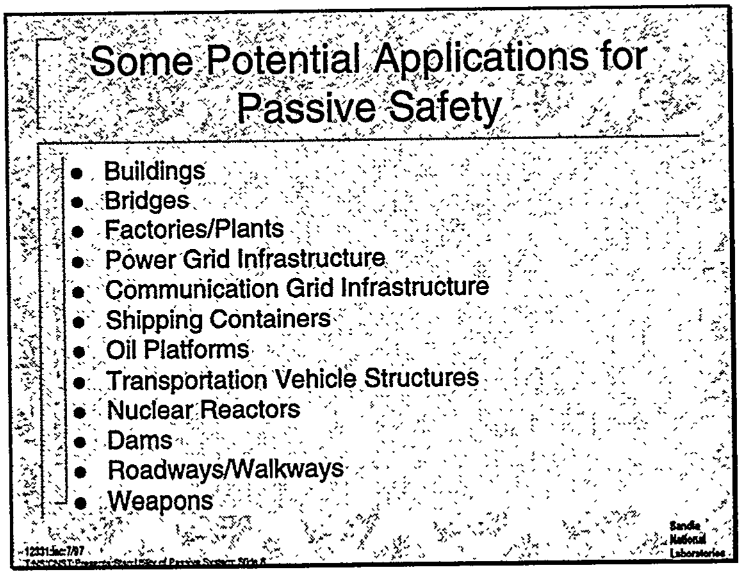
Passive Safety Features

- Airplane Wings
- Non-Flammable Materials
- Electrical Isolation Barrier
- Building Structures

12331:lac:7/97
TAS/CNST-Presents-Start Utility of Passive Systems Slide 7

Sandia National Laboratories

Slide 8



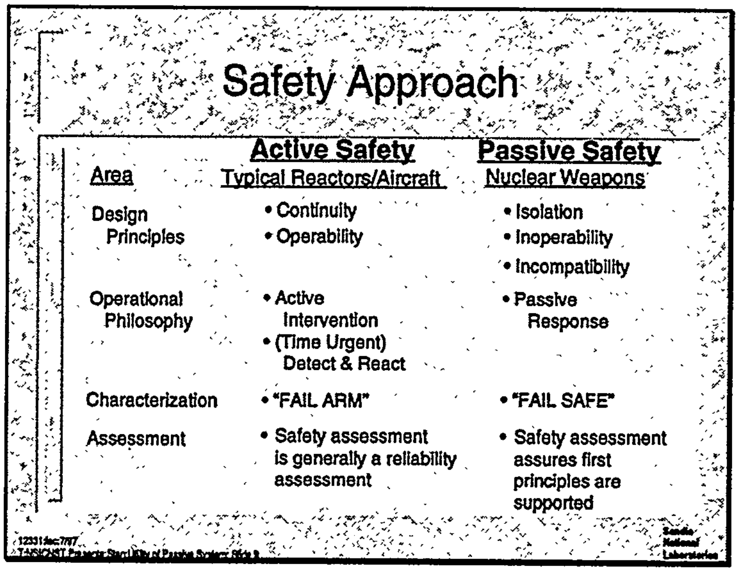
Some Potential Applications for Passive Safety

- Buildings
- Bridges
- Factories/Plants
- Power Grid Infrastructure
- Communication Grid Infrastructure
- Shipping Containers
- Oil Platforms
- Transportation Vehicle Structures
- Nuclear Reactors
- Dams
- Roadways/Walkways
- Weapons

12331:lac:7/97
TAS/CNST-Presents-Start Utility of Passive Systems Slide 8

Sandia National Laboratories

Slide 9

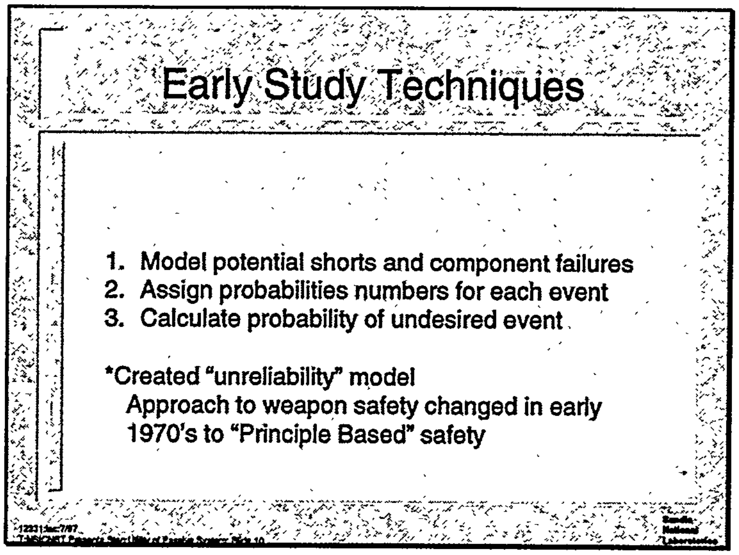


Safety Approach

Area	Active Safety Typical Reactors/Aircraft	Passive Safety Nuclear Weapons
Design Principles	• Continuity • Operability	• Isolation • Inoperability • Incompatibility
Operational Philosophy	• Active Intervention • (Time Urgent) Detect & React	• Passive Response
Characterization	• "FAIL ARM"	• "FAIL SAFE"
Assessment	• Safety assessment is generally a reliability assessment	• Safety assessment assures first principles are supported

Sandia National Laboratories

Slide 10



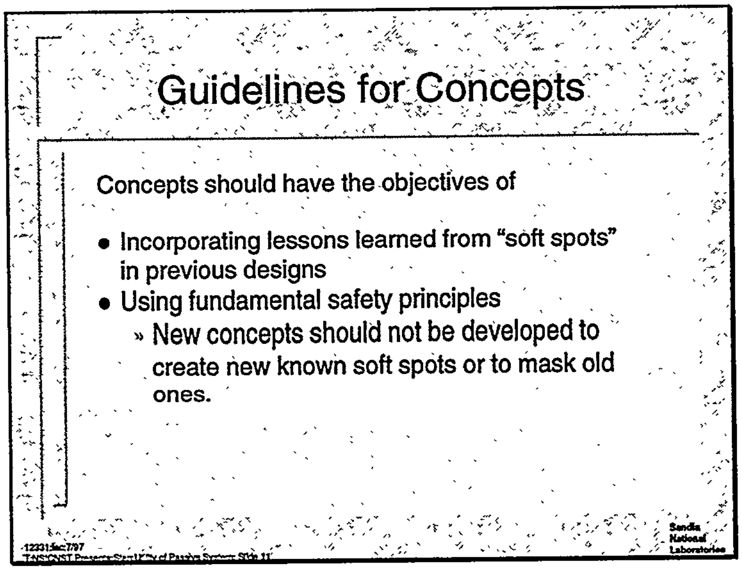
Early Study Techniques

1. Model potential shorts and component failures
2. Assign probabilities numbers for each event
3. Calculate probability of undesired event.

*Created "unreliability" model
Approach to weapon safety changed in early 1970's to "Principle Based" safety

Sandia National Laboratories

Slide 11



Guidelines for Concepts

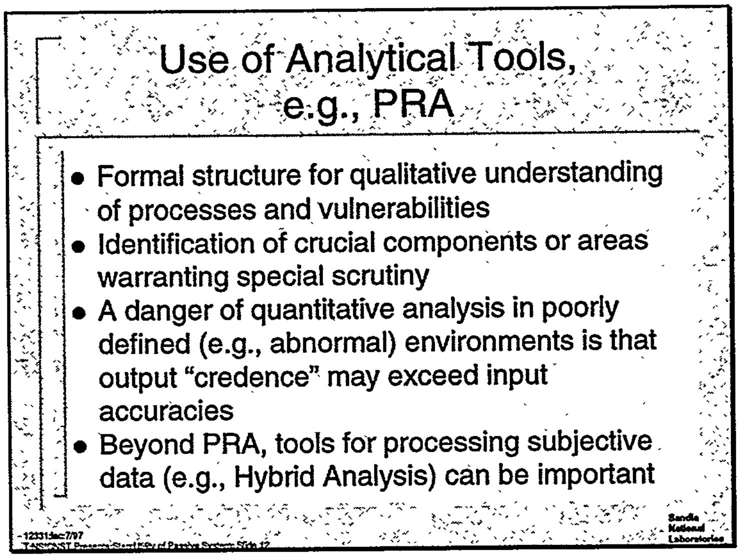
Concepts should have the objectives of

- Incorporating lessons learned from “soft spots” in previous designs
- Using fundamental safety principles
  - » New concepts should not be developed to create new known soft spots or to mask old ones.

-12331:lac:7/97
TNS/CNST Presents-[illegible] of Passive Systems Slide 11

Sandia National Laboratories

Slide 12



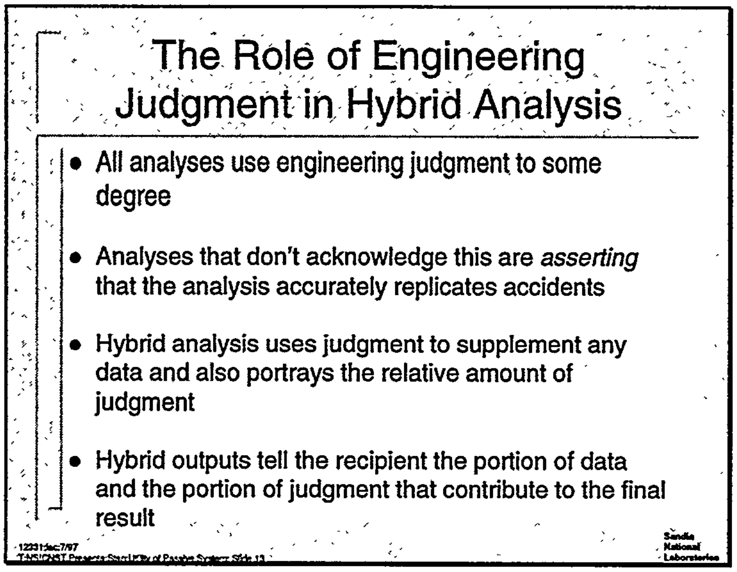
Use of Analytical Tools, e.g., PRA

- Formal structure for qualitative understanding of processes and vulnerabilities
- Identification of crucial components or areas warranting special scrutiny
- A danger of quantitative analysis in poorly defined (e.g., abnormal) environments is that output “credence” may exceed input accuracies
- Beyond PRA, tools for processing subjective data (e.g., Hybrid Analysis) can be important

-12331:lac:7/97
TNS/CNST Presents-[illegible] of Passive Systems Slide 12

Sandia National Laboratories

Slide 13



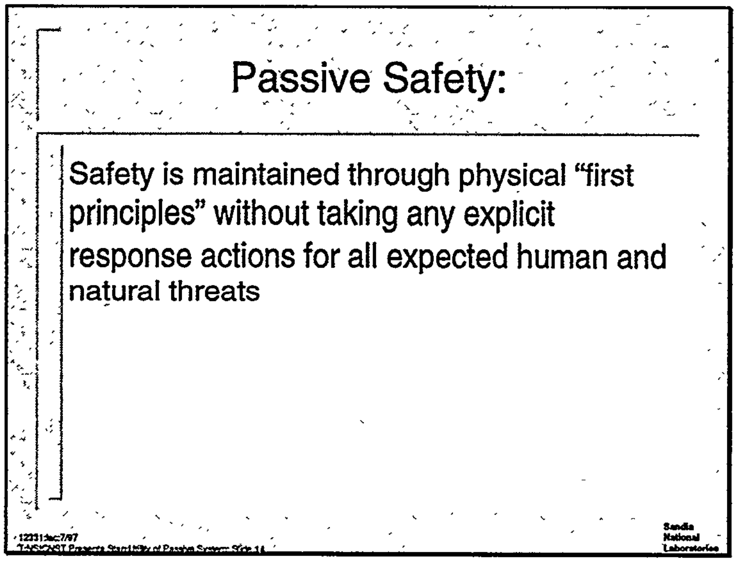
The Role of Engineering Judgment in Hybrid Analysis

- All analyses use engineering judgment to some degree
- Analyses that don't acknowledge this are *asserting* that the analysis accurately replicates accidents
- Hybrid analysis uses judgment to supplement any data and also portrays the relative amount of judgment
- Hybrid outputs tell the recipient the portion of data and the portion of judgment that contribute to the final result

12331:lac:7/97
TAS/CNST Presents Standability of Passive Systems Slide 13

Sandia National Laboratories

Slide 14



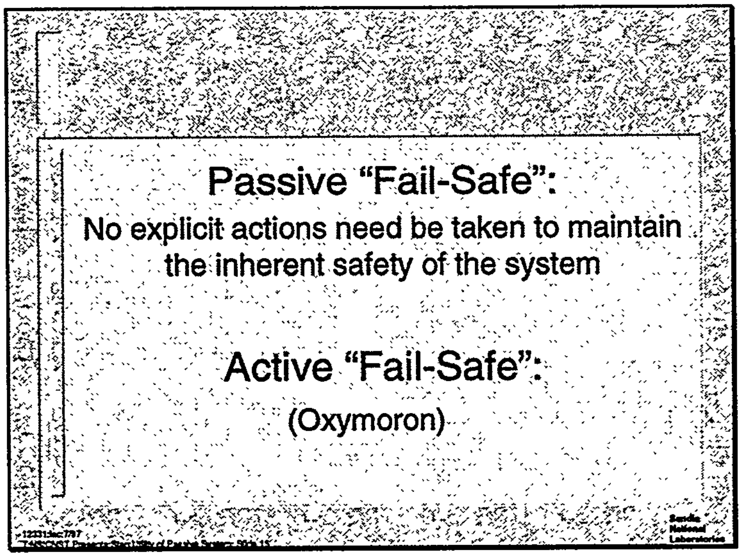
Passive Safety:

Safety is maintained through physical "first principles" without taking any explicit response actions for all expected human and natural threats

12331:lac:7/97
TAS/CNST Presents Standability of Passive Systems Slide 14

Sandia National Laboratories

Slide 15



Passive "Fail-Safe":

No explicit actions need be taken to maintain the inherent safety of the system

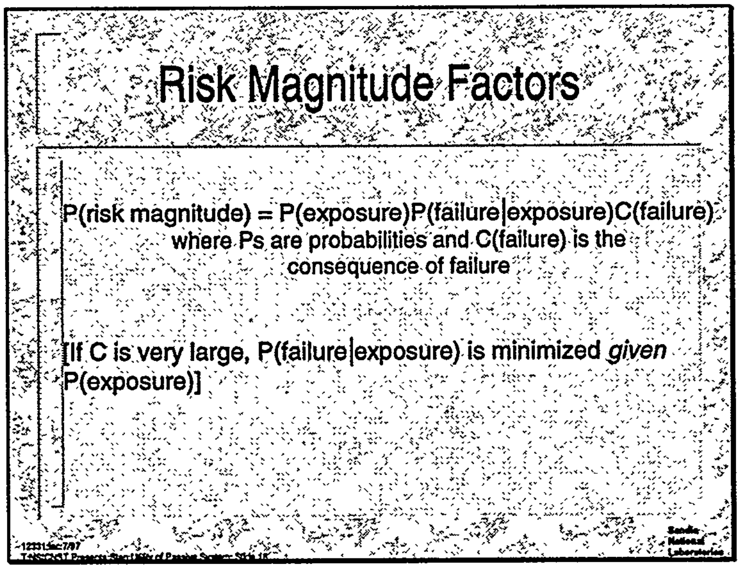
Active "Fail-Safe":

(Oxymoron)

12331sac7/97
T:\NSCHST Presents Start Utility of Passive Systems Slide 15

Sandia National Laboratories

Slide 16



Risk Magnitude Factors

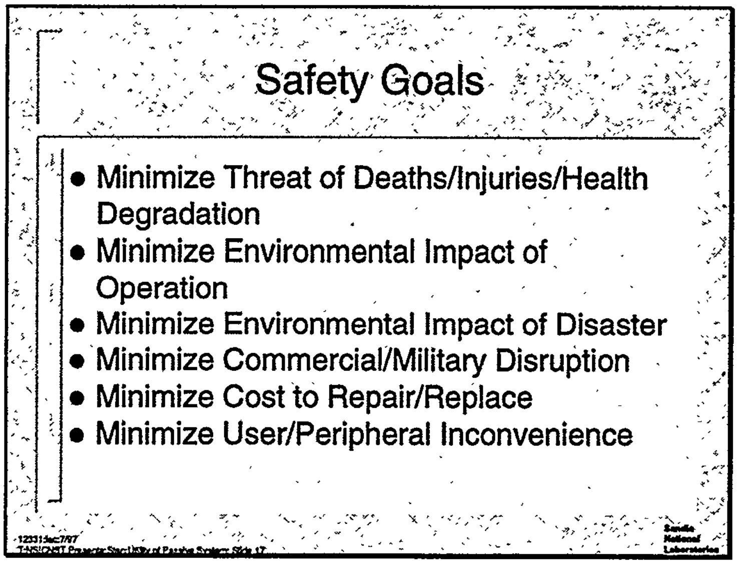
P(risk magnitude) = P(exposure)P(failure|exposure)C(failure) where Ps are probabilities and C(failure) is the consequence of failure

[If C is very large, P(failure|exposure) is minimized *given* P(exposure)]

12331sac7/97
T:\NSCHST Presents Start Utility of Passive Systems Slide 16

Sandia National Laboratories

Slide 17



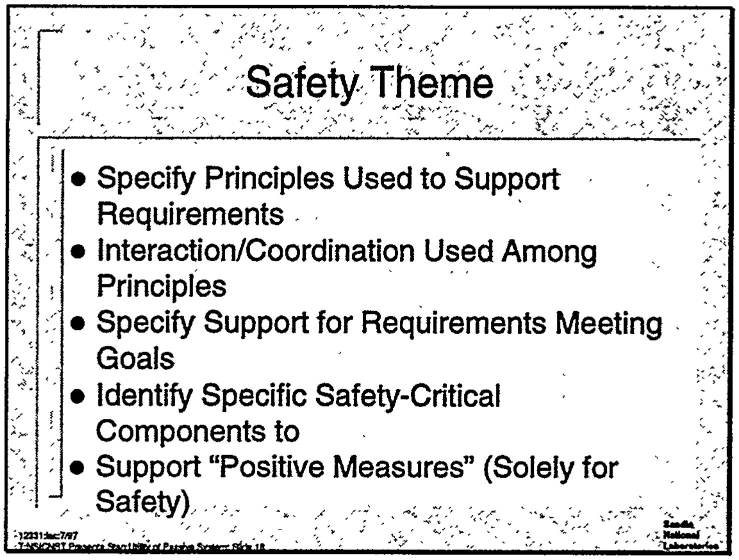
Safety Goals

- Minimize Threat of Deaths/Injuries/Health Degradation
- Minimize Environmental Impact of Operation
- Minimize Environmental Impact of Disaster
- Minimize Commercial/Military Disruption
- Minimize Cost to Repair/Replace
- Minimize User/Peripheral Inconvenience

12331:lsc:7/97
T-NS/CNST Projects: Stat Utility of Passive Systems: Slide 17

Sandia National Laboratories

Slide 18



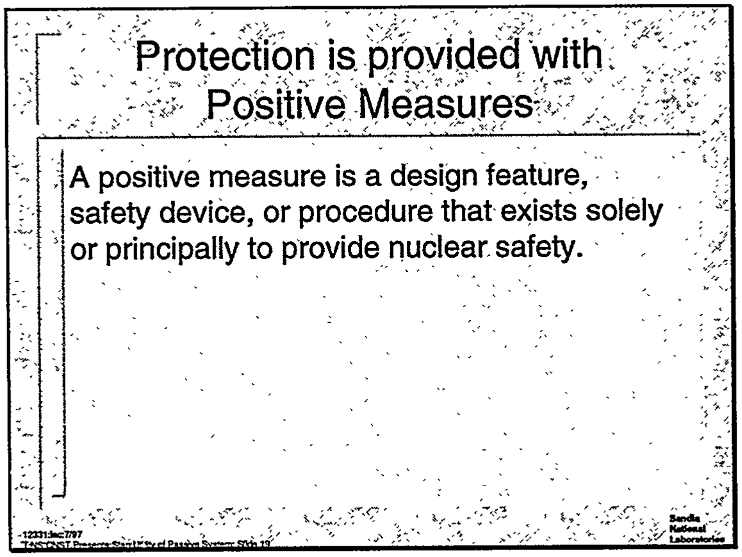
Safety Theme

- Specify Principles Used to Support Requirements
- Interaction/Coordination Used Among Principles
- Specify Support for Requirements Meeting Goals
- Identify Specific Safety-Critical Components to
- Support "Positive Measures" (Solely for Safety)

12331:lsc:7/97
T-NS/CNST Projects: Stat Utility of Passive Systems: Slide 18

Sandia National Laboratories

Slide 19



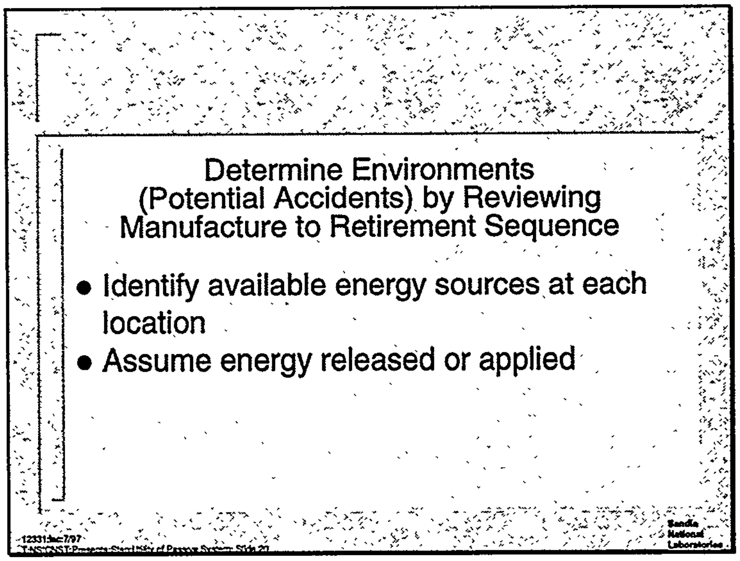
Protection is provided with Positive Measures

A positive measure is a design feature, safety device, or procedure that exists solely or principally to provide nuclear safety.

12331:lac:7/97
T-NS/CNST Presents [illegible] of Passive Systems Slide 19

Sandia National Laboratories

Slide 20



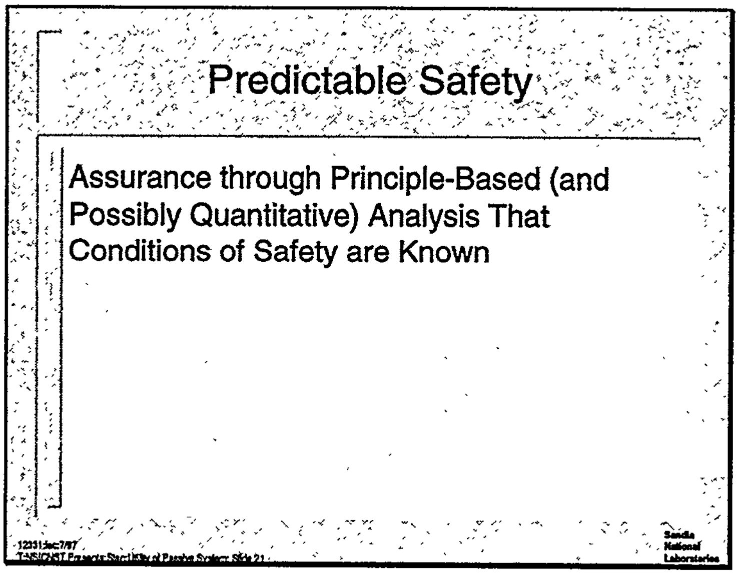
Determine Environments
(Potential Accidents) by Reviewing
Manufacture to Retirement Sequence

- Identify available energy sources at each location
- Assume energy released or applied

12331:lac:7/97
T-NS/CNST Presents [illegible] of Passive Systems Slide 20

Sandia National Laboratories

Slide 21



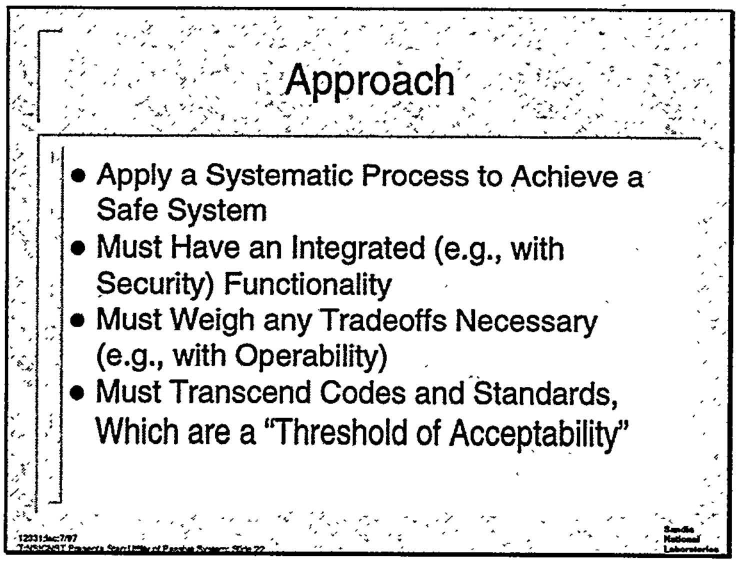
Predictable Safety

Assurance through Principle-Based (and Possibly Quantitative) Analysis That Conditions of Safety are Known

12331:lac:7/97
T-NS/CNST Presents Start Utility of Passive Systems Slide 21

Sandia
National
Laboratories

Slide 22



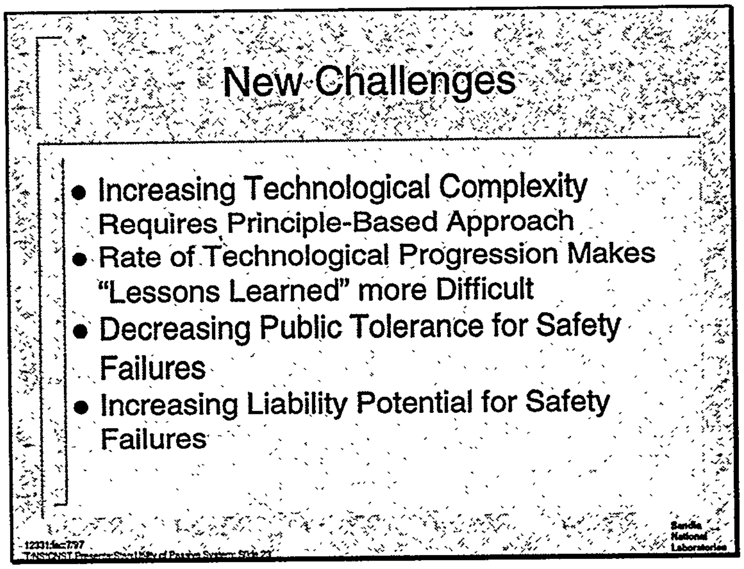
Approach

- Apply a Systematic Process to Achieve a Safe System
- Must Have an Integrated (e.g., with Security) Functionality
- Must Weigh any Tradeoffs Necessary (e.g., with Operability)
- Must Transcend Codes and Standards, Which are a "Threshold of Acceptability"

12331:lac:7/97
T-NS/CNST Presents Start Utility of Passive Systems Slide 22

Sandia
National
Laboratories

Slide 23



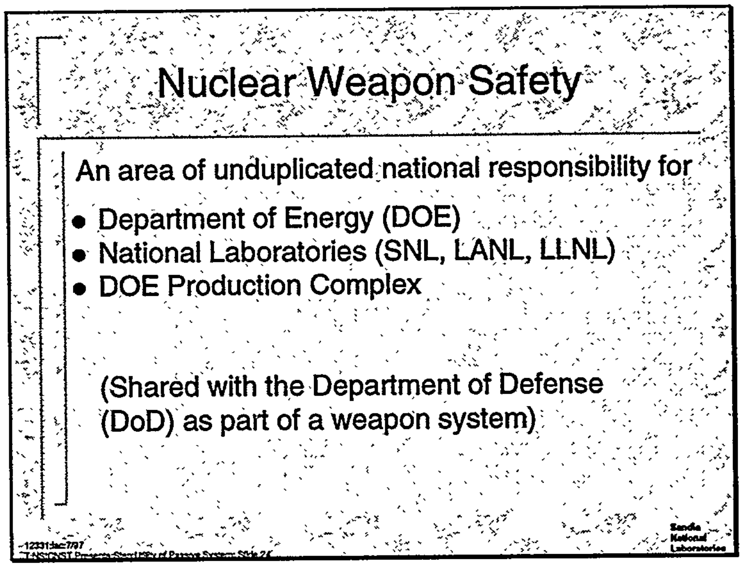
New Challenges

- Increasing Technological Complexity Requires Principle-Based Approach
- Rate of Technological Progression Makes "Lessons Learned" more Difficult
- Decreasing Public Tolerance for Safety Failures
- Increasing Liability Potential for Safety Failures

12331:lac:7/97
TNS/CNST Presents: Stan Ulity of Passive Systems Slide 23

Sandia National Laboratories

Slide 24



Nuclear Weapon Safety

An area of unduplicated national responsibility for

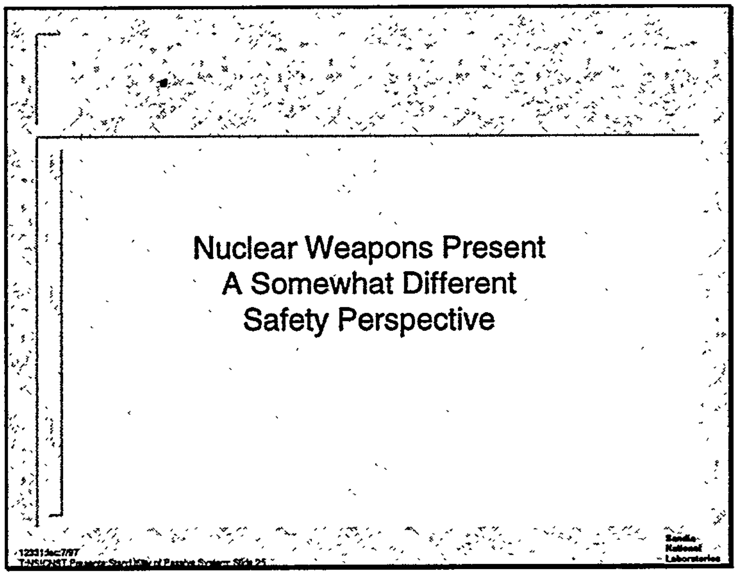
- Department of Energy (DOE)
- National Laboratories (SNL, LANL, LLNL)
- DOE Production Complex

(Shared with the Department of Defense (DoD) as part of a weapon system)

12331:lac:7/97
TNS/CNST Presents: Stan Ulity of Passive Systems Slide 24

Sandia National Laboratories

Slide 25

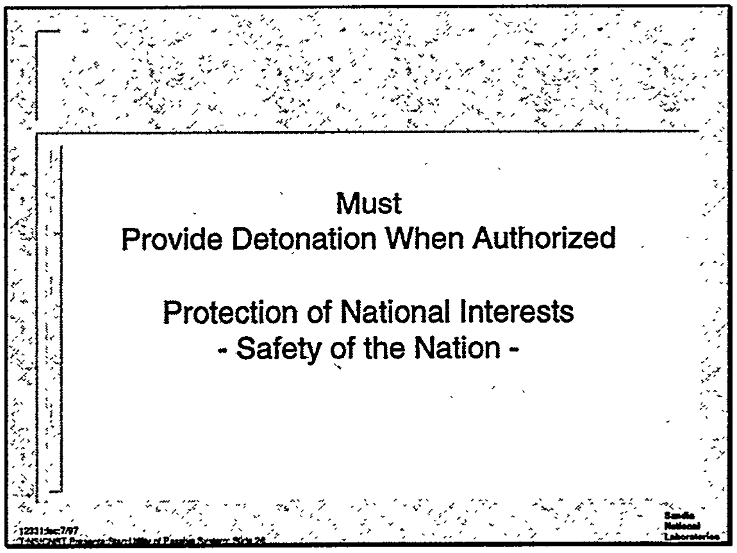


Nuclear Weapons Present
A Somewhat Different
Safety Perspective

12331:dec:7/97
[illegible] Slide 25

Sandia
National
Laboratories

Slide 26



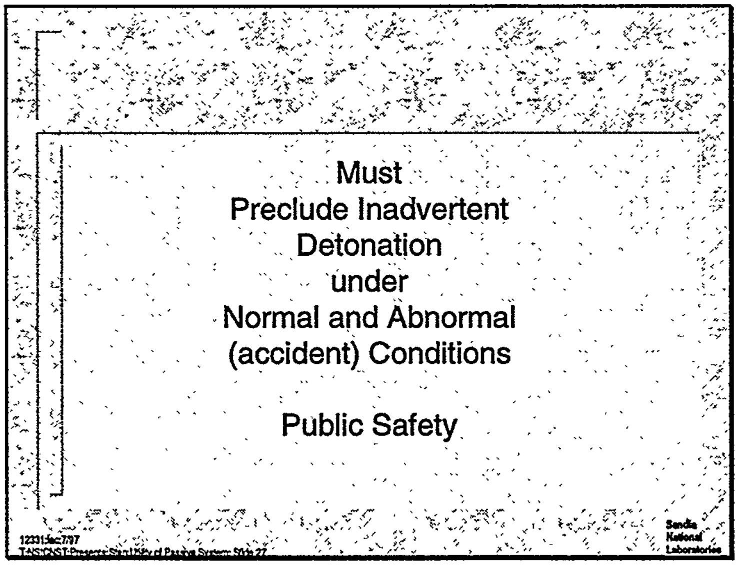
Must
Provide Detonation When Authorized

Protection of National Interests
- Safety of the Nation -

12331:dec:7/97
[illegible] Slide 26

Sandia
National
Laboratories

Slide 27



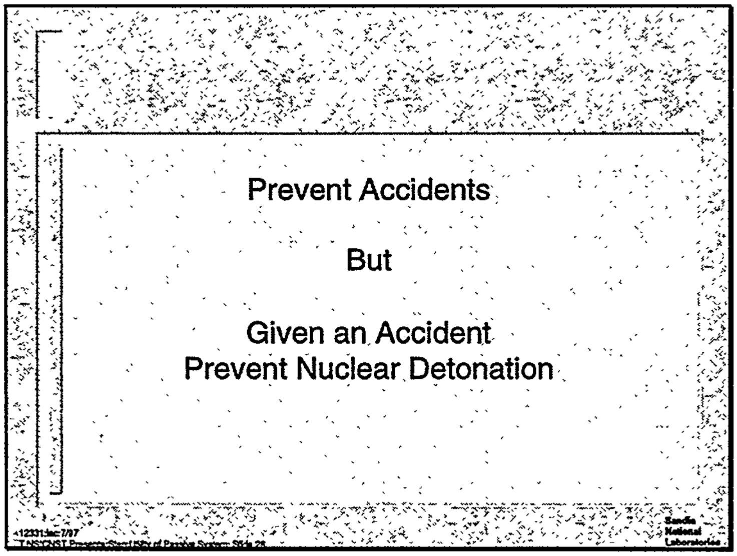
Must
Preclude Inadvertent
Detonation
under
Normal and Abnormal
(accident) Conditions

Public Safety

12331:lac:7/97
T:NS/CNST Presents/Stan/Utility of Passive System: Slide 27

Sandia
National
Laboratories

Slide 28



Prevent Accidents

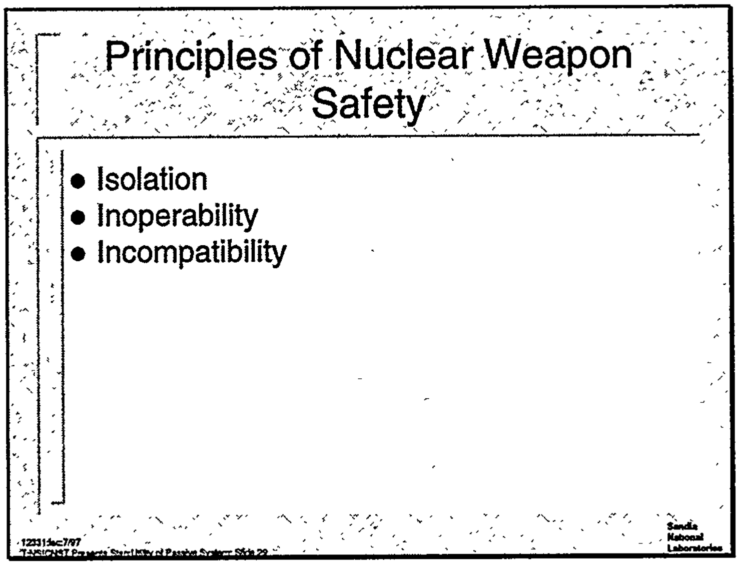
But

Given an Accident
Prevent Nuclear Detonation

12331:lac:7/97
T:NS/CNST Presents/Stan/Utility of Passive System: Slide 28

Sandia
National
Laboratories

Slide 29



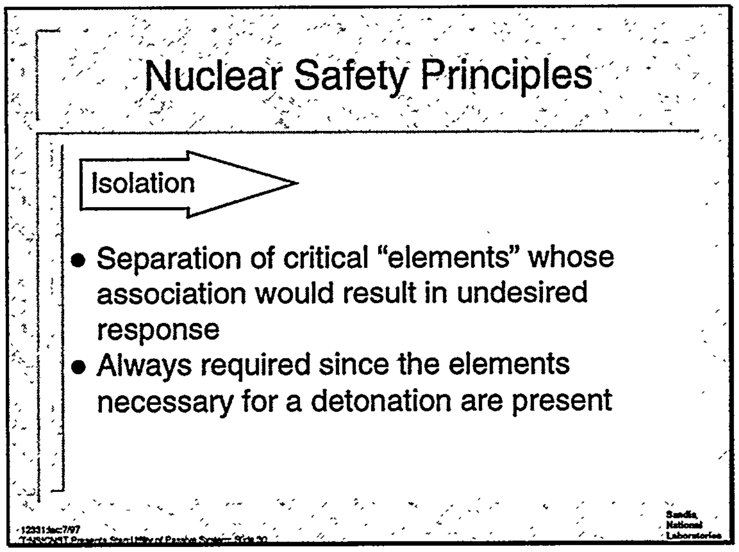
Principles of Nuclear Weapon Safety

- Isolation
- Inoperability
- Incompatibility

12331dec7/97
T-NSIC/NST Presents Start Utility of Passive Systems Slide 29

Sandia National Laboratories

Slide 30



Nuclear Safety Principles

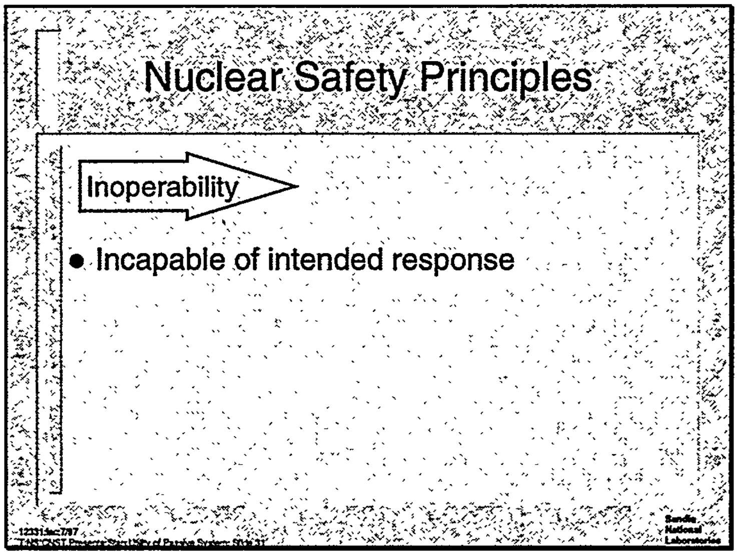
Isolation

- Separation of critical "elements" whose association would result in undesired response
- Always required since the elements necessary for a detonation are present

12331dec7/97
T-NSIC/NST Presents Start Utility of Passive Systems Slide 30

Sandia National Laboratories

Slide 31



Nuclear Safety Principles

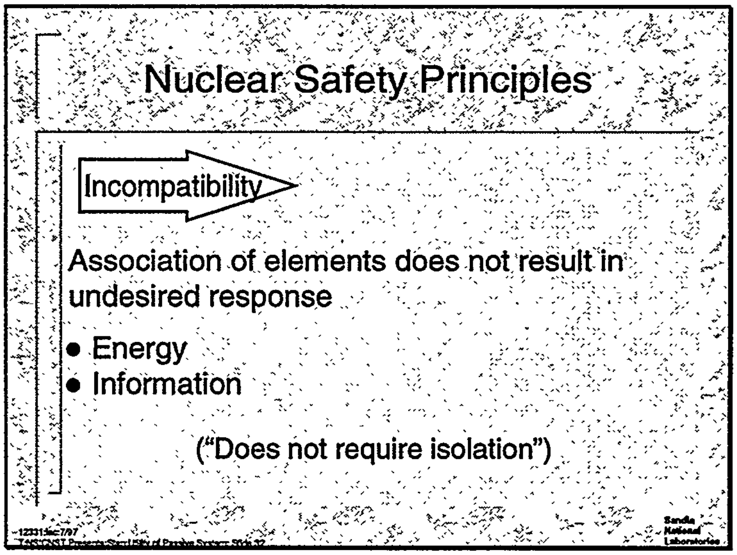
Inoperability

- Incapable of intended response

12331lac7/97
TNS:CNST Presents: [illegible] of Passive Systems: Slide 31

Sandia National Laboratories

Slide 32



Nuclear Safety Principles

Incompatibility

Association of elements does not result in undesired response

- Energy
- Information

("Does not require isolation")

12331lac7/97
TNS:CNST Presents: [illegible] of Passive Systems: Slide 32

Sandia National Laboratories

Slide 33

Basic Design Approach

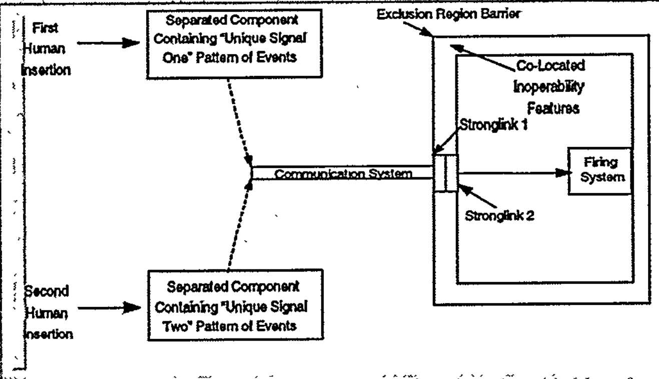
- Physics package is inoperable without an additional element vital to the nuclear detonation process
- Weapon system is designed to Preclude / Provide the element

12331:lac:7/97
[illegible] Presents [illegible] Utility of Passive Systems Slide 33

Sandia National Laboratories

Slide 34

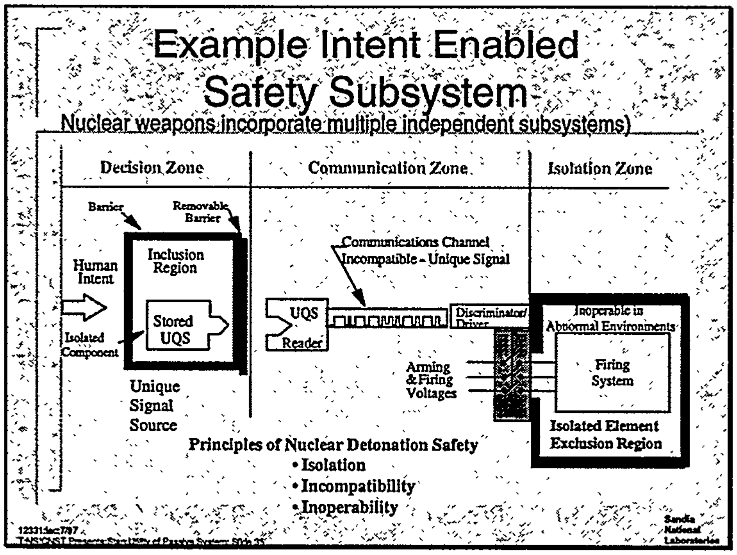
Example Double Intent Safety Subsystems


First Human Insertion
Separated Component Containing "Unique Signal One" Pattern of Events
Exclusion Region Barrier
Co-Located Inoperability Features
Stronglink 1
Communication System
Firing System
Stronglink 2
Second Human Insertion
Separated Component Containing "Unique Signal Two" Pattern of Events

12331:lac:7/97
[illegible] Presents [illegible] Utility of Passive Systems Slide 34

Sandia National Laboratories

Slide 35



Example Intent Enabled Safety Subsystem

Nuclear weapons incorporate multiple independent subsystems)

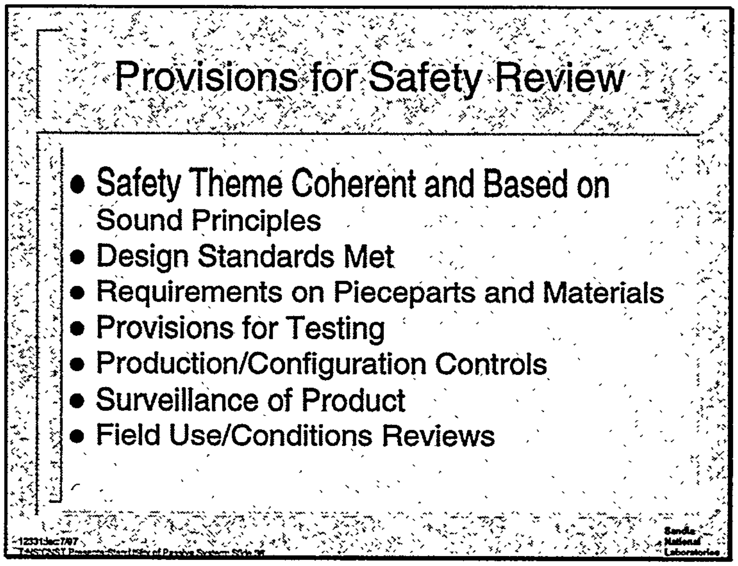
Principles of Nuclear Detonation Safety

- Isolation
- Incompatibility
- Inoperability

12331.lec7/97

Sandia National Laboratories

Slide 36



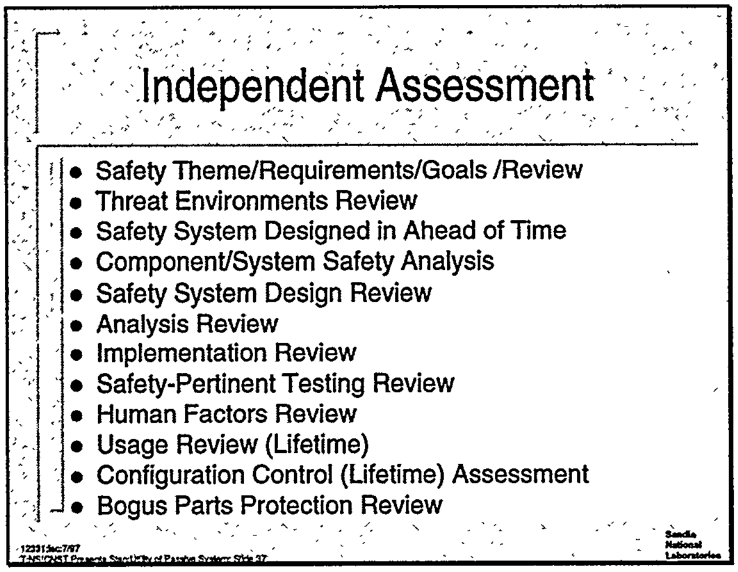
Provisions for Safety Review

- Safety Theme Coherent and Based on Sound Principles
- Design Standards Met
- Requirements on Pieceparts and Materials
- Provisions for Testing
- Production/Configuration Controls
- Surveillance of Product
- Field Use/Conditions Reviews

12331.lec7/97

Sandia National Laboratories

Slide 37



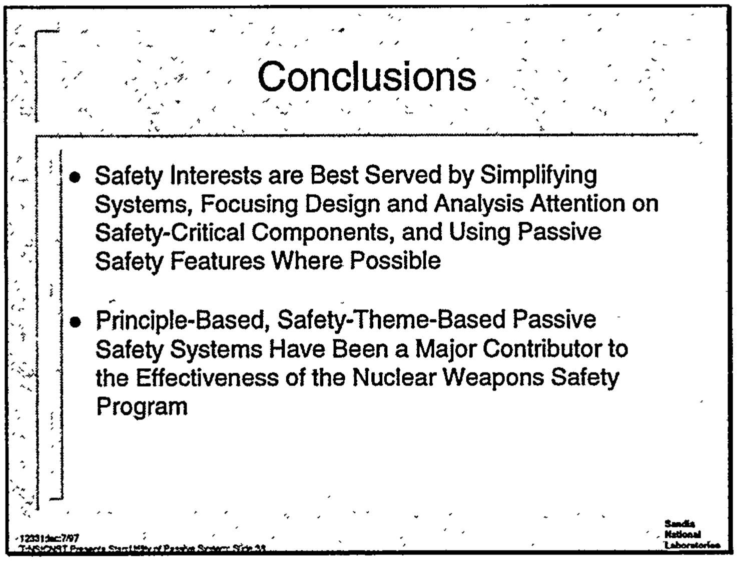
Independent Assessment

- Safety Theme/Requirements/Goals /Review
- Threat Environments Review
- Safety System Designed in Ahead of Time
- Component/System Safety Analysis
- Safety System Design Review
- Analysis Review
- Implementation Review
- Safety-Pertinent Testing Review
- Human Factors Review
- Usage Review (Lifetime)
- Configuration Control (Lifetime) Assessment
- Bogus Parts Protection Review

12331.doc:7/97
T-NS/CNST Presents Stan Utility of Passive Systems Slide 37

Sandia National Laboratories

Slide 38



Conclusions

- Safety Interests are Best Served by Simplifying Systems, Focusing Design and Analysis Attention on Safety-Critical Components, and Using Passive Safety Features Where Possible

- Principle-Based, Safety-Theme-Based Passive Safety Systems Have Been a Major Contributor to the Effectiveness of the Nuclear Weapons Safety Program

12331.doc:7/97
T-NS/CNST Presents Stan Utility of Passive Systems Slide 38

Sandia National Laboratories

Intentionally left blank

Lightning and Ordnance Safety

Malcolm Jones
Atomic Weapons Establishment
Hunting BRAE, United Kingdom

Marvin Morris
Sandia National Laboratories*
Albuquerque, New Mexico

Abstract

Lightning represents one of the most potent "natural environment" threats to ordnance systems, either through direct attachment to electro-explosive circuits or through the generation of other abnormal environments. The initial current pulse in the lightning stroke has a format ideally matched to the requirement for functioning high-voltage initiators.

For these reasons, care has always been exercised in terms of the protection afforded against this environment, and this is particularly so for high-consequence ordnance systems because of the potential for catastrophic consequences in that case.

Lightning-generation phenomenology, its characteristics and protection strategies for the typical life phases of an ordnance system including, assembly/disassembly, in service and post accident phases, are discussed.

Introduction

Lightning represents a potent threat to the safety of ordnance systems because its format (a fast rising [μs], high amplitude [~ 10^5A] pulse) is an ideal inadvertent source for firing ordnance initiators including high-voltage detonators. The latter typically require 10^2 to 10^3A with a similar rise time for function. For this reason, great care has always been taken in the design and protection of ordnance systems and, in particular, high-consequence systems with regard to this threat. This overall protection improves as our knowledge and technology evolves. All UK high-consequence systems (or more correctly 'inert representations' thereof) are tested against lightning strike as part of the safety assessment and certification process for service.

Although lightning phenomenology has been the subject of international study for more than a century, no sensible scientist or engineer will claim that it is fully understood. It can still spring the odd surprise and the phenomena are statistical in nature. Design and

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

protection are based on a combination of analysis, testing, best practice (in the UK this includes British Standards [BS] and UK Ministry of Defence [MOD] requirements such as DEF STANs and so on), expert opinion, and a conservative approach.

There are three generic phases in the ordnance system's life when such safety is assessed. These are:

(1) The factory plant phase
(2) The in-service phase
(3) The potential weapon-accident phase

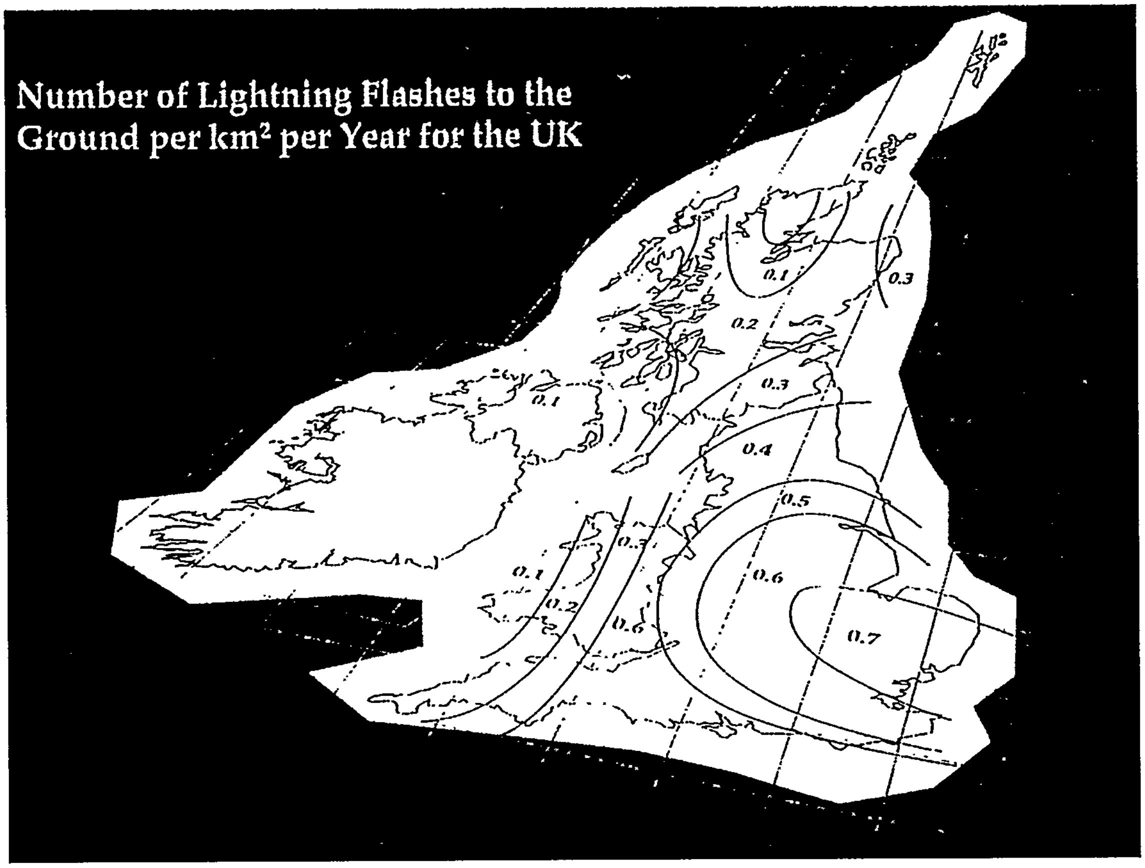
The broad issues involved in each of the phases are discussed in the following sections for high-consequence ordnance.

The Lightning Threat

In the UK, the lightning flash density rate is of the order of a few tenths/km^2/year with a maximum of 0.7 in the southeast of England, as shown in Figure 1, taken from BS 6651. This rate is associated with ~ 10 thunderstorm days per year. Other areas of the world are subject to much higher thunderstorm activity.

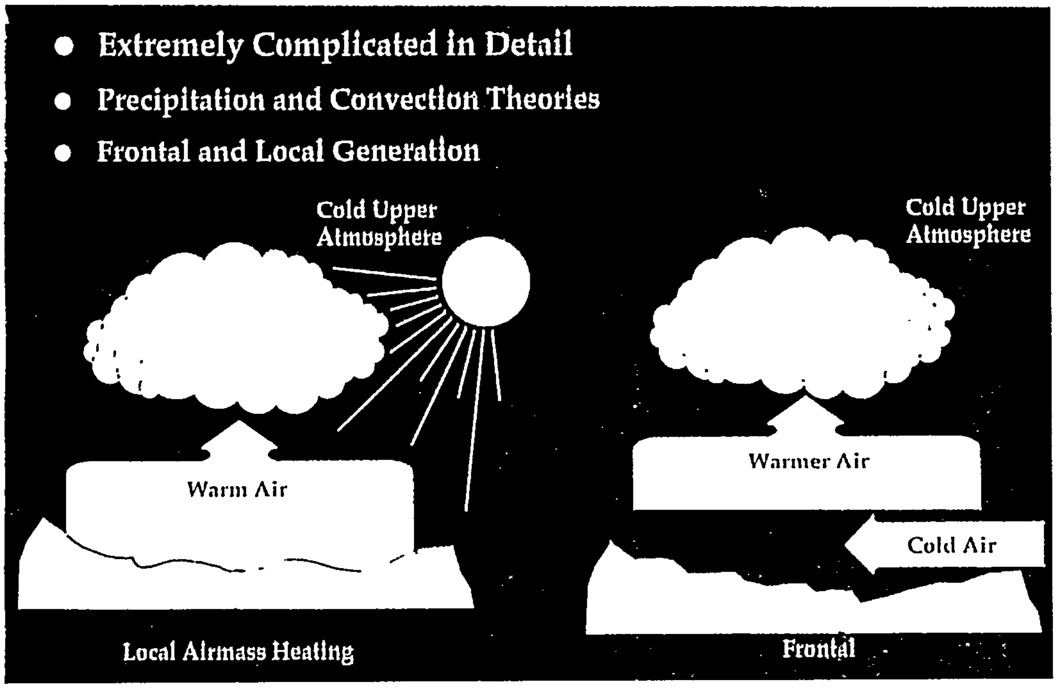
Lightning storms are either generated through local heating or by cold fronts moving into a warm air region. These phenomena are depicted in Figure 2. The typical thunder head cloud is that shown in Figure 3, with the base of the cloud of a predominantly negative nature and which gives rise to negative strokes. The inverse condition is also possible, but is much rarer and can occur at the end of a thunder cell's activity, when the original charge configuration nears depletion and when the flashes are weaker. However, in some instances not associated with an end-of-storm effect, positive strikes are the most severe of all. For this reason, lightning tests are undertaken with both positive and negative polarities. The charging of a thunder head cloud is a complex phenomenon and is not fully understood. Two basic mechanisms have been postulated, convection and precipitation, and these processes are illustrated in Figures. 4 and 5. In fact, the overall activity may well include contributions from both processes.

The lightning flash is initiated as a result of 'step leader' activity, as depicted in Figure 6. Electrons from the base of the cloud move down in a series of steps forming a branching pattern. This process continues until these step leaders meet the upward moving positive streamers from the ground. At this stage, complete conducting channels are formed resulting in the lightning return stroke, whose passage is from ground to cloud. A lightning flash may consist of a number of return strokes with separations of tens of ms between each stroke. Generally, successive strokes will be of declining amplitude and these subsequent strokes are generally initiated by 'dart leaders,' which transit the cloud to ground gap in one step. Of course, it is the stroke (and the stroke series in a flash), with its attendant spectacular electromagnetic and thermodynamic properties, which is the subject of our concern. The above general phenomena also take place between thunderclouds and within thunderclouds, but the strokes are less severe for these cases and have far less relevance to ordnance safety issues.



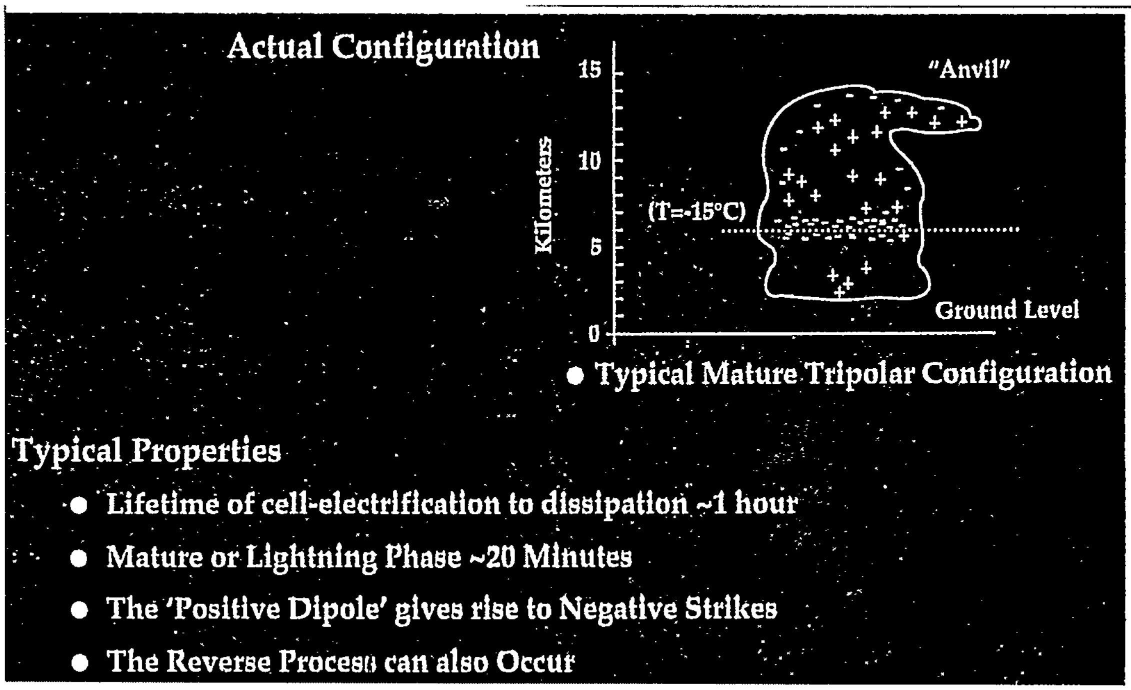
Number of Lightning Flashes to the Ground per km² per Year for the UK

Figure 1. UK flash rate densities.



- Extremely Complicated in Detail
- Precipitation and Convection Theories
- Frontal and Local Generation

Figure 2. Thunderstorm types.



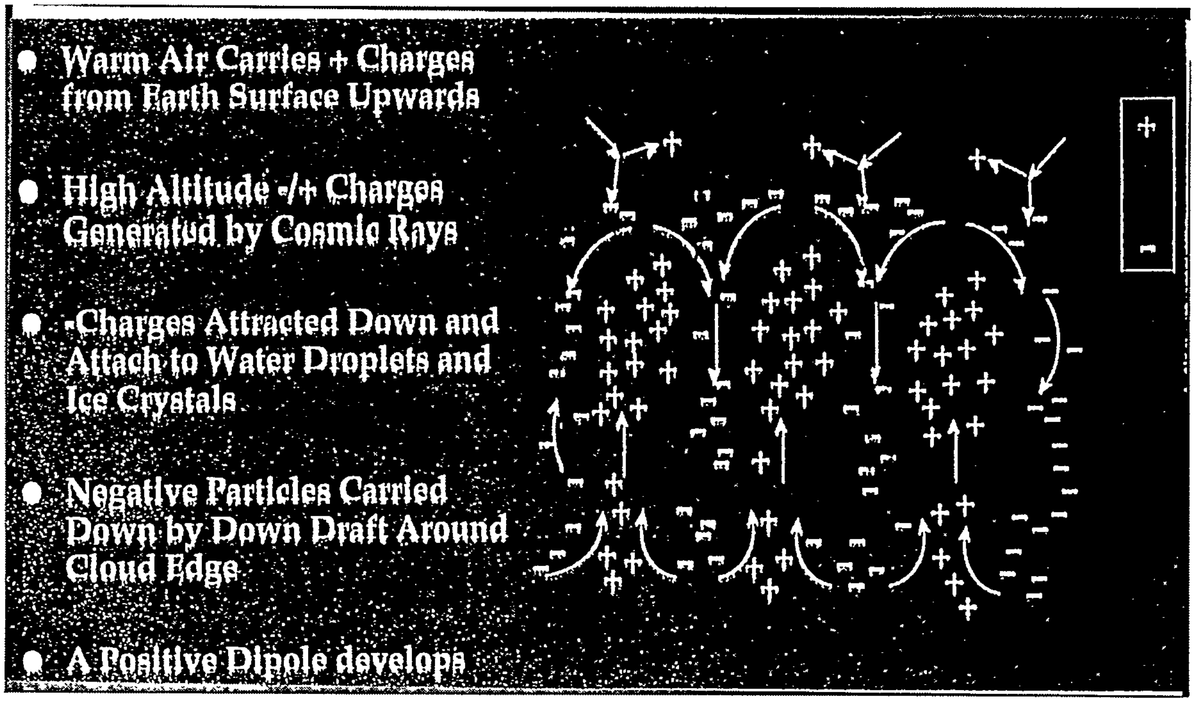
Actual Configuration

- Typical Mature Tripolar Configuration

Typical Properties

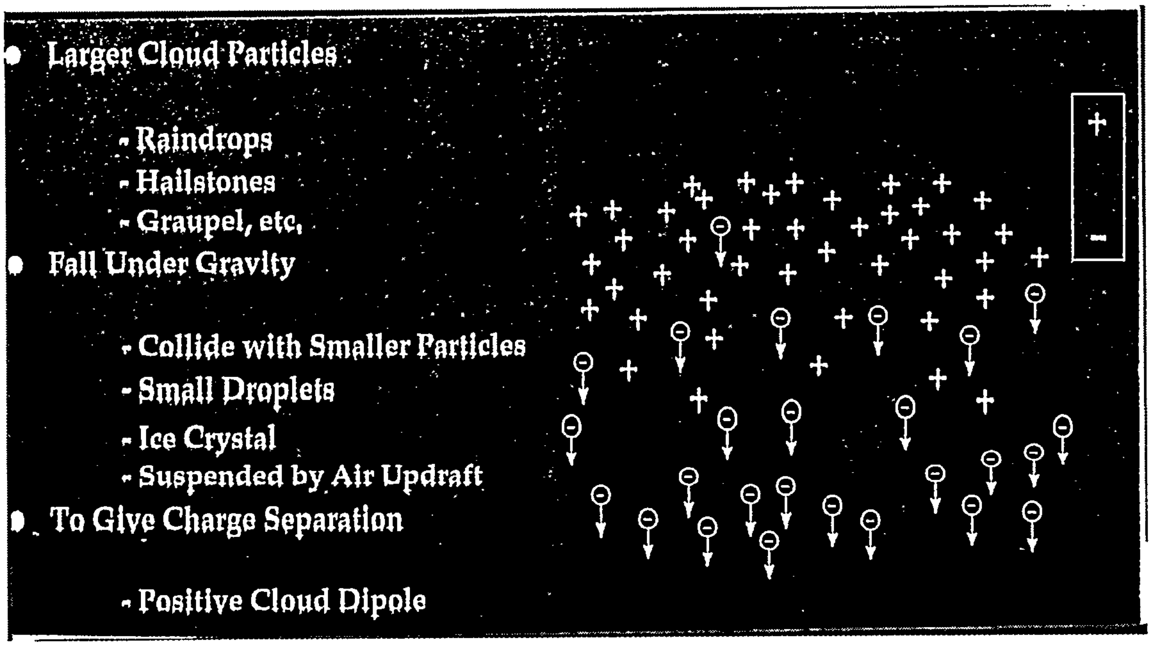
- Lifetime of cell-electrification to dissipation ~1 hour
- Mature or Lightning Phase ~20 Minutes
- The 'Positive Dipole' gives rise to Negative Strikes
- The Reverse Process can also Occur

Figure 3. Thunderhead configuration.



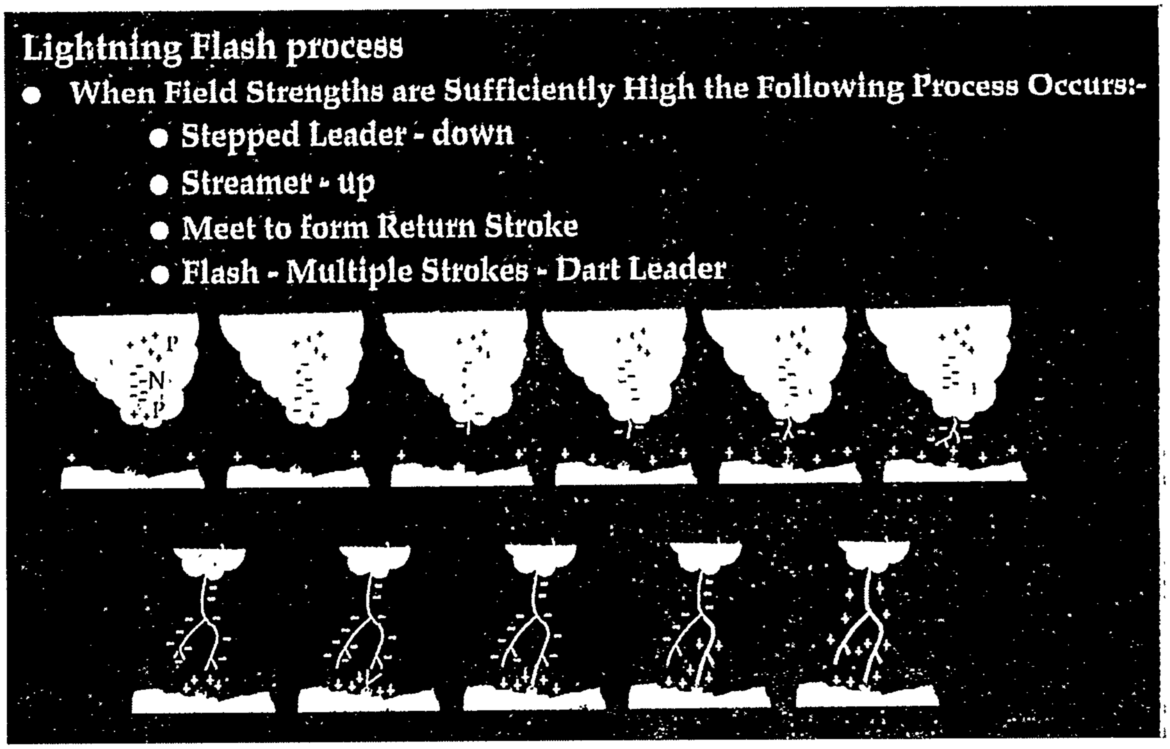
- Warm Air Carries + Charges from Earth Surface Upwards
- High Altitude -/+ Charges Generated by Cosmic Rays
- -Charges Attracted Down and Attach to Water Droplets and Ice Crystals
- Negative Particles Carried Down by Down Draft Around Cloud Edge
- A Positive Dipole develops

Figure 4. Thunderhead generation by convection.



- Larger Cloud Particles
    - Raindrops
    - Hailstones
    - Graupel, etc.
- Fall Under Gravity
    - Collide with Smaller Particles
    - Small Droplets
    - Ice Crystal
    - Suspended by Air Updraft
- To Give Charge Separation
    - Positive Cloud Dipole

Figure 5. Thunderhead generation by precipitation.

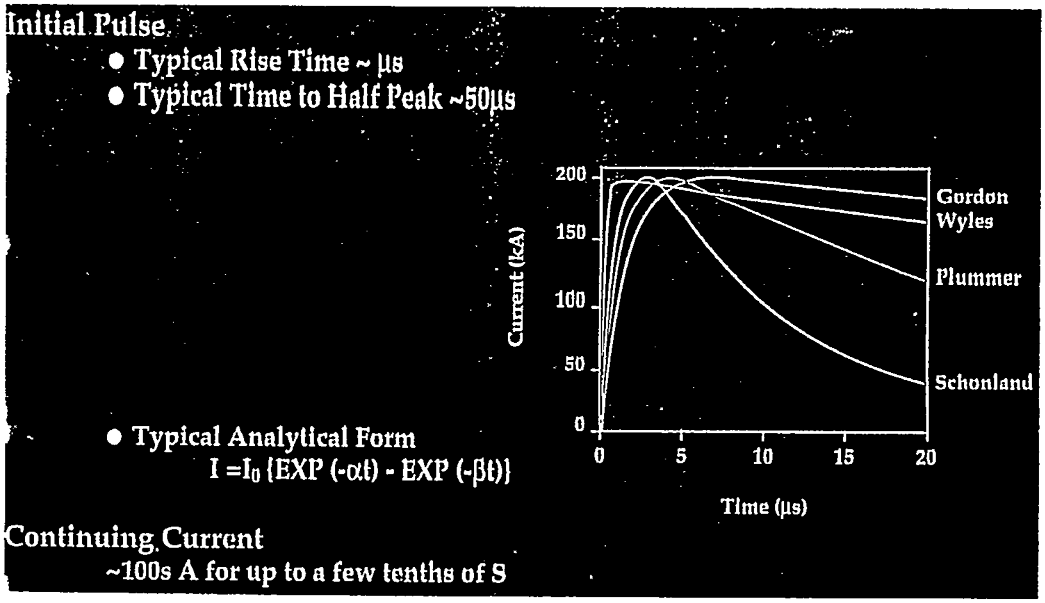


Lightning Flash process

- When Field Strengths are Sufficiently High the Following Process Occurs:-
    - Stepped Leader - down
    - Streamer - up
    - Meet to form Return Stroke
    - Flash - Multiple Strokes - Dart Leader

Figure 6. Sequence leading to a lightning flash.

The lightning stroke usually consists of two component: the initial pulse (always present) and the follow-on current. These are illustrated in Figure 7. The initial pulse has a rise time of μs order with a decay constant of tens of μs. Only 1% of the strokes have an amplitude exceeding 200kA. It is this component which gives rise to the high voltages associated with the lightning strike (including both resistive and inductive components).



Initial Pulse

- Typical Rise Time ~ µs
- Typical Time to Half Peak ~50µs

- Typical Analytical Form

  $I = I_0 \{EXP(-\alpha t) - EXP(-\beta t)\}$

Continuing Current

~100s A for up to a few tenths of S

Figure 7. Typical current stroke profiles.

The follow on current may have an amplitude of up to many hundreds of A, with a few tenths of a second duration. This latter component usually carries the bulk of the charge, and has the potential for burning through materials. The flash can transport 10 Coulombs of charge.

Some typical thunderstorm properties are summarised in Table 1.

Thunderstorm Forecasting

As well as adopting good design, protection and general procedural practices, minimisation of the lightning risk also includes the adoption of special procedures when a thunderstorm is forecast. Generally, the special procedures take the form of suspending activities and keeping ordnance systems under cover for all-up rounds, and adopting additional safeing procedures during assembly/disassembly phases. Additional safeing procedures have been identified, tested and exercised, to cover potential weapon accident phases. All these additional procedures depend on timely forecasting of thunderstorm activity at the location. In the United Kingdom, these forecasts are based on the UK's Meteorological Office reports or through on-site detection devices or both in concert. For example, Service and Explosive Ordnance Disposal (EOD) activities are generally based on Meteorological Office reports and operations in assembly areas (associated with high consequence ordnance) on both Meteorological Office reports, and locally based electromagnetic detectors.

This general subject is currently under review.

Table 1. Typical Thunderstorm Properties

Step leader	Travels at ~ 2 x 10^5 m/s Current Av ~ 100A Current Steps ~ kA Step Length – Strength dependent
Dart leader	Travels at ~ 3 x 10^6 m/s Single transit
Return Stroke	99% below 200 kA Up to 10^{12} A/s Travels at c/3 ~ microsecond Rise Time Raises channel to 30,000K ~ 1MV/m
Flash	Continuing Current 100s A Can contain up to ~ 10 strokes Typically every 50ms First usually biggest ~ 10C ~10^{20} electrons

Several 100s MV generated; average moderate storm generates 100s MW

General Protection Principles

The general principles adopted for designing against the lightning threat, and particularly for high consequence ordnance, are:

Unique Firing Formats: Main explosive charge initiating trains are of the type which require unique format high power signals to function.

Isolation: This takes the form of the provision of positive insulating breaks between any lightning impingement point and the potentially hazardous electro-explosive components.

More advanced safety concepts, currently under study, are directed towards the so-called 'Wireless Approach' where there is no conducting link to the explosive's detonators.

Diversion: This takes the form of the provision of bypass paths to ground, to complement the isolation principle. General safety architectures are based on this principle, with the conducting weapon case and container(s) playing an important role. Special-purpose lightning surge arrestors, employing high dielectric constant material with a rapid electron emission characteristic are employed in umbilical connectors to enhance this protection

Screening: As well as current diversion, ordnance cases and containers also give protection against EM (Electromagnetic) penetration and subsequent coupling to electro-explosive circuits; they form Faraday screens. Internal compartmentalisation and screened cables (coaxial, and so on) give further protection of this nature. Field joints should not be capable of supporting high voltages due to lightning currents flowing in the shell and all essential apertures need to be analysed for EM leakage. Of course, where appropriate, all external connectors should be capped off.

Single point grounding: Ideally ordnance systems should only be electrically grounded to the case at one point to ensure that lightning currents flowing on the weapon skin cannot be shared with internal circuitry. The multi-point grounding hazard only arises if weapon case joints become resistive, or if there is massive case damage. The single-point grounding philosophy is carried over into the grounding of ordnance to containers and containers to load carriers or to buildings.

Multiple protective layers: The components of protection are identified above and the overall strategy is to go for defence in depth (in as far as it is possible), for each phase of the ordnance system's life. For example, there is strength in depth in terms of the ordnance system's internal protection, its case, its containers and its housing, that is. either in its protective building, with its own Lightning Protection System (LPS), or within the metal enveloped load carrier. Protection against the lightning hazard is not restricted to the general electro-magnetic threat, but also covers the secondary threats of potential fragment generation, spark of thermally initiated ignitions and fire.

Testing: Ordnance systems, particular of high-consequence type, are put through a lightning simulator test programme to ensure that they are intrinsically "lightning" proof in the undamaged state.

The US Ammunition Igloo Incident and Subsequent Trials

Before dealing with the generic ordnance life phases identified earlier, it is worth identifying some recent thinking and developments in terms of lightning protection of buildings.

Current best practice for the lightning protection of buildings in the UK is essentially contained within British Standard (BS) 6651 and MOD Prescriptions, and these form the basis for the protection of buildings within which ordnance systems are stored and processed. However, a few years ago the US experienced the salutary lesson of an ordnance igloo, protected by a regulation grounded air terminal LPS, blowing up. A subsequent investigation came to the conclusion that is was caused by a lightning strike which had caused internal scabbing of the structure, leading to impact on and detonation of exposed ordnance items. The explanation was based on the inductive voltage generated in the LPS system and the discontinuity between the roof and wall metal reinforcing (re-bar). The re-bar system has a much lower inductive impedance to ground, due to its "multiple" structure and, as a result, the lightning strike will seek to take this path if it can and the high voltages generated across the LPS can potentially lead to this occurrence. In the instance above, this voltage was generated across the roof to wall re-bar gap leading to a flashover and electrical explosion in the enveloping concrete with ensuing internal fragment generation.

This event led the US, in the form of an army contract to Sandia National Laboratory Albuquerque (SNLA), to conduct an investigation into lightning phenomenology associated with ammunition igloos. The main thrust of the work has centred on Rocket Triggered Lightning (RTL) trials, using the Sandia Transportable Triggered Lightning Instrumentation Facility (SATTLIF). These trials were conducted at the Pelham army range in Alabama. Tests were conducted on established igloos and a "special to purpose" building in which re-bar structures could be connected or disconnected for the purpose of phenomenology testing. Of course, in this form of testing, one has to settle for the lightning strikes one can bring down and these are generally below the worst case values in terms of peak current and rate of current rise. However, the general conclusion was that, in air terminal protected buildings, most of the current flowed through the re-bar system which, because of its lower inductive impedance, represented the most effective component of lightning protection. Of course, high voltages would be generated at any re-bar discontinuities and this would result in significantly large wall potential differences or even electrical explosion if the conditions were sufficiently severe. These trials have been supplemented with SNLA computer analysis work. As part of this programme, SNLA has undertaken the development of "non intrusive" re-bar continuity measuring equipment, which currently appears to be available in development, if not commercial form.

The United Kingdom Atomic Weapons Establishment (AWE) has been a party to these trials and, in addition, has been an active contributor towards the goal of understanding the phenomenology. AWE's involvement has primarily arisen through our joint trials and analysis programme geared to establishing best lightning protection procedures in the context of weapon accidents. These latter trials have "piggy backed" onto the igloo work, using the same SATTLIF facility, but of course with different "targets." These trials moved to the University of Florida lightning test range last year, where the objective was more strongly directed towards EOD aspects and to examining the response of HE to direct lightning strike.

The Lightning Risk to Ordnance

The primary safety issues with respect to high consequence ordnance systems are the risks of detonation of the conventional high explosive with the potential follow on consequences. The overall risk of the occurrence is based on a product of the probability of a number of events, including the probability per unit time of a strike in the "locality" of the abnormal environment generated by the strike interacting with the weapon and the probability that this environment leads to a high order reaction in the ordnance's main explosive. The strike can potentially lead to three classes of abnormal environment at the weapon, whose occurrence and consequence depends very much on the scenario. These are:

- Electromagnetic (EM) penetration - Giving rise to an electro- explosive threat.
- Fragment generation - Giving rise to a direct impact threat on the High Explosive (HE).
- Fire generation - Giving rise to thermal penetration to the HE

A high-order HE event arising from these environments leads directly to the prospect of inadvertent dispersal of harmful material and to a very low probability of an even more severe event.

In the UK, the top-level criteria for preventing major hazards from a high-consequence ordnance system are contained within the appropriate Proceeding of a very long standing body called the Ordnance Board and also within MOD Prescriptions. The criteria relating to the inadvertent initiation of conventional explosives are very stringent, and even more so for more severe consequences. These criteria are couched in terms of limiting event rates and risks,

$$\text{Risk} = \text{Event Rate} \times \text{Consequence},$$

and the overall lightning hazard has to be evaluated against these criteria.

In addition, for certain phases of the ordnance system' life, we have to comply with the UK's civil regulator requirements in order to be licensed (1974 Factories act and the HSE regulators).

Threats to Ordnance Explosive Originating From Lightning

EM Penetration of Structures

For typical materials and thicknesses, lightning currents flowing on intact cases will generate internal surface voltages of ~ V/m during the initial pulse phase. Voltage gradients of this order pose no direct threat to explosives or to high-voltage detonators and are marginal for squib safety. However, as noted previously, resistive field joints (under high current-flow conditions) can significantly change the situation. Significant holes in the case structure can lead to internal magnetic field coupling whose result relates to the hole size, location, and the orientation of the internal circuits and their degree of screening.

These latter issues arise particularly in the context of post accident conditions.

Case Burn-Through

The follow-on pulses in a lighting flash can lead to the burn-through of conducting shells. Case thicknesses, usually chosen for other reasons, are normally sufficient to prevent this. However, this can become an issue when hole-patching procedures are deemed necessary following an accident. Simulator tests, which include burn-through onto inner circuits, have shown electrical results in these circuits which were far less severe than expected.

Response Characteristics of Low-Voltage Initiators

These devices vary in type, but in the main require currents of 0.1 to 10A applied for the order of ms to function and are associated with circuits typically having an impedance ~ 0.1 ohm. They represent the most sensitive class of initiator and their inadvertent function in a high-consequence ordnance system will only lead to relatively minor effects.

High-Voltage Initiators

These generally come under the categories of electrical exploding bridgewire (EBW) devices and electrical exploding foil initiators (EFIs). There are also optical (laser) driven equivalents. These devices normally function from high-amplitude pulsed currents with amplitudes of a few hundred to a few thousand A with rise times in the μs and sub μs range. Further, they are also characterised by the so-called burst action A_b, the action value required to burst the wire or foil

$$\text{Action} = \int I^2 \, dt,$$

where I is the current (typically in the range 0.01 to $0.1A^2s$) and the current at burst, which represents the major factor in the strength of the electrical explosion (and the impetus given to the receptor explosive). The so-called I_{50} is that value of burst current that gives a 50% success of an end event from the initiator.

These requirements are far more unique than those for squibs, but lightning has the correct format if all forms of protection fail.

High-Velocity Impact on HE

High-velocity fragment impact on explosives can cause initiation and even detonation for sufficiently high fragment velocity and mass. High-voltage EFIs are based on this phenomenon. The response will depend on the type of explosive and on any layers of interposed protection. Fragments of ~ g order travelling at mm/μs velocities will cause concern for all explosives other than special Insensitive High Explosive (IHE). Not only can projectiles originate from lightning strikes on surrounding structures but also they can result from large currents flowing in conductors immediately adjacent to the explosive, such as those in cables.

Thermal Response

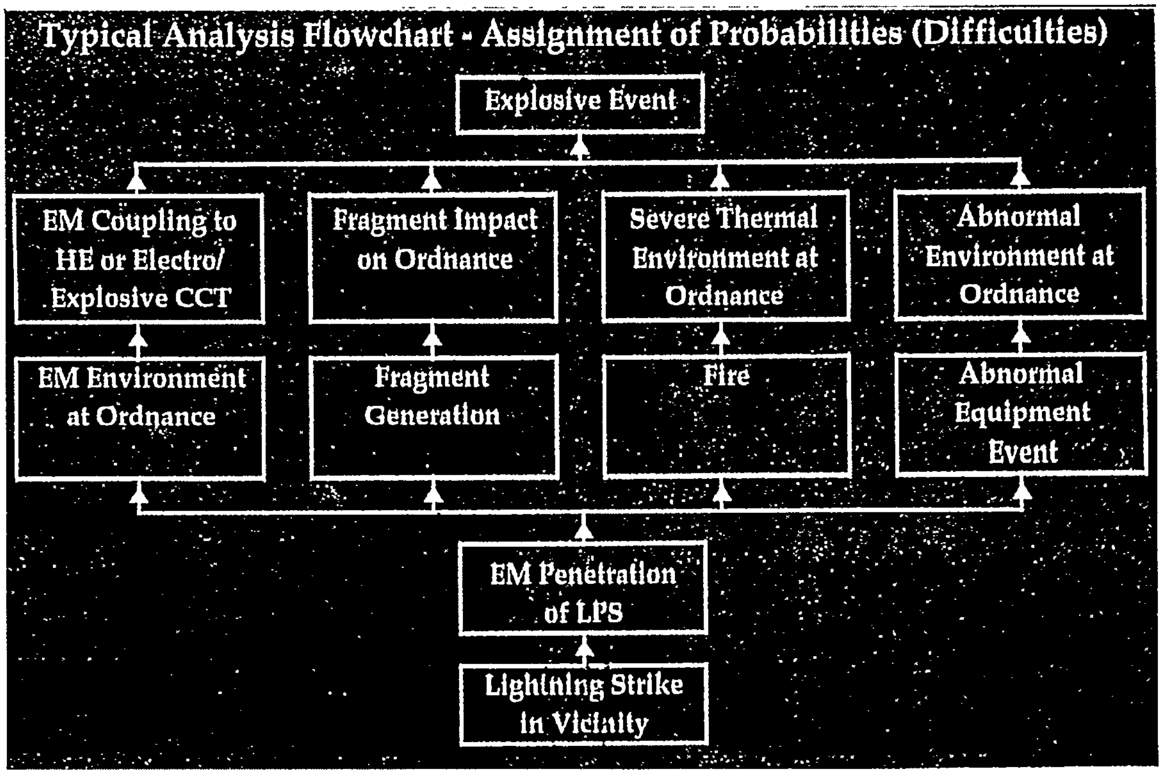
The response of explosives to thermal environments will depend on the explosive type, its degree of containment and the heating rate. In many cases, the result in a consuming fire would be a relatively mild deflagration.

Direct Strike on Explosive

In principle, a direct lightning strike onto explosive has sufficient concentrated power to cause initiation. This topic is the subject of current investigations.

Generic Risk-Assessment Approach

The generic risk-assessment approach is illustrated in simple form in Figure 8 in the form of a fault tree with a high-order event in the main explosive charge identified as the top unwanted event.



Typical Analysis Flowchart - Assignment of Probabilities (Difficulties)

Explosive Event
EM Coupling to HE or Electro/ Explosive CCT
Fragment Impact on Ordnance
Severe Thermal Environment at Ordnance
Abnormal Environment at Ordnance
EM Environment at Ordnance
Fragment Generation
Fire
Abnormal Equipment Event
EM Penetration of LPS
Lightning Strike in Vicinity

Figure 8. Generic risk assessment fault tree.

There are four general hazard paths to the this top event: the EM environment threat, the impact threat, the thermal environment threat, and the potential for abnormal equipment performance (which in turn can rise to abnormal environments) as a result of a lightning strike.

Any risk assessment will need to identify and detail all of the branches and components associated with each path and then, with some difficulty, assign the relevant probabilities of occurrence and response. Of course separate analyses will be required for each life phase of a particular ordnance system. The quantitative assessment of lightning risks has to be made along the lines described above. This includes the probability of a lighting strike in the relevant area, the probability that all of the lightning protection defences are defeated, that the "abnormal" environments reach the "sensitive regions" of the ordnance item, together with an assessment of its response. These aspects are briefly covered in the next sections.

Assessment of the Manufacturing Phase

High-consequence ordnance assembly areas have a strength in depth strategy for lightning protection. A lighting strike has to defeat an overhead catenary system, conducting mesh blankets, and the conducting structure of the buildings, for example re-bars. Further, prevention of EM coupling to, fragment impact on, and thermal exposure to the ordnance items is enhanced through separation from walls, internal grounding schemes, conductor continuity, and the absence of combustible materials. This is in addition to any intrinsic protection offered by the ordnance system itself which will include lightning-proof cases and containers in early disassembly and late assembly phases. In addition, operations are suspended during thunderstorm periods.

The In-Service Phase

Weapons earmarked for service (and particularly high-consequence ordnance) are required to demonstrate robustness to lightning strike in the un-containerised configuration and are tested on lightning simulators to demonstrate this. Of course, one can only sensibly carry out a limited number of tests and confidence is based on the very small monitored currents that "leaked" (typically tens of mA or less) into the system. Such tests also include strikes to umbilicals, such as at the electrical entry port for uncapped conditions, which in modern design have surge-arrestor devices. High-consequence ordnance systems are designed on the single grounding point principle, and this is carried over into the container, transportation, and storage configuration logic in order to maximise protection against the lightning threat.

The overall safety assessment follows along similar lines to that of the previous section in terms of the probability of strike, levels of protection, generation of abnormal environments, and their potential effects on the weapon. In transport, one has similar load carrier and container protection; in storage there is similar building and container protection. Building protection varies depending on weapon type and location, but it is usually of at least air-terminal LPS type coupled with a re-enforcing structure. Further, external movements are suspended when potential thunderstorm activity is forecast. Most high-consequence ordnance operations are also suspended during thunderstorm periods, particularly those activities that are not "under cover."

During this phase, we are always dealing with essentially intact ordnance items which include their own Faraday screening embodied in mechanically and thermally robust structures, together with their internal safety systems.

The Weapon-Accident Phase

The UK has not experienced a significant event of this nature in relation to high-consequence ordnance. Nevertheless, well-planned and exercised procedures have to be put in place to cover such an unlikely eventuality. EOD procedures are based on applying the most sensible and safest procedures available in relation to the problem in hand. In UK parlance this is termed ALARP (As Low As Reasonably Practicable). In this scenario, the ordnance item could well be out of its container with its Faraday screening damaged and the single grounding point arrangement compromised. There are many possibilities.

The pursuance or suspension of procedures and the urgency for further lightning protection measures, including their level, will obviously be influenced by the meteorological conditions, the level of damage and the degree of controlled disassembly, if this is in progress. For example, we have a broad understanding of the electromagnetic levels generated within intact and damaged containers and ordnance cases. Sources of combustion should of course be removed as soon as possible. Container and ordnance case breaches will be "secured" with conducting foils and tapes, and portable LPS systems can be erected if deemed necessary.

In fact, the UK's portable LPS has been the main subject of the RTL EOD tests in the US, where the telescopic lightning pole, which has been strongly advocated by the UK, has demonstrated its value. Figure 9 shows a typical RTL flash with its multiple stroke signature. The aim has been to identify a means of providing flexible enhanced protection, which is easily portable, easy to erect and poses no other safety threats as a result of its erection process and presence.

There are a number of aspects to the potential lightning threat to an ordnance item involved in an accident, and these are:

(1) The direct strike
(2) The side strike
(3) The strike point plasma
(4) The ground arcs
(5) The ground currents
(6) The associated electric and magnetic fields

and these are depicted in Figure 10. This range of phenomena is present in the absence of a pole. The pole is intended to protect against direct strikes, to prevent side strikes, to draw the impact point plasma away from the weapon position and to ensure that ground arcs, ground currents and electromagnetic fields are orientated into the least hazardous direction. Figure 11 illustrates the, in-principle, extra protection and grounding arrangements for ground arc suppression. Figure 12, taken from one of the RTL tests in the US, shows the typical ground plasma and ground arcs associated with a lightning strike. These latter phenomena had previously been suspected of being present, but had not been directly observed.

The motivation for this trials programme originated as a result of a debate between the US and UK about protection schemes. Our understanding of the lightning phenomenon (including its spectrum of threats), and our ability to mitigate against it in ordnance system accident scenarios, has increased significantly over the past four to five years.

Typical Facility Pitfalls

Figure 13 illustrates some generic potential lightning safety pitfalls to be avoided with regard to general facilities. These range from, "What was the LPS plan and rationale; was it built to the plan; have subsequent activities disturbed the original rationale?" to "Are all penetrations properly bonded to ground, are all electrically services surge arrested and are all conducting structures continuous?"

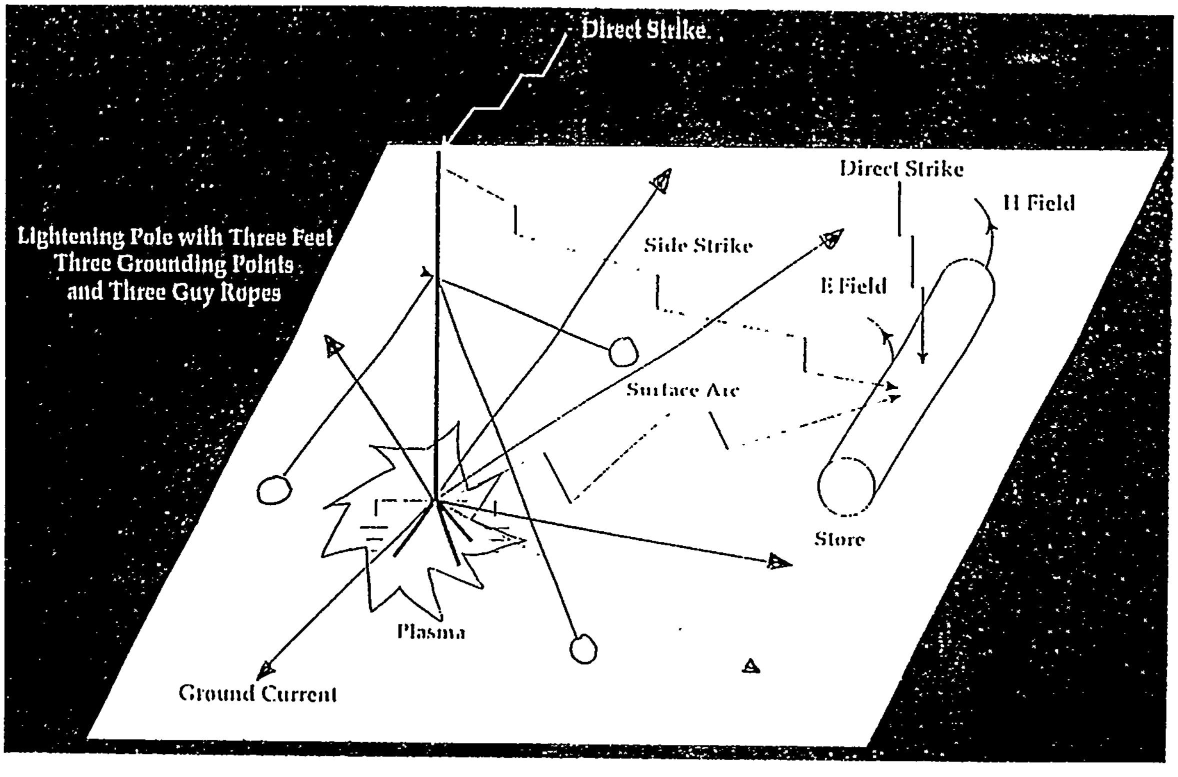


Figure 10. Schematic lightning threats.

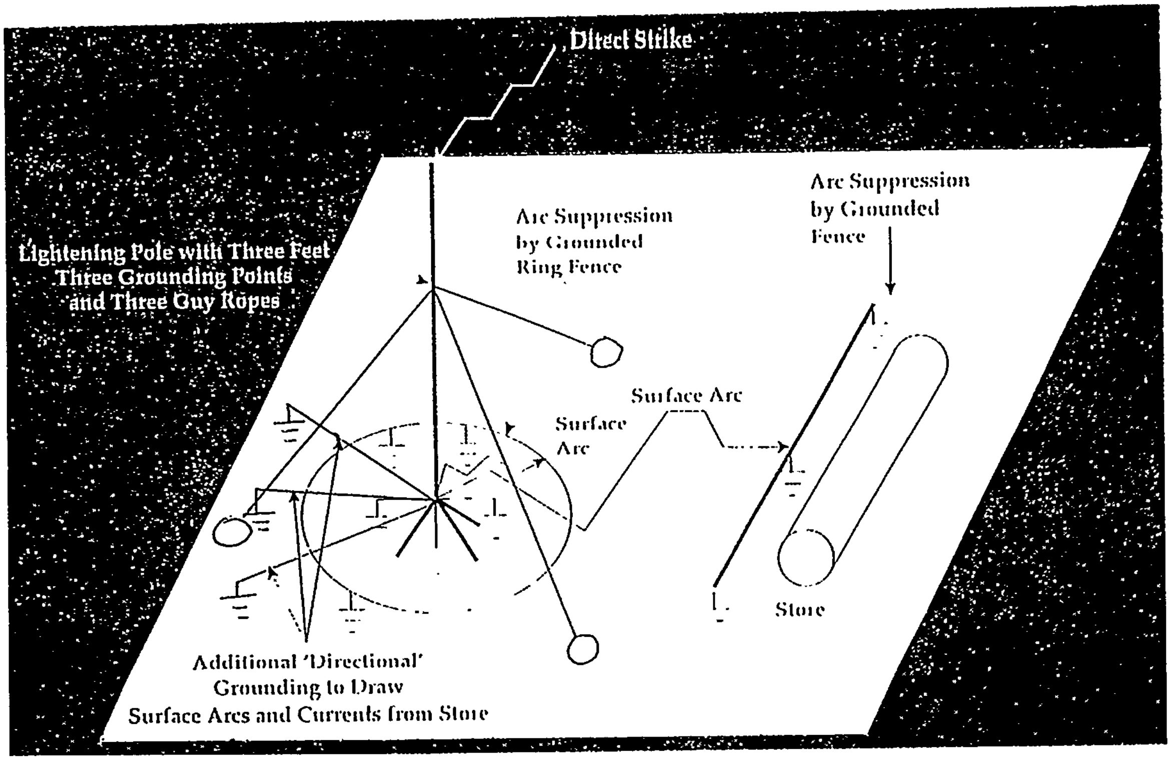


Figure 11. Additional protection schemes.

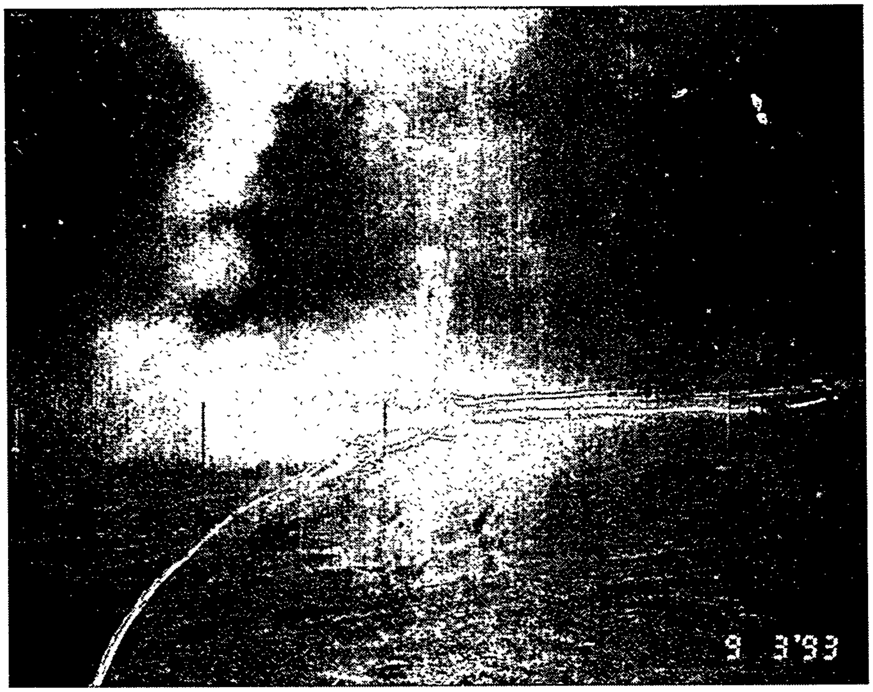


Figure 12. Strike showing surface arcs.

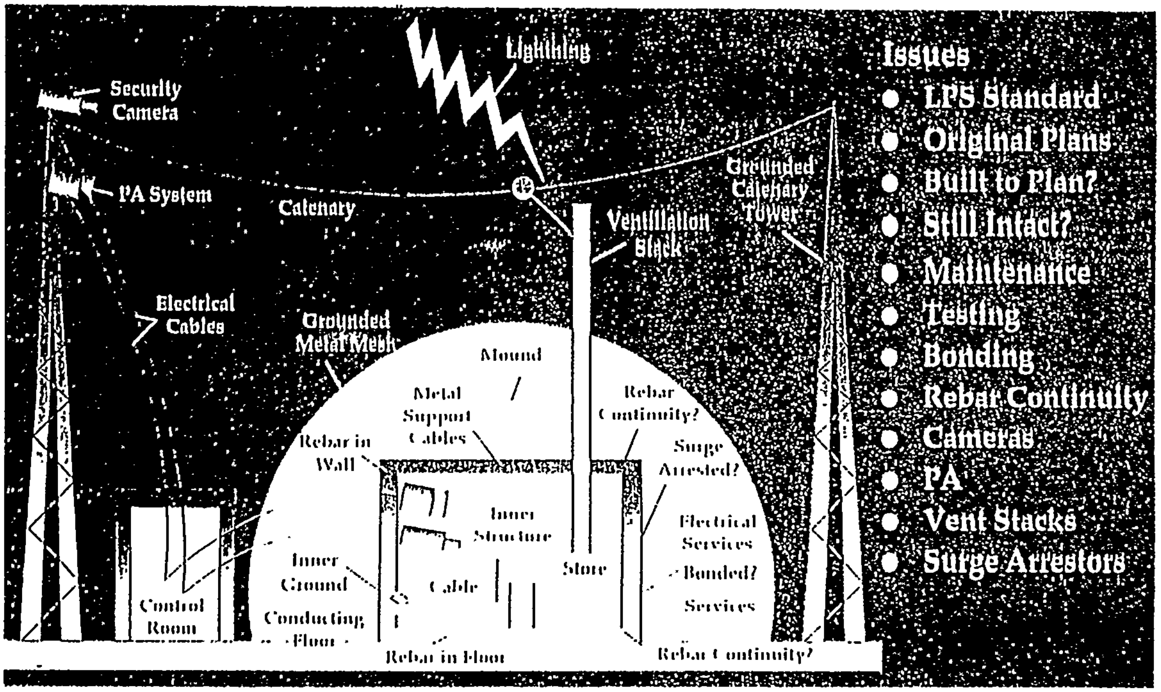


Figure 13. Illustrative facility pitfalls.

Summary

The lightning threat and its hazards to ordnance items, particularly to high-consequence ordnance systems, has always been recognised in the UK. As a result, high-consequence ordnance, testing, protection and procedures have embodied the highest standards of implementation. Safety assurance against this hazard has continued to improve with improvements in our understanding and with the evolution of safety concepts and technologies. More advanced design safety concepts, currently under study, are directed towards the so-called "Wireless Approach" where there is no conducting link to the major explosive parts.

External protection centres on associated high-quality Faraday containment systems and many activities are suspended during thunderstorm periods. When processed within special facilities or stored within service facilities, high-consequence ordnance systems also enjoy the extra protection afforded by these, which themselves follow best lightning-protection practice.

High-consequence-ordnance design, protection, and procedures minimise the potential for accidents leading to the loss of protection against the lightning threat particularly in the context of today's more relaxed political atmosphere. Road transport is associated with robust containerisation, robust load carriers, and restricted convoy speed limits. However, even in the very unlikely event of an accident leading to a significant loss of protection, coupled with a lightning threat, well exercised EOD teams together with their equipment and procedures are in place to further mitigate against the lightning threat.

Acknowledgements

The authors gratefully acknowledge the helpful discussions and support given by members of the Atomic Weapons Establishments (AWE) Electrical Systems Department and Sandia National Laboratories/Albuquerque Electromagnetics Department.

Biography

Malcolm is currently the Scientific Adviser to the Director of Warhead Engineering at AWE and has, for some considerable time, been responsible for, amongst other things, the development of advanced warhead system safety concepts, together with the assessment of their safe implementation. His previous post was Head of the Warhead Electrical Safety Group.

Malcolm joined AWE in 1967, after Graduating (BSc) from the University of Wales in 1964 with first class honours in physics, followed by a Ph.D. (1967) in solid state physics, from the same establishment. His career at AWE has taken him through a wide range of scientific and engineering topics, but he has maintained a continuous association with electrical based systems. He is an adviser to a number of UK Ministry of Defence and AWE safety bodies.

Marvin Morris

Biography unavailable.

Development of an Accident Scenario with the Help of a Complex Numerical Analysis Using as an Example an Accident at a Compressor Gas Transfer Station

G.S. Klishin
V.E. Seleznev
A.A. Mukashev
Russian Federal Nuclear Center (RFNC)-All-Russian Research Institute
of Experimental Physics (VNIIEF)
Russia

Abstract

The present approach to the failure analysis demands conduction of complex calculations in different areas, along with the usual phenomenological situation assessment. At such a case, numerical methods of continuous medium mechanics, techniques of chemical physics, mathematical optimization, and the theory of reliability are implemented. Experience combined with the evaluations of experts who have good knowledge of the failure object and the results of mathematical simulation of the accident makes it possible to define the actual reasons of the accident in the shortest period of time and work out preventive measures for the future. An example of such an experience in the analysis of the reasons, mechanism, and consequences of the accident at the compressor gas transfer station is presented.

Preliminaries of the Accident

A new compressor shop (CS) was built at a compressor gas transfer station (CGTS). The new shop comprised three gas-transferring units (GTU) that were joined together with pipes following a parallel scheme. By the time of the accident, start-up and adjustment work was going on at the shop. These works took place in wintertime, December to February. In the beginning of winter, the shop pipelines were subjected to a hydrostatic test to check out their tightness. Start-up of the GTUs began at the beginning of January. In order to analyze their operation before the accident we give the units numbers.

GTU#1 was started up four hours before the accident and switched off two hours before the accident. Before that, it had not been in operation. During those two hours it worked in the "Ring" mode. This means that the transported gas was not fed into the main pipeline, but was recycled in the ring of the anti-surge channel. The pressure during the GTU#1 operation was 5.43 MPa in the recycle channel. When GTU #1 finished its operation (two hours before the accident) the pressure in the recycle channel was relieved to atmospheric, 0.1 MPa.

GTU#2 was started in January. The forced pressure in the main pipeline was 5.48Mpa. This pressure was not relieved after GTU#2 finished its operation.

GTU#3 was started for gas transportation in the main pipeline 320 hours before the accident. The pressure in the main pipeline was 7.33MPa.

The Accident

The accident took place at the end of February. Attending personnel heard the noise of a dull blow. In this moment the diagnostics of the GTU#3 registered the failure of its operation and automatically halted the unit.

During examination of the place of the accident the following was discovered:

- GTU#2, GTU#3, and their pipe bindings did not have any evident damage;
- GTU#1 was partly damaged, plucked off from its fasteners and its basement. Judging by the traces, the pipe binding of the unit underwent a strong oscillation displacement (350 mm), but managed to preserve its integrity;
- In the pipe binding of GTU#1, an ice fuse was found in the pipe 12 m from tap#2.

A team of experts, including specialists of conversion Design Bureau #5, were called to investigate the reasons for the accident.

After examination of the place of the accident, *the commission made a supposition, that during the hydrostatic test of the shop pipes in the beginning of winter the water was left in the pipes. That happened because of the drawbacks of the hydrostatic test technology. The total amount of water was equal to 11 tons. Only small amount of water happened to be in the zone of the frozen ground (Figure 1). That part of the water froze and an ice fuse was formed. The reason for the accident was the plucked-off ice fuse blowing against two lead-a-way pipelines sequentially and then directly against bulb tap #2 of the force pipe of GTU#1 (Figure 1).*

The RFNC-VNIIEF specialists were to confirm or to rebut the supposition of the experts, to work out a calculated accident scenario and evaluate the effect on the construction elements of the accident. The time limit for this analysis was 10 days. The assessment was done with the help of calculating techniques implemented in the DB #5 RFNC-VNIIEF, based on ata provided by the "GAZPROM" organizations and enterprises.

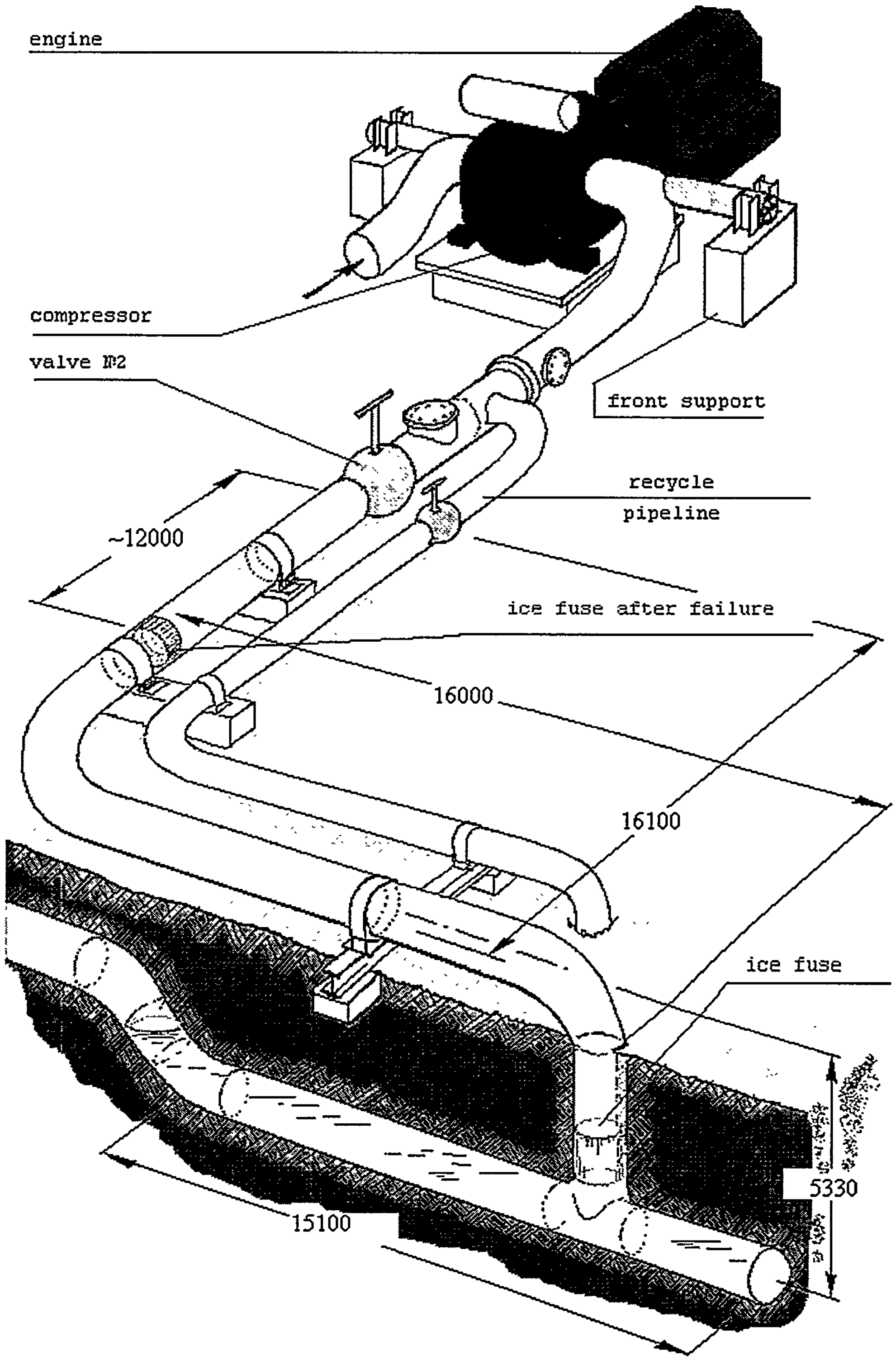


Figure 1. Sketch of failure location.

An Abridged Variant of the Calculated Scenario of the Accident

1. In a three-way pipe there was a water column (Figure1). Under the influence of the environment the water froze and an ice fuse was formed. The thickness of the fuse, L, (Figure 2) was determined by the depth of the frozen ground and was approximately 1m. The fuse diameter was equal to the diameter of the pipe D~1m, neglecting the expansion of the pipe that resulted from the ice fuse formation.

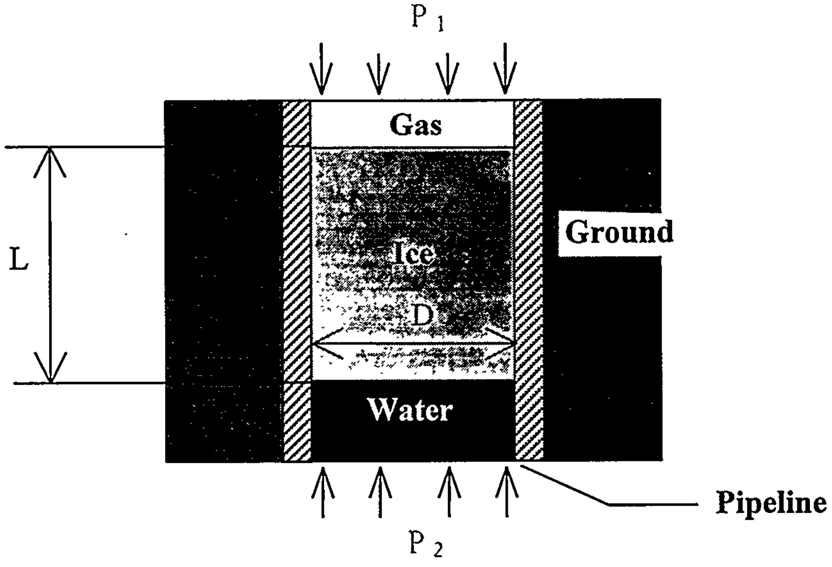


Figure 2. Ice fuse.

2. After the hydrostatic test, GTU#1 was started in January. It created a pressure of 5.48MPa in the main pipeline that was not relieved until the accident. So, water crystallization when it was freezing took place either at the atmospheric pressure, or under the conditions of the compression of the water column by the natural gas (the pressure of the natural gas on the surfaces of the water column was P_0=5.48MPa). As it was shown by further calculations, the fuse was formed under compression, as failing this, the pressure difference on the ice fuse, ^P=P_1-P_2~5.38MPa, P_1=P_0=0.1 Mpa, would have inevitably resulted in the immediate fuse pluck off.

3. 320 hours before the accident, GTU#3 was put into operation. It increased the pressure in the main pipeline up to P_{out}=7.33MPa. There was a pressure difference at the fuse of not less ^P=1.85MPa, that continued to affect the fuse during the 320 hours until the time of the accident. This time will be called the prefault time.

4. At the long strained and stressed state ice has plastic properties. Here it is important to consider ice's ability to creep. In this very case, the strength assessments are made basing on shearing stress values (Zaretski-Trude model). The calculation results show

that to pluck-off the ice fuse 1m thick (the thickness was defined by the thickness of the frozen ground in the accident area) due to the ice-creep process during 320 hours there must be pressure differences on the fuse more than 2.38 MPa (Table 1).

Table 1. The pluck off time t of the 1m thick ice fuse depending on the pressure differences on it Δ**

Δ• , MPa	4,83	3,00	2,80	2,60	2,40	2,38	2,20
t^{**}, hour	0,91	19,1	36,2	81,8	251,8	320	325 days

The pressure differences on the ice fuse in the prefault period of less than 2,0 MPa does not result in the pluck-off of this fuse (if the reason for the pluck-off is the ice creep). 1,85 MPa difference of the pressure in 320 hours can pluck off a fuse of not more than 45-cm thick. So, if the gas was relieved a little from tap#2 and an overflow valve during the prefault time there could be created conditions for the fuse pluck-off because of ice creep.

5. Four hours before the accident, GTU#1 had been operated in the "ring" mode. The pressure at the outlet of the GTU#1 was 5.48 MPa (that is the pressure difference at the fuse practically did not change after GTU#1 started up). According to the algorithms of the taps opening, the heated gas at 19C began to come to the force pipe of the GTU#1 (Figure 1). Calculations of the heat effect on the ice fuse were done with a finite element technique. The results of the calculations excluded the influence of the heating factors on the fuse pluck-off. So, in this case there is only one reason for the fuse pluck-off left, that is, the creep of the ice.

6. Let us analyze two extreme variants of the calculations of the fuse pluck-off as a result of ice creep. In the first case, it is assumed that after GTU#1 has finished its operation and the gas was discharged from the part between the taps #1 and #2 of the GTU#1 to reach the atmospheric pressure, the discharge from the part of the force pipe between the ice fuse and tap#2 through the tap#2 and the overflow valve was insignificant (the pressure differences did not surpass 2.38 MPa) (Figure 1). In the second case, a considerable discharge of the gas through tap#2 and the overflow valve is assumed.

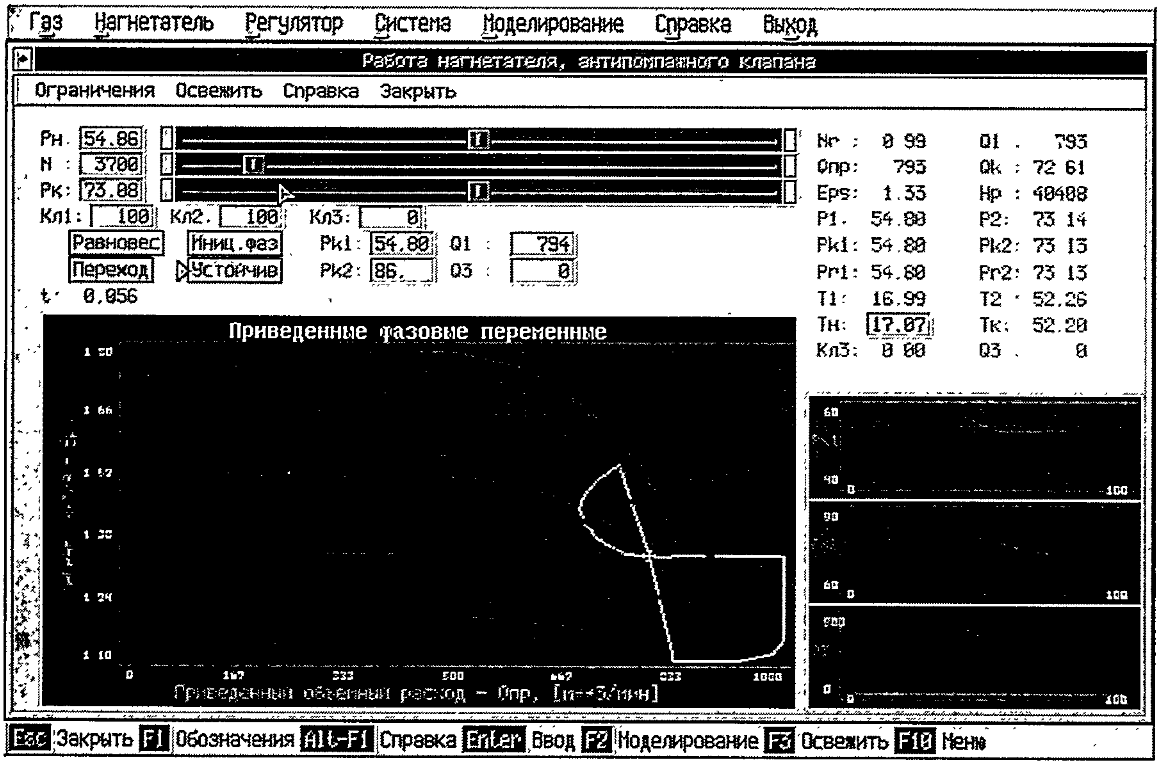
7. The first case demonstrates fuse pluck-off resulting from the slow (during 320 hours) creep of the ice. The pressure difference at the fuse in this case is evaluated higher. Gas dynamic calculations that were performed using the techniques of RFNC-VNIIEF prove that the blow impact of the ice fuse against tap#2 happened through the column of air. There was no direct blow of the fuse against tap#2. The effect of the compression - dilatation waves (with the calculated parameters) on the stable operation of GTU#3 was insignificant (see Figure 3). Mathematical simulation shows that the failure of GTU#3 because of such impacts is improbable.

8. The second case demonstrates the pluck off the fuse resulting from the quick (during two hours) creep of the ice. The pressure difference at the fuse in this case must exceed 4.165 MPa (here we did not consider the retrospective of the creep of the ice during 318 hours before that). For example, if the pressure difference at the fuse is 4.83 MPa, its pluck off will take place in approximately 55 minutes after it is set. Figure 4 shows the results of the calculations of the gas dynamic effect on GTU#1, a force part of the compressor shop bindings and GTU#3. The calculations prove that the blow effect of the ice fuse on tap #2 was through the column of the air. There was no direct blow of the fuse against tap#2. The influence of the compression - dilatation waves (with the calculated parameters) on the stable operation of GTU#3 was considerable. Mathematical simulations let us assume that in this very case the failure in the operation of GTU#3 is connected with the accident.

9. To choose the most preferable variant of the calculated scenario of the accident development among the above-mentioned ones, a dynamic analysis of the strength of pipeline binding and the fastening elements of the GTU#3 is to be done. Calculations showed that the amplitude of the shock effect on the bulb tap#2 must be significantly more than 3.6 MPa to reach the registered values of the force pipeline displacements in the direction of GTU#1 (~400mm) and the cutting of the anchor bolts. Such consequences of the failure take place when the amplitude of the shock effect increases up to 15.5 MPa, that corresponds to the fuse pluck off at the pressure difference of 4,83 MPa. So, the second variant of the calculated scenario of the failure development is preferable. The results of these calculations are in Table 2.

Table 2. Maximum Calculated Values of the Parameters of the Dynamic Behavior of the GTU#1 Force Pipeline Construction

Load	Cut force in assembly bolts	Pipeline displacement in compressor 1 direction, mm		
$\cdot 10^6$,N	$\cdot 10^6$,N	rigid compressor fastening	free compressor movement	compressor fastening from movement
2,7	2,15	42,5	156	77
11,9	9,14	180	800	350


Газ Нагнетатель Регулятор Система Моделирование Справка Выход
Работа нагнетателя, антипомпажного клапана
Ограничения Освежить Справка Закрыть
Равновес
Иниц.фаз
Переход
Устойчив
Приведенные фазовые переменные
1 50
1 66
1 52
1 38
1 24
1 10
0
167
333
500
667
833
1000
Приведенный объемный расход - Опр, [м**3/мин]
60
40
0
100
80
60
0
100
500
0
0
100
Esc Закрыть F1 Обозначения Alt-F1 Справка Enter Ввод F2 Моделирование F3 Освежить F10 Меню

Рн. 54.86
N : 3700
Рк: 73.88
Кл1: 100 Кл2. 100 Кл3: 0
Pk1: 54.80 Q1 : 794
Pk2: 86. Q3 : 0
t· 0,056

Nr : 0 99 Q1 . 793
Qпр: 793 Qk : 72 61
Eps: 1.33 Hp : 40408
P1. 54.80 P2: 73 14
Pk1: 54.80 Pk2: 73 13
Pr1: 54.80 Pr2: 73 13
T1: 16.99 T2 · 52.26
Tн: 17.07 Tк: 52.20
Кл3: 0 00 Q3 . 0

Figure 3. Effect on GTU#3 at the big pressure difference.

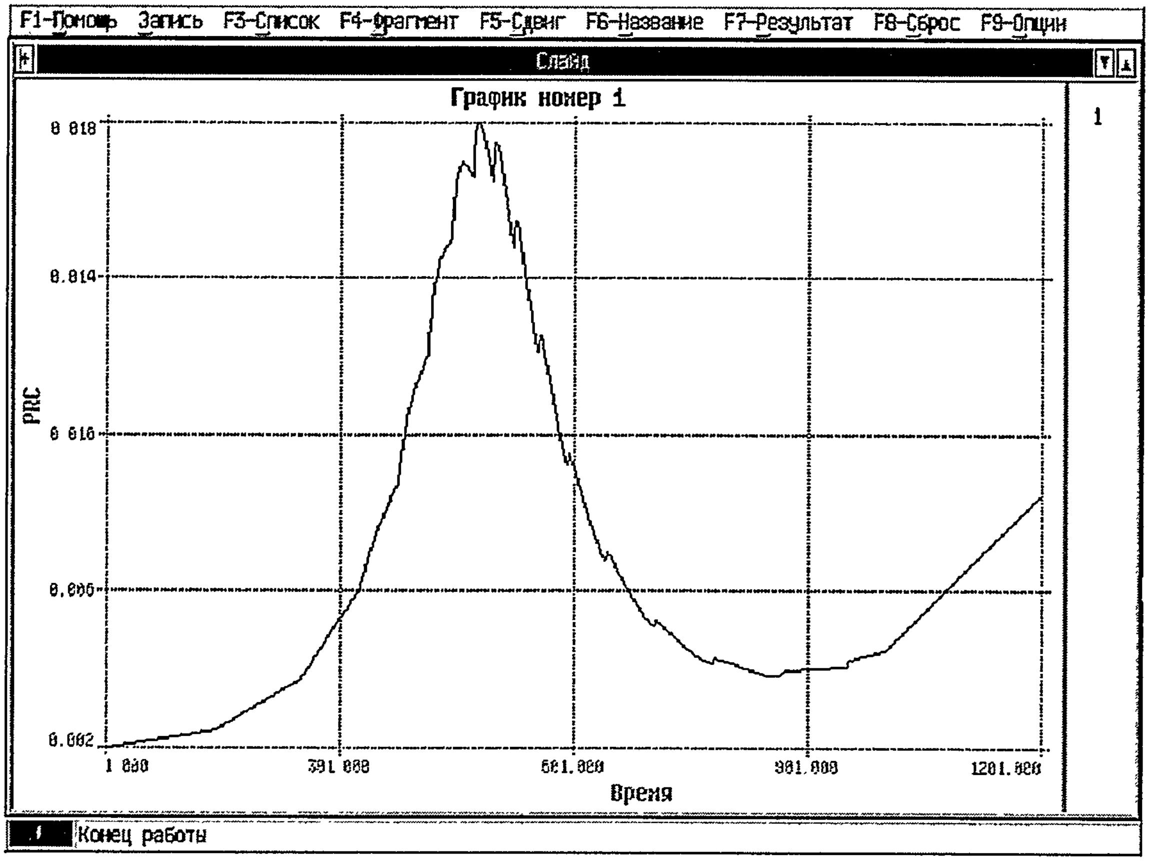


Figure 4. Dynamic pressure on valve # 2 at the big pressure difference on the ice fuse.

Biography

Biographies not available.

Process Failure Mode, Effects, and Criticality Analysis (FMECA) Commercial Application to a High Reliability Navy Microelectronics System

James Heinz
US Navy Space and Warfare Systems Command
Falls Church, Virginia

Jon A. Lumpkin
PVA, Inc.
Burlington, North Carolina

Brian Moriarty
David Wise
TRW System Service Company
McLean, Virginia

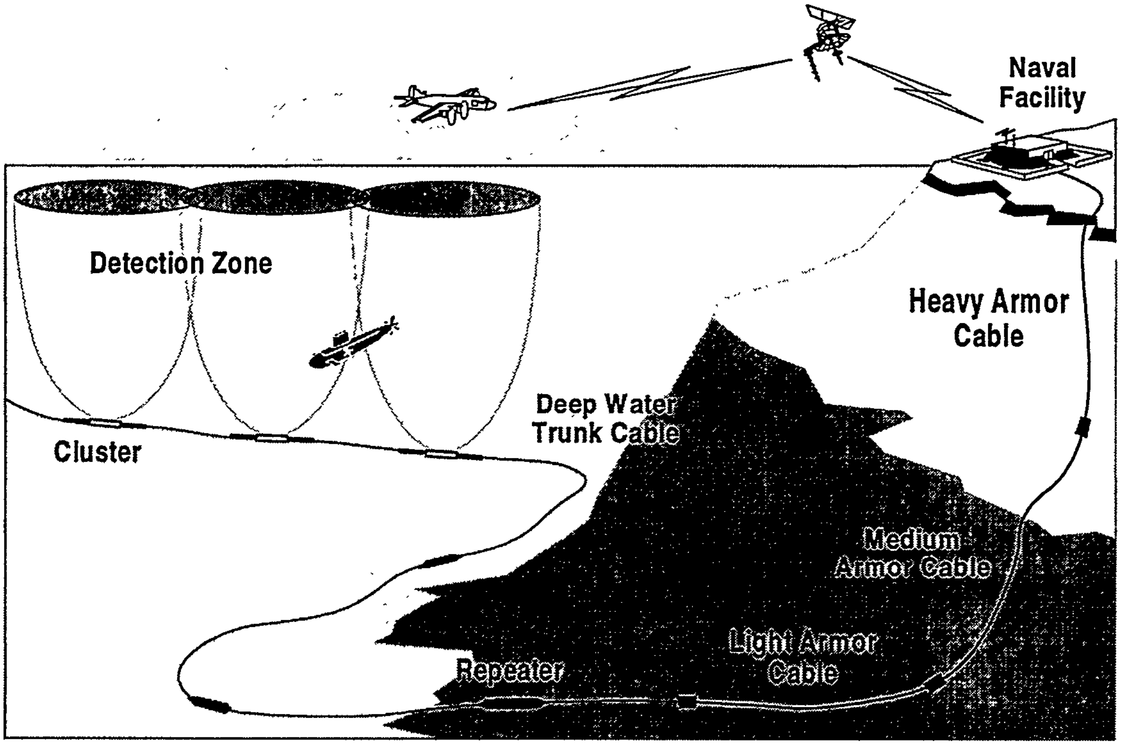


Figure 1. Fixed Distributed System Underwater Segment (FDS UWS)

Abstract

The US Navy performed a Process Failure Mode, Effects and Criticality Analysis (FMECA) using key features of the automobile industry published Failure Mode and Effects Analysis (FMEA) instruction manual. The FMECA examined a high reliability electro-mechanical subsystem during the manufacturing processes. Potential manufacturing-induced failure modes were evaluated to mitigate costly repairs in an operational environment. Application of this commercial method proved to be a major step in early identification, verification, and correction of system, design, and manufacturing process-related failure modes. In the automobile industry, a process FMEA emphasizes the safety of the automobile product and the minimization of costly repairs. The Navy's use of this methodology focused on identifying and correcting failure modes of critical shop processes which could impact operational reliability. Early identification and correction of these failure modes enhanced product quality, reliability, and the cost effectiveness of the delivered product. It also clearly identified areas which, had they not been identified, could have compromised the integrity of the system.

In the past, typical military programs focused on design related FMECAs. Now, a proven commercial methodology has been applied to manufacturing processes for a high reliability military program. In particular, a Process FMECA approach has been applied to the US Navy Fixed Distributed System (FDS) Underwater Segment (UWS) wet-end hardware manufacturing and integration processes (Reference Figure 1). It identified potential process-induced reliability problems impacting the system life and storage life. This was accomplished by performing a systematic review of all potential process-related failure modes, identifying associated causes and effects, and ranking each failure mode in terms of criticality in order to prioritize corrective actions. It was critical that no manufacturing process-induced failure modes remain in the system as they are extremely costly and difficult to repair. Appropriate corrective actions were taken to eliminate or control the high-risk failure modes.

Introduction

The Ford Motor Company FMEA System-Design-Process Handbook was examined for its usage of manufacturing process-related FMEA techniques. These processes included shop applications combined with high reliability, microelectronics parts in a fiber optic cable system. The Process FMECA examined manufacturing and assembly processes over a two-year period for potential process-related failure modes. It identified the causes and effects, and ranked each failure mode in terms of criticality in order to prioritize corrective actions. The examination resulted in recommended corrective actions to eliminate or control high risk failures.

Program Plan

Reference Documents: The Department of Defense (DoD) and commercial documentation were used to support the development of the FDS UWS Process FMECA. MIL-STD-1629A was used as the basic format for the generation of failure modes, causes, and effects. The Ford System Design Process Handbook FMEA was used to enhance the analysis of criticality issues and the priority ranking of relative criticality to ensure effective corrective action and mitigation of critical failure modes.

Type of Work: The development of the Process FMECA consisted of four types of activities:

1. Developing relational databases to document the large number of process-related failure modes and to ensure linkage to the design-related failure modes and shop process documentation.
2. Performing a detailed review and analysis of shop processes and procedures (work instructions for shop personnel), including visual review of shop manufacturing processes.
3. Identifying potential process-related failure modes, causes, and effects by reviewing documentation and shop processes. An initial relative criticality assessment was performed, and where indicated by the criticality assessment, corrective action was initiated. The criticality assessment was based on a prioritization of the relative criticality number (the product of the probability of occurrence, the severity of impact if the failure mode occurred, and the probability of detection of the potential failure mode).
4. Reassessing the critical failure mode after corrective action resolution by assigning a final criticality assessment.

Activities 2 through 4 above were performed as a team effort with the manufacturing groups using Statistical Process Control (SPC) techniques. Process Qualification Teams (PQT) for each shop were tasked with qualifying their shop in accordance with SPC requirements. The Process FMECA team participated in these activities, by providing input relative to critical process parameters and using PQT data to support the identification of failure modes.

Why was the work performed: The FDS UWS system is in an environment wherein operational repairs are very costly and time consuming. A very high reliability design (24-year system life) was therefore required. The design required the process integration of new, unproven manufacturing technology for electronic, mechanical, and fiber optic parts. Many new manufacturing processes were also introduced to perform this integration. Although a Design FMECA was performed, a Process FMECA was considered necessary to ensure the manufacturing processes would not introduce undetected failure modes which could degrade system reliability.

How was the work performed: An integrated team effort between reliability engineering and manufacturing was implemented in conjunction with an SPC process to ensure the integrity of the manufacturing processes.

The fundamental approach implemented the basic FMECA requirements identified in MIL-STD-1629A, in addition to the criticality features of the Ford Motor Company Failure Mode Effects Analysis (FMEA) System Design Process Handbook. Tables 1 and 2 show the format and types of data collected for analysis, documentation, and implementation of corrective actions.

The criteria for determining if corrective action was required for a given process failure mode was a function of the three criticality evaluation factors (probability of occurrence (PO), severity level (SL), and detectability level (DL)) and their impact to the potential reliability of the 24-year system life. The product of the three criticality factors provided an initial criticality number (CNI). The first assessment focused on the highest initial criticality numbers (a parato listing). Within this listing, failure modes with the highest criticality numbers impacting design changes, such as single point failures or critical attributes (dimensional tolerances, materials, etc.) were always candidates for corrective actions. After the correction actions have been completed, another criticality evaluation was performed. This resulted in a final criticality number (CNF).

Failure modes were identified along with associated causes, effects, and criticality assessments in order to prioritize subsequent corrective actions. The same techniques and approaches used for a design-oriented FMECA, were also used to develop a Process FMECA. Instead of inherent hardware and design failure modes, potential process-induced failure modes were considered. Since a hardware design FMECA was already accomplished, using a relational database each process failure mode was related to the resulting hardware design failure mode/cause to correlate processes. In this way, Configuration Item (CI) hardware/design failure modes were categorized in terms of process related failures, and vice versa. The approach taken for the Process FMECA consisted of the following steps:

- Identifying major and subordinate CIs.
- Documenting the work instructions, shop aids, test requirements, routing documents, and drawings associated with each Make Item (a unique item with specific manufacturing instructions and processes).
- Establishing an indentured product list for each Make Item within the overall system.
- Developing or using existing process flows based on the indentured product list.
- Performing a desktop review of all documentation to identify process steps and the most obvious process related failure modes.
- Inputting all process steps into the relational databases.
- Performing a physical review of manufacturing processes for each Make Item
- Performing a detailed failure mode analysis (identifying the failure modes, causes, effects and criticality assessments).
- Identifying corrective actions to mitigate high criticality failure modes.
- Reviewing corrective action resolution, re-evaluating criticality assessments, and documenting the results.

Process FMECA and Manufacturing Integration

Statistical Process Control (SPC): Process FMECA personnel actively participated in the SPC process for all shops. Since the SPC effort utilized many of the elements required to perform a Process FMECA, these two tasks were coordinated to capitalize on common elements. This coordination eliminated some duplication of effort and provided each valuable input to improve each effort. For example, Process Engineering developed extensive Process Flow Charts, and defined how each work cell in a given shop related to one another. This included process times, yields, and routing as model inputs. These same process flows were used by the Process FMECA effort as the initial (high level) process steps for subsequent failure mode analysis. Initial output of the Process FMECA was provided to shop personnel to aid in the selection of process parameters.

Table 1 - Process Document Procedures and Steps

(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)	(k)	(l)
Process Document (PD)	Process Step (PS)	Failure Mode (FM)	Process Failure Mode Indicator (PFMI)	Design Failure Mode Indicator (DFMI)	Failure Effect(s) (FE)	Sev. Lvl . (SL)	Failure Causes (FC)	Prob. Of Occur. (PO)	Existing Process Controls	Dect. Lvl. (DL)	Criticality Number (Initial) (CNI)*

*** CNI = SL x PO x DL**

(m)	(n)	(o)			(p)
	Responsibility/Action Taken • Action Item # • Actionee	Final Criticality Factors			
Recommended Actions	• Closure Date	SL	PO	DL	Criticality Number (Final) (CNF)**

****CNF = SL x PO x DL**

Table 2 - Primary Database Definitions

Step	Data Field	Data Definition
(a)	Process Document (PD)	Part number of the process document.
(b)	Process Step (PS)	A logical procedure or step within the process document.
(c)	Failure Mode (FM)	The reason a component fails to meet requirement specifications of this step or a process that fails its intended function.
(d)	Process Failure Mode Indicator (PFMI)	A numeric code to sequence and identify multiple failure modes within a given process step (Codes are 01 thru 99).
(e)	Design Failure Mode Indicator (DMFI)	A numeric code to sequence and identify multiple failure modes within the design evaluation (Coded are 01 thru 99).
(f)	Failure Effect(s) (FE)	The result of the failure mode at some point after the current process step. Identify different levels of effects as appropriate.
(g)	Severity Level (SL)	The severity in terms of the seriousness of the failure mode effects.
(h)	Failure Causes (FC)	The process defect that results in the failure mode.
(i)	Probability of Occurrence (PO)	The relative probability ranking given the process step as currently defined.
(j)	Existing Process Controls	Existing process controls that can prevent or detect the failure mode. Detection can also occur in a downstream process.
(k)	Detection Level (DL)	The ranking of the probability that the existing controls will enable failure mode detection.
(l)	Criticality Number - Initial (CNI)	The product of: SL x PO x DL. A relative number that only has meaning when compared to other criticality numbers.
(m)	Recommended Actions	Identify recommended actions that can reduce CNI. The priority of solutions should begin with Severity Level, then Probability of Occurrence, and finally Detection Levels. Since process improvement is the goal, actions should be oriented toward correcting causes.
(n)	Action Taken	The result of the recommendations.
(o)	Final Criticality Factors	Reassess SL, PO and DL based on the action taken results.
(p)	Criticality Number - Final (CNF)	Final Criticality Number based on process changes.

Process Qualification Team (PQT): To provide objective evidence of a shop's ability to meet production and quality requirements, a formal qualification process was implemented for all shops. The first step in formal qualification was satisfactory completion of the SPC process. Process FMECA personnel (including the Quality Segment) were permanent members of the PQT and the resulting Process Change Control Board (PCCB). Both the Process FMECA and Failure Reporting, Analysis and Corrective Action System (FRACAS) efforts supported this process in conjunction with Quality Segment support.

Action items were generated during the audit of each shop-seeking qualification. The change recommendations identified during the Process FMECA were provided as action items during the PQT. All action items required closure prior to formal shop qualification.

Process FMECA Reviews in the FDS UWS Program

Three types of reviews were conducted during the Process FMECA tasks:

- SPC/PQT reviews with Reliability Engineering as part of these teams.
- Periodic reviews with the Navy to assess progress, review findings, and identify interim results and problems.
- Final review with the Navy to document final findings and lessons learned.

These independent reviews were critical for periodically checking the status and resolution of overall analysis, critical findings, and action items. Summaries of action items and activities resulting in manufacturing control and elimination of failure causes were discussed and verified by an audit group not involved in the actual work (similar to the Quality organizations of companies). Use of a pre-defined acceptance criteria (checklist) was key to assuring a complete well-balanced review.

Final Findings

Over 2000 unique process manufacturing steps were evaluated for potential failure modes. Many of these process steps had multiple failure modes/causes/effects requiring evaluation. Approximately 70 of these identified failure modes were of such significance (criticality) that corrective actions were required for mitigation. Of these 70, four resulted in design changes, 10 required major process changes, and the remainder required clarifications to reduce ambiguity. The following is a summary of key findings and recommendations:

- The majority of change recommendations were oriented toward process clarifications to reduce ambiguity. A small number of process-related failure modes resulted in design changes to mitigate the potential process failure mode.

- Good detection levels and/or low probability of occurrences mitigated potential process failure modes with high severity levels. Testability was excellent. A very high level of detectability of potential process failure modes was apparent; either in the next process step or in subsequent downstream steps.
- The use of three criticality parameters for failure mode analysis greatly improved the subjective process for evaluating the criticality of a particular failure mode. The usual MIL-STD-1629A approach uses Severity Level and Probability of Occurrence for evaluation. The UWS Process FMECA added a Detectability Level to enhance the criticality analysis.
- Even with good detectability, if the Probability of Occurrence is high, then rework will still be extensive and costly. So the use of these three parameters for criticality assessments provided a good tool to evaluate the effectiveness of processes from both a reliability and cost perspective.
- Training of shop personnel must be maintained to a high level; adequate Work Instructions are not sufficient without personnel who understand those instructions. This is especially true when turnover of personnel is extensive and high skill levels are required to build a very complex product.
- Process FMECA personnel actively participated in the Statistical Process Control and Process Qualification tasks for shops. These two tasks were coordinated to capitalize on common elements. This coordination eliminated some duplication of effort and provided both tasks supplemental input improving each respective efforts.

Lessons Learned

Lessons Learned from the usage of the Process FMECA clearly showed that the Process FMECA methodology was of great value for a high reliability military designed system. It clearly identified areas which had they not been corrected, could have compromised the system. Starting this process early in the manufacturing planning cycle is necessary to eliminate failure modes that may occur later when equipment becomes operational. The Process FMECA represents follow-on to the Design FMECA, and it is necessary to ensure a thorough examination of potential failure modes and their risks defined with corrective action applied. Lessons Learned Highlights - Process FMECA tailoring should include the following:

- Initiate the Process FMECA effort concurrently with the design activity (design/manufacturing/reliability). Insight gained at this point can help drive the selection of tooling and test equipment that is integral to the manufacturing process. This also highlights design-induced manufacturing problems.
- Begin at a generic (high) level and gradually add more detail as the design matures.
- Coordinate Process FMECA effort with the design/hardware FMECA effort.
- Develop histories for typical failure modes, failure effects, and causes that an analyst can choose from. This will standardize descriptions and terminology (especially important if several different analysts are identifying failure modes). This will also help to perform analysis tasks more quickly.
- Use relational databases which can then correlate different elements. Future efforts should be automated as much as possible (utilizing historical data as input). One

example used for this effort was the automatic calculation of the Initial and Final Criticality Numbers (the product of severity level, probability of occurrence, and detectability levels).

- Limit analysis effort to the primary failure mode/cause/effect, criticality tasks, and corrective action resolution. The level of effort should be tailored to the schedule and cost structure appropriate for each program. To be cost effective, the Process FMECA must provide results in a timely manner to manufacturing; hence the need to focus the analysis effort on critical areas.
- Closely couple the Process FMECA with SPC implementation to provide a wider view of potential process-related failure modes and to limit duplication of effort.

Value Added

The Process FMECA performed for the FDS UWS program supported the initial qualification of each manufacturing shop by helping identify critical process parameters and their controls. There is a synergy of effort associated with establishing an effective SPC process and identifying process related failure modes. Both activities looked for critical process parameters and whether these parameters are in control. These tasks improve the quality and reliability of products and eliminate costly rework.

Future of Process FMECA for Industry

The use of a Process FMECA is appropriate in any program where cost effective manufacturing, product safety, or high product reliability is required.

Cost effective manufacturing requires that processes be in control; a Process FMECA in conjunction with an SPC process supports this goal. The Process FMECA provides cost effective results by identifying criticality issues relative to detectability levels and probability of occurrence for each process failure mode. For example, a high detectability level (assured of detecting the potential process failure mode) and a high probability of occurrence results in costly manufacturing rework.

Where product safety issues are paramount or if high reliability is required, it is essential that both manufacturing processes and design failure modes be evaluated. The inherent design may have no significant failure modes; however, manufacturing processes can introduce undetected failure modes as a result of inadequate process controls (insufficient training, misunderstood process documentation/instructions or deficient processes).

References

1. Military Standards: MIL-STD-1629A; Procedure for Performing a Failure Mode, Effects and Criticality Analysis.

2. Commercial Documents: Ford System-Design-Process Handbook Worldwide Potential Failure Mode and Effects Analysis (FMEA), December 1992. Prepared by Engineering Materials and Standards Technical Affairs, Suite 700C Fairlake Plaza South, 300 Town Center Drive, Dearborn, MI 48126, Attn: FMEA Administrator.

Biography

James D. Heinz, Electronics Engineer, 5201 Leesburg Pike, Sky 3 Suite 1501, Falls Church, VA 22041, USA, telephone - (703) 681-0180 x124, facsimile - (703) 681-0184, e-mail - heinzj@ncr.disa.mil

James D. Heinz, formally of U.S. Navy SPAWAR Underwater Segment Division Director for the Fixed Distributed System, holds a B.S. in Electrical Engineering from the University of Nebraska, a Master of Science in Engineering from the Catholic University of America and is a graduate of the Defense System Management College Program Manager Course (PMC 94-1) at Ft. Belvoir VA. He is a member of IEEE, ASQC and the Project Management Institute. He is currently working in C4I related areas in DoD.

Jon A. Lumpkin, Reliability Engineering Consultant, PVA, Inc; 2260 S. Church St., Suite 506, Burlington, N.C. 27215, USA; telephone (910) 625-5832, email: jon1459@nt.infi.net.

Mr. Lumpkin is currently employed by PVA, Inc., as a Reliability Engineer. This work was performed when he was employed by Lucent Technologies Advanced Technology Systems in Greensboro, NC, as a Reliability and Maintainability Engineer, in support of Electro-Optic Underwater Hardware Development. Prior to the work he was employed by the Boeing Military Airplane Company in Wichita, KS, as a Reliability and Maintainability Engineer for aircraft systems. Jon holds a Bachelor of Science Degree in Aerospace Engineering from N. C. State University.

Brian M. Moriarty, P.E., Product Assurance Manager, TRW Systems Integrated Group (SIG), P.O. Box 10400, Fairfax, VA 22033, USA, telephone - (703) 968-1000, e-mail - Brian_Moriarty@coral.spawar.navy.mil

Brian M. Moriarty is a licensed Professional Engineer (P.E.) in Safety and Quality Engineering. Mr. Moriarty is currently the System Safety & Risk Assessment Program Manager supporting the Government Information Services Division (GISD) of the TRW SIG. He is responsible for the Hazard Analysis of the Amtrak Life Safety Improvement project for the Pennsylvania Station, New York, with the ICF Kaiser Team. He has been the Reliability, Maintainability and Availability (RM&A) Senior Engineer for the Integrated Undersea Surveillance System (IUSS) program the last nine years. Previously he was responsible as the Chief Safety Engineer for the Parsons Transportation Corp. In support of the Washington Metropolitan Authority and Transit Association (WMATA) rail transit program. He is a Fellow, current Director and past President of the System Safety Society. Currently he is Program Chair for the 15th International System Safety Conference (ISSC).

David R. Wise, Systems Quality Engineer, TRW, One Federal Systems Park Drive, Fairfax, VA 22033, USA, telephone (703)734-6670, facsimile (703) 734-6525, e-mail: David_Wise@coral.spawar.navy.mil

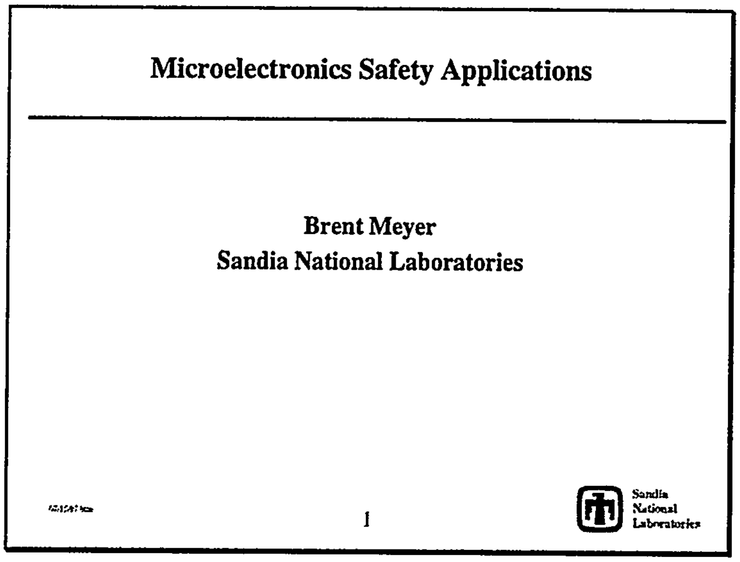
David R. Wise works for TRW as a Systems Quality Engineer designing and building fiber-optic cable systems for military applications. Mr. Wise received a B.S. Degree in Industrial Management in 1983 from Clemson University, Clemson, South Carolina, after serving 6 years in the U.S. Navy Submarine Service.

Intentionally left blank

Microelectronics Safety Applications

Brent Meyer
Sandia National Laboratories*
Albuquerque, New Mexico

Slide 1



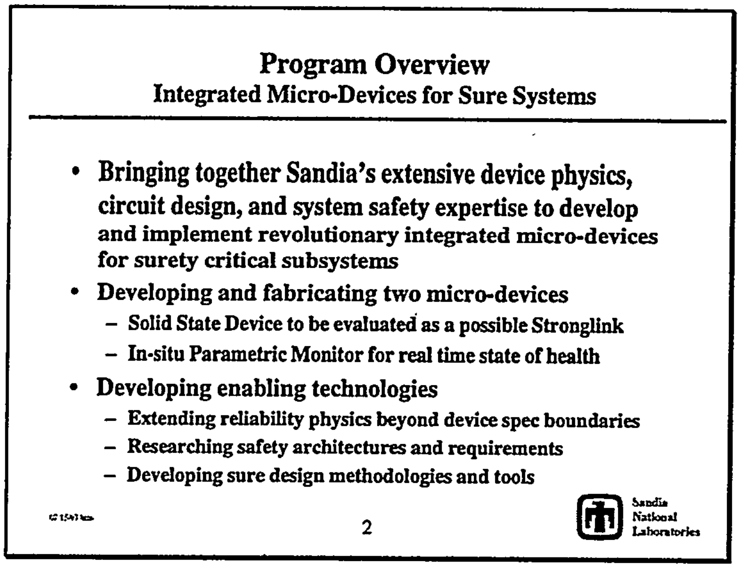
Microelectronics Safety Applications

Brent Meyer
Sandia National Laboratories

1

Sandia National Laboratories

Slide 2



Program Overview
Integrated Micro-Devices for Sure Systems

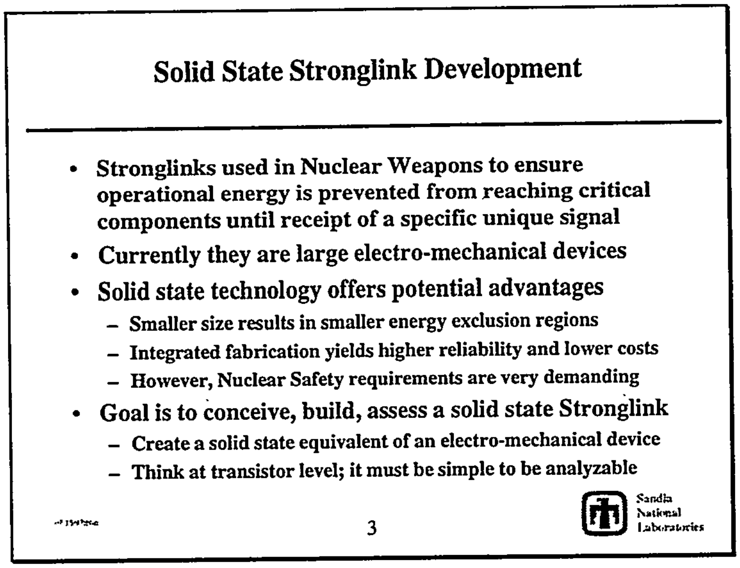
- Bringing together Sandia's extensive device physics, circuit design, and system safety expertise to develop and implement revolutionary integrated micro-devices for surety critical subsystems
- Developing and fabricating two micro-devices
  - Solid State Device to be evaluated as a possible Stronglink
  - In-situ Parametric Monitor for real time state of health
- Developing enabling technologies
  - Extending reliability physics beyond device spec boundaries
  - Researching safety architectures and requirements
  - Developing sure design methodologies and tools

2

Sandia National Laboratories

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

Slide 3



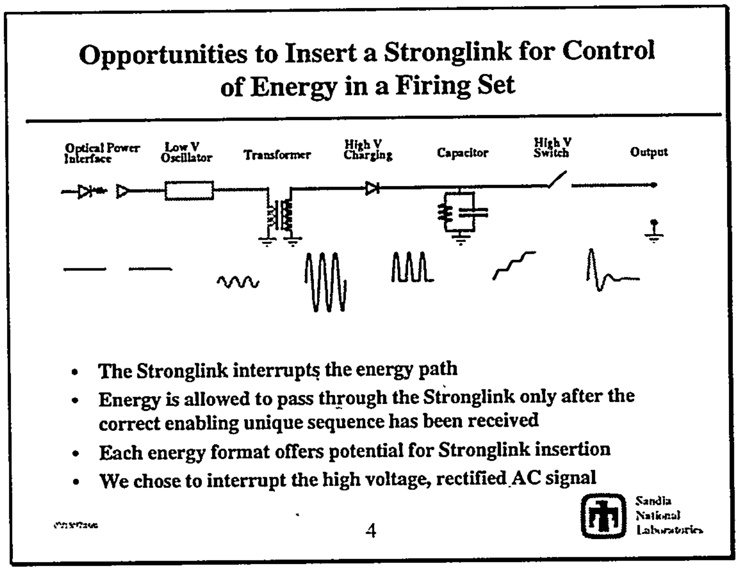
Solid State Stronglink Development

- Stronglinks used in Nuclear Weapons to ensure operational energy is prevented from reaching critical components until receipt of a specific unique signal
- Currently they are large electro-mechanical devices
- Solid state technology offers potential advantages
  - Smaller size results in smaller energy exclusion regions
  - Integrated fabrication yields higher reliability and lower costs
  - However, Nuclear Safety requirements are very demanding
- Goal is to conceive, build, assess a solid state Stronglink
  - Create a solid state equivalent of an electro-mechanical device
  - Think at transistor level; it must be simple to be analyzable

3

Sandia National Laboratories

Slide 4



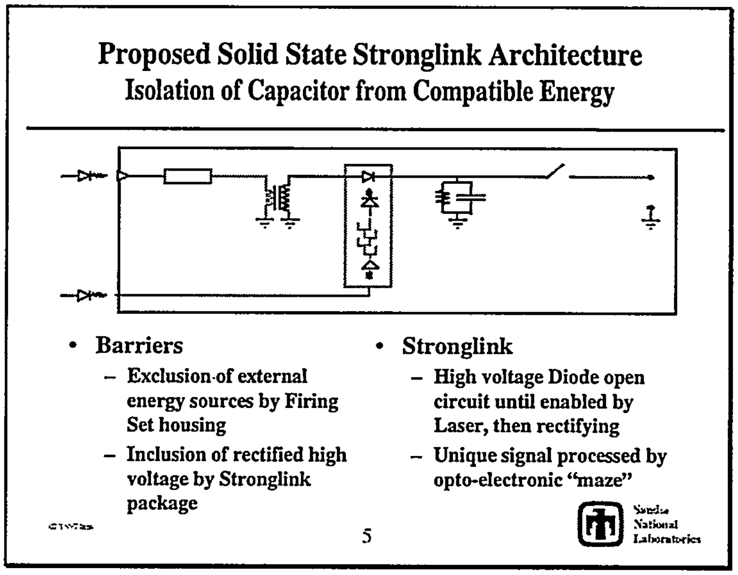
Opportunities to Insert a Stronglink for Control of Energy in a Firing Set

- The Stronglink interrupts the energy path
- Energy is allowed to pass through the Stronglink only after the correct enabling unique sequence has been received
- Each energy format offers potential for Stronglink insertion
- We chose to interrupt the high voltage, rectified AC signal

4

Sandia National Laboratories

Slide 5



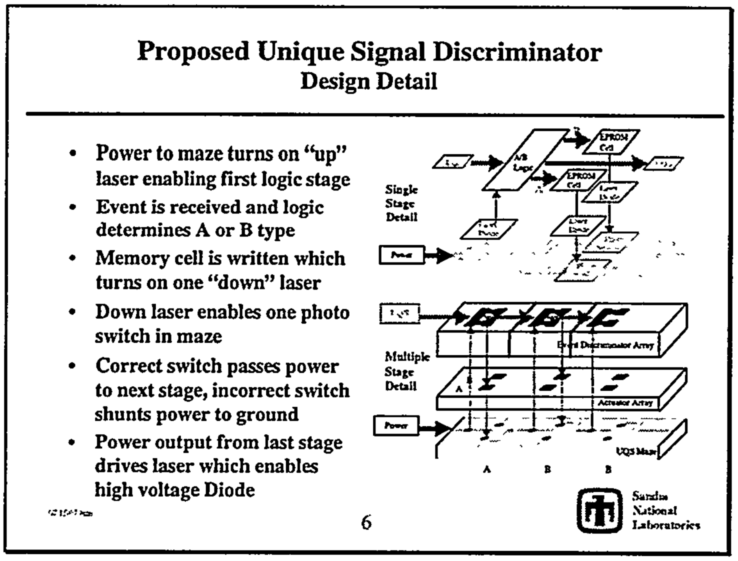
Proposed Solid State Stronglink Architecture
Isolation of Capacitor from Compatible Energy

- Barriers
  - Exclusion of external energy sources by Firing Set housing
  - Inclusion of rectified high voltage by Stronglink package
- Stronglink
  - High voltage Diode open circuit until enabled by Laser, then rectifying
  - Unique signal processed by opto-electronic "maze"

5

Sandia National Laboratories

Slide 6



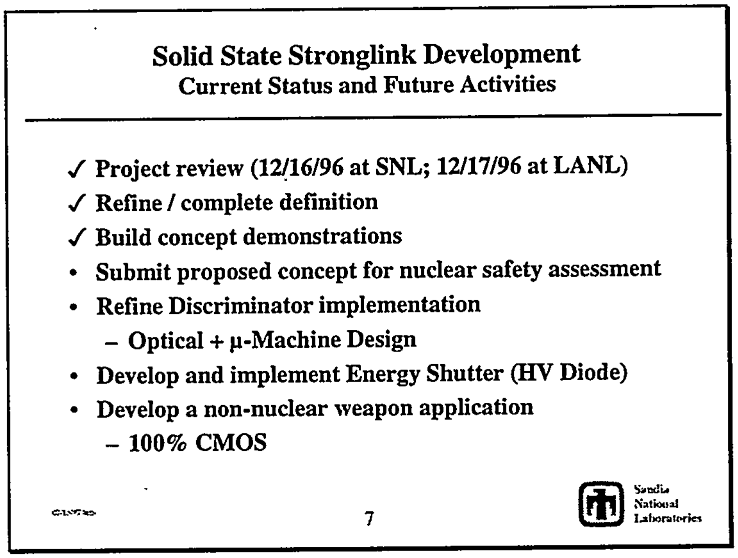
Proposed Unique Signal Discriminator
Design Detail

- Power to maze turns on "up" laser enabling first logic stage
- Event is received and logic determines A or B type
- Memory cell is written which turns on one "down" laser
- Down laser enables one photo switch in maze
- Correct switch passes power to next stage, incorrect switch shunts power to ground
- Power output from last stage drives laser which enables high voltage Diode

6

Sandia National Laboratories

Slide 7



Solid State Stronglink Development

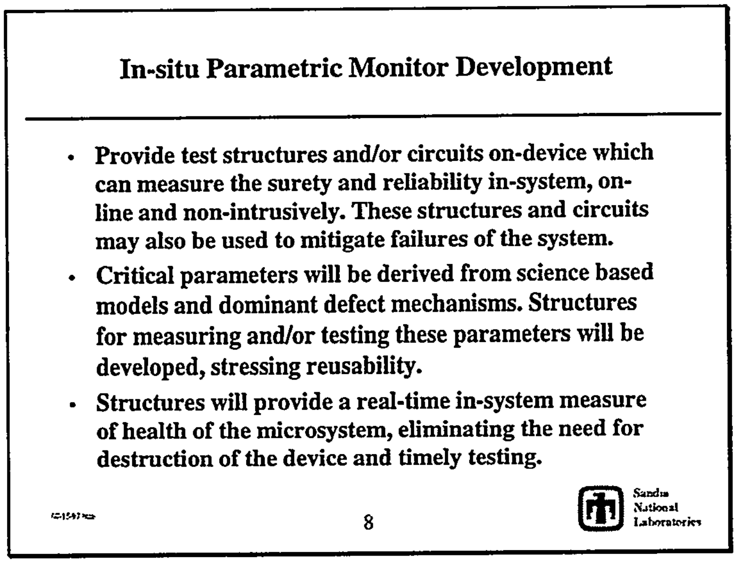
Current Status and Future Activities

- ✓ Project review (12/16/96 at SNL; 12/17/96 at LANL)
- ✓ Refine / complete definition
- ✓ Build concept demonstrations
- Submit proposed concept for nuclear safety assessment
- Refine Discriminator implementation
  - Optical + µ-Machine Design
- Develop and implement Energy Shutter (HV Diode)
- Develop a non-nuclear weapon application
  - 100% CMOS

7

Sandia National Laboratories

Slide 8



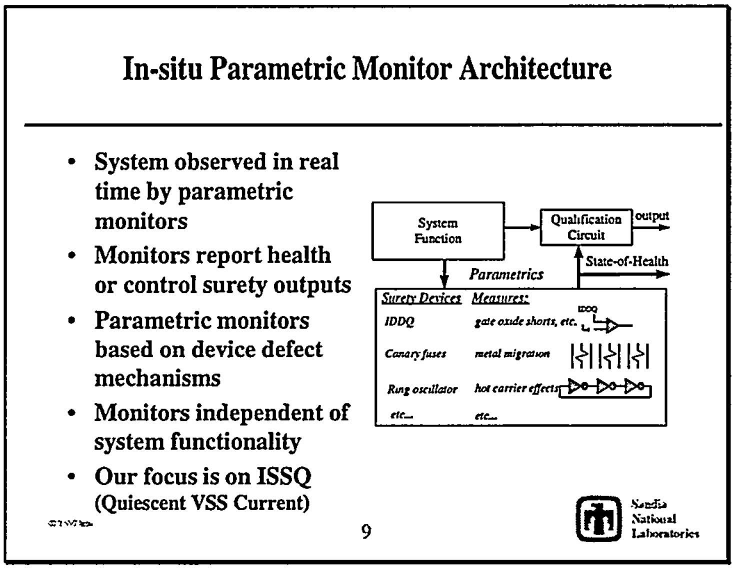
In-situ Parametric Monitor Development

- Provide test structures and/or circuits on-device which can measure the surety and reliability in-system, on-line and non-intrusively. These structures and circuits may also be used to mitigate failures of the system.
- Critical parameters will be derived from science based models and dominant defect mechanisms. Structures for measuring and/or testing these parameters will be developed, stressing reusability.
- Structures will provide a real-time in-system measure of health of the microsystem, eliminating the need for destruction of the device and timely testing.

8

Sandia National Laboratories

Slide 9



In-situ Parametric Monitor Architecture

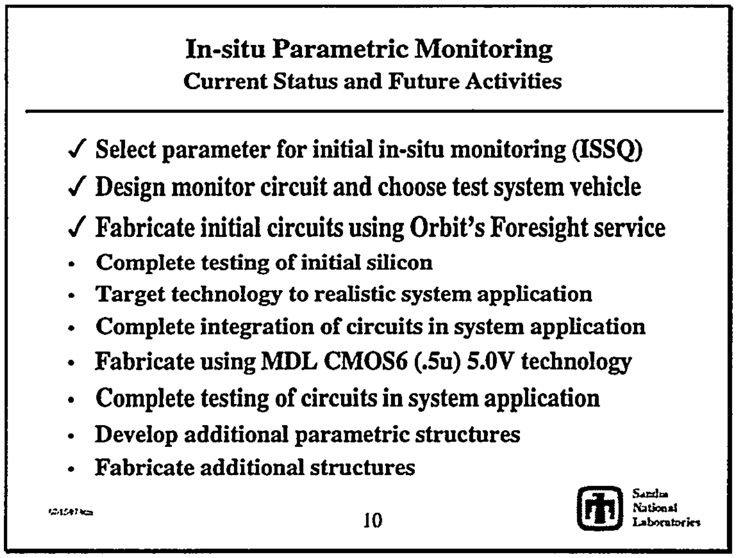
- System observed in real time by parametric monitors
- Monitors report health or control surety outputs
- Parametric monitors based on device defect mechanisms
- Monitors independent of system functionality
- Our focus is on ISSQ (Quiescent VSS Current)

System Function
Qualification Circuit
output
State-of-Health
Parametrics
Surety Devices
Measures:
IDDQ
gate oxide shorts, etc.
IDDQ
Canary fuses
metal migration
Ring oscillator
hot carrier effects
etc...
etc...

9

Sandia National Laboratories

Slide 10



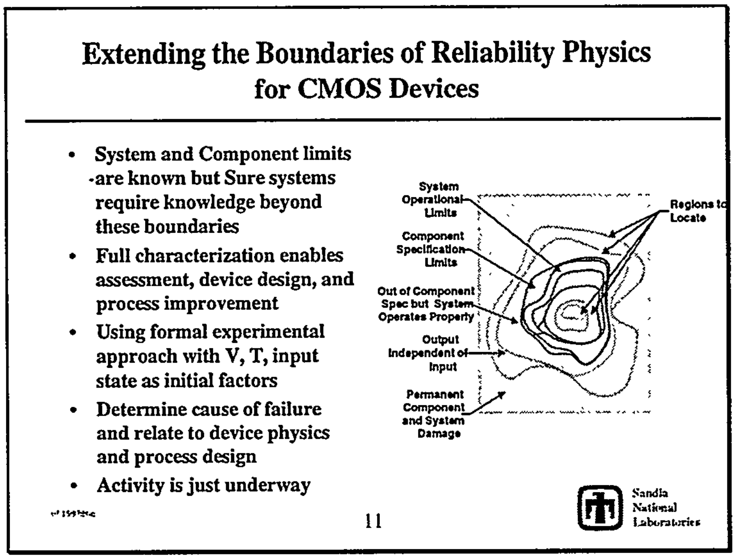
In-situ Parametric Monitoring
Current Status and Future Activities

- ✓ Select parameter for initial in-situ monitoring (ISSQ)
- ✓ Design monitor circuit and choose test system vehicle
- ✓ Fabricate initial circuits using Orbit's Foresight service
- Complete testing of initial silicon
- Target technology to realistic system application
- Complete integration of circuits in system application
- Fabricate using MDL CMOS6 (.5u) 5.0V technology
- Complete testing of circuits in system application
- Develop additional parametric structures
- Fabricate additional structures

10

Sandia National Laboratories

Slide 11



Extending the Boundaries of Reliability Physics for CMOS Devices

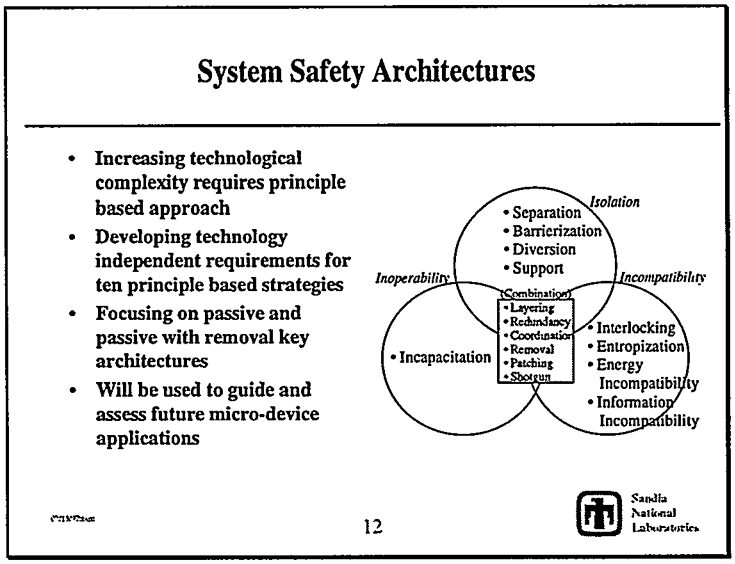
- System and Component limits -are known but Sure systems require knowledge beyond these boundaries
- Full characterization enables assessment, device design, and process improvement
- Using formal experimental approach with V, T, input state as initial factors
- Determine cause of failure and relate to device physics and process design
- Activity is just underway

System Operational Limits
Component Specification Limits
Out of Component Spec but System Operates Properly
Output Independent of Input
Permanent Component and System Damage
Regions to Locate

11

Sandia National Laboratories

Slide 12



System Safety Architectures

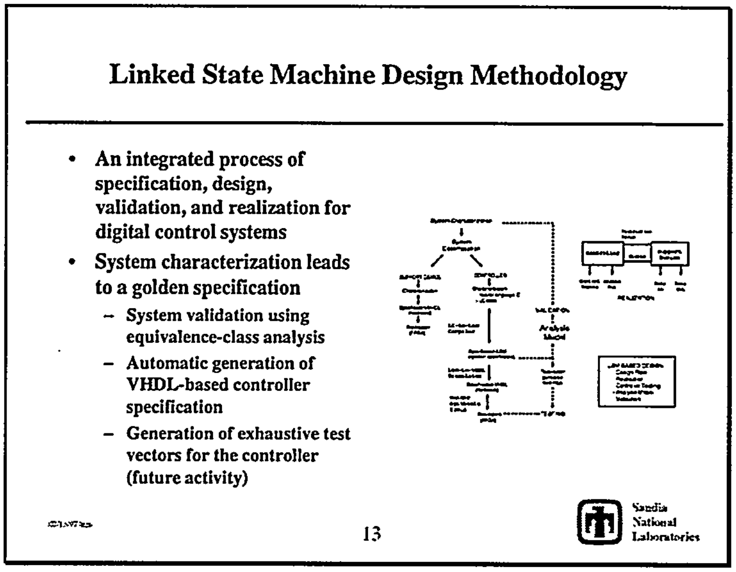
- Increasing technological complexity requires principle based approach
- Developing technology independent requirements for ten principle based strategies
- Focusing on passive and passive with removal key architectures
- Will be used to guide and assess future micro-device applications

Isolation
• Separation
• Barrierization
• Diversion
• Support
Inoperability
• Incapacitation
Incompatibility
• Interlocking
• Entropization
• Energy Incompatibility
• Information Incompatibility
(Combination)
• Layering
• Redundancy
• Coordination
• Removal
• Patching
• Shotgun

12

Sandia National Laboratories

Slide 13



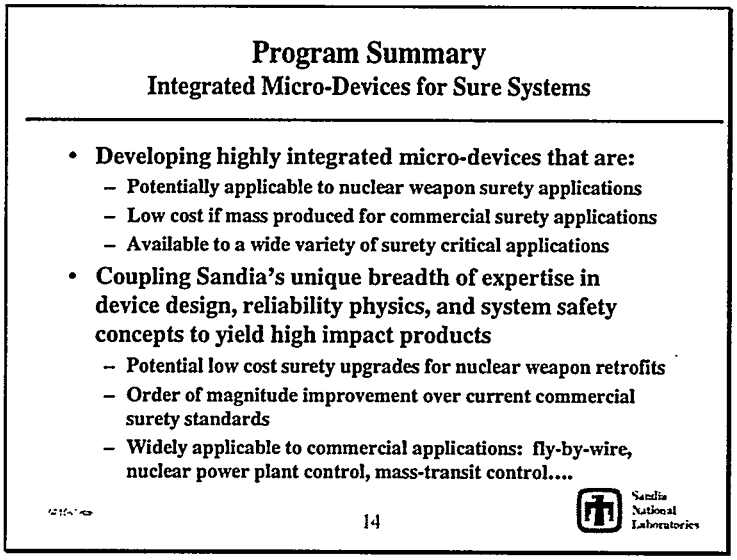
Linked State Machine Design Methodology

- An integrated process of specification, design, validation, and realization for digital control systems
- System characterization leads to a golden specification
  - System validation using equivalence-class analysis
  - Automatic generation of VHDL-based controller specification
  - Generation of exhaustive test vectors for the controller (future activity)

13

Sandia National Laboratories

Slide 14



Program Summary

Integrated Micro-Devices for Sure Systems

- Developing highly integrated micro-devices that are:
  - Potentially applicable to nuclear weapon surety applications
  - Low cost if mass produced for commercial surety applications
  - Available to a wide variety of surety critical applications
- Coupling Sandia's unique breadth of expertise in device design, reliability physics, and system safety concepts to yield high impact products
  - Potential low cost surety upgrades for nuclear weapon retrofits
  - Order of magnitude improvement over current commercial surety standards
  - Widely applicable to commercial applications: fly-by-wire, nuclear power plant control, mass-transit control....

14

Sandia National Laboratories

Intentionally left blank

Applications for Software Safety

Archibald McKinlay
McKinlay and Associates
St. Louis, Missouri

Intentionally left blank

Surety Principles Development and Integration for Nuclear Weapons

Perry D'Antonio
Sandia National Laboratories*
Albuquerque, New Mexico

Abstract

The purpose of this paper is to lay a common foundation for integrating surety elements into the design of our nuclear weapon systems and nuclear explosive operations. This foundation will be developed through the adaptation of the safety principles approach that has been used to achieve nuclear detonation safety in modern nuclear weapon designs. Identifying commonalties within these surety elements will provide a fundamental and more consistent basis for the designer and decision maker to make appropriate tradeoffs to ensure a balanced approach that will maximize the surety designed into our weapon systems and into our nuclear explosive operations consistent with operational requirements.

The focus of this paper is on achieving integrated *intrinsically sure designs* as opposed to tacking on individual elements of surety to an otherwise already-committed-to *system* design. I define the term "system" in a broad sense in that it encompasses the entire life cycle (manufacture to dismantlement) operations of the nuclear explosive assembly[1].

For this paper I will limit the discussion to the surety elements *safety, security,* and *use-control.* Standard practice, as it currently exists, is to develop these elements/subsystems somewhat in isolation from each other. Such practice can, and does, lead to design choices that do not optimize surety performance and system function with respect to other constraints. What is sought here is a common assurance and assessment basis that will rationalize the inevitable tradeoffs among surety elements and system operability such that optimum system performance is enabled.

In order to create this foundation we draw on and build from an analogy to the decades-old process for designing detonation safety into nuclear weapons. This process relies on sound philosophy and fundamental physical principles to prevent inadvertent nuclear detonation under a variety of operational and accident-related environments. I seek to adapt this process to the domain of surety, to include the elements of security and use-

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

[1] An assembly containing fissionable and/or fusionable material called Special Nuclear Material (SNM) and main high explosive parts capable of producing a nuclear detonation.

control, so that the entire system benefits from predictably sure responses to expected and unexpected stresses.

Background

Modern nuclear weapon detonation safety is the result of decades of analysis, testing, and experience that has led to a process for keeping the weapon *predictably* safe under a variety of stresses, both operational (expected) and accident-based (unexpected). The process relies on mutually supportive safety design principles that are integrated through properly implementing fundamental physical principles known as *first-principles.* The design principles of *isolation, inoperability,* and *incompatibility* form the philosophical basis for the concept of Enhanced Nuclear Detonation Safety (ENDS). The appropriate use of first-principles in the implementation of ENDS provides the assured predictably safe behavior required for nuclear weapons. It is believed that the ENDS philosophy can be adapted to the other attributes of surety, namely, security and use control to achieve a *predictably sure response* for nuclear weapon systems under expected and unexpected stresses.

Structure of This Paper

The remainder of this paper describes and illustrates the safety principles in more detail and then draws analogies as to how they collectively could be adapted to the other elements of surety and to system operation. It also describes the attendant benefit that integrated development brings, namely a rational and recognized process for developing better *system surety solutions* rather than making sub-optimal tradeoffs among the elements of surety and between surety and operability.

Safety Themes for Nuclear Weapons

A Safety Theme seeks to prevent unintended nuclear detonation and allow the system to meet operability requirements without unduly compromising safety. In developing this theme, the three principles of *isolation, inoperability, and incompatibility* are integrated into multiple *independent* safety subsystems. The following sections will describe the importance of this integration and the key role that independence plays in developing a Safety Theme.

Safety Principles

The principle of *Isolation* is first among equals in the Safety Theme. Isolation means to protect elements necessary for producing a nuclear detonation from inadvertent activation until weapon use is authorized. In early weapon designs (1950-1970s), this principle was implemented by physically separating all or some of the weapon high explosive from the fissile material. Because of operational desires or requirements in modern delivery systems this separation strategy has been abandoned (due, in part, to technology limitations as well) with the advent of sealed-pit designs. The focus has shifted to protecting the firing chain that initiates the weapon high explosive.

In modern stockpiled weapons, isolation prevents premature operation of the firing system caused by inadvertent flow of energy or information. In the case of unintended energy flow, energy is blocked or diverted from *exclusion regions* containing elements critical to the nuclear detonation process, such as a firing set capacitor or the weapon detonators.

For some weapon systems, isolation of information is still achieved through a separation strategy. That is, safety-critical information, like those signals that operate the safety devices in the weapon, is not stored in the weapon system and is only entered after proper authorization is received. For other systems, isolation of safety-critical information is achieved through the use of barriers that block the safety-critical information from the weapon.

In the weapon, isolation of unwanted energy is achieved by the use of robust barriers penetrated only by special devices known as *stronglinks* that are activated (or enabled) in the event that weapon detonation is intended. The design intent for a stronglink is that it is the only pathway into an exclusion region, for all other circumstances, it and the rest of the exclusion region barrier remain impervious to all unwanted energy sources. In practice, however, isolation is maintained in all operational (normal) environments and in low-to-moderate intensity abnormal environments, but eventually fails when exposured to high intensity abnormal environments. Because of this potential failure, an adjunct, fail-safe principle, known as *Inoperability*, is invoked to make the weapon inoperable before such levels are reached.

Inoperability is the fail-safe criterion. Inoperability relies on inherent or designed-in fragility to permanently safe the weapon before isolation is lost. Fragile elements are called *weaklinks*. They are components that are key to successful weapon detonation and are located just within the isolating barrier to experience essentially the same environments potentially threatening to bypass the isolation features. The design intent for these weaklinks is to fail irreversibly, permanently dudding the weapon, before isolation is lost.

Multiple weaklinks may be necessary to cover various types of environments (thermal, crush, etc.) or geometric considerations that could threaten isolation. In practice, however, these weaklinks may only render safe the intended detonation pathway while the physics package itself remains operational, and thus vulnerable to subsequent externally generated power sources. In addition, acceptable weaklink performance is heavily dependent on its collocation with the weakest part of the exclusion region barrier to ensure it experiences close to the same environment and thus becomes inoperable, before isolation is lost.

There is a profound benefit from the sound employment of the barrier/weaklink design. Such a design avoids the need to limit the ultimate intensity of abnormal environments and it avoids the requirement to analyze and test a bewildering array of accident environment scenarios (for example, directional threats, sequencing of environments, time races, and so on.) that would threaten the standard *ad hoc* design.

The *Incompatibility* principle uses signals or energy forms designed to be highly unlikely to be inadvertently duplicated by nature or machine in normal and abnormal environments. Nuclear weapons use this principle in two ways: (1) to prevent accidental loss of isolation by inadvertent stronglink closure and (2) to complete the nuclear detonation pathway into the exclusion region when intended. These two functions provide a better system solution by increasing system safety while maintaining system operability requirements.

Incompatibility is achieved by requiring stronglink enablement through the use of specially engineered signals known as "unique signals." Great care is required to prevent the inadvertent, premature transmission of these signals. In addition to designing in their rarity, the principle of isolation is sometimes invoked to maintain the signals within an *inclusion region* until their construction and transmission is intended.

This inclusion region is a form of isolation because it prevents the inadvertent release of safety-critical information. Like the exclusion regions, the inclusion region has a removable barrier that is designed to be abnormal-environment resistant. In practice, this barrier design has not been termed a stronglink but it does employ a design philosophy that the action to release the unique signal is abnormal-environment resistant. For example, a removable key that is stored in a separate location under a lock-wired cover.

The balanced combination of these three principles forms the basis for ENDS.

Control Themes for Nuclear Weapons

A Control Theme combines the elements of *security* and *use control* to maintain positive control over and prevent unauthorized use of nuclear weapons, yet allow timely authorized use. Security features attempt to minimize unauthorized access or loss of custody, and effectively assure that the weapon can and will be recaptured or recovered. Given access, use-control features attempt to minimize the possibility of, or delay unauthorized use, yet allow timely authorized use.

Safety/Control Theme Relationship

Security attempts to prevent or delay unauthorized access under a specified range of threats. For security, these threats are human malevolence rather than nature or inadvertent human error. In both security and safety, judgment is used to determine the credibility of these threats. A key difference between the two is that, for safety, there are consistent data, and limiting data (for example, the temperature at which the weapon carrier's fuel burns), on the accident environments for a given situation. For security, typically there are no historical data for a specific site and unless the threat is limited we cannot, in principle, prevent unauthorized access. Another way to look at this is that the abnormal environments and the sequencing of these abnormal environments are random, yet deterministic, within some known (first-principles) boundary. For example, the aircraft will eventually stop and the fire will eventually burn itself out or be extinguished. A first-principles boundary does not exist in security. The adversary can be looked at like the "Energizer Battery," it can just keep coming and coming.

Thinking back to the safety principles, one could say security focuses on the *isolation* principle. That is, the weapon is being isolated from unauthorized access rather than from energy. However, because threats greater than those specified are possible, security must also consider loss of this isolation. In safety terms, we defined the fail-safe principle of *inoperability* to address loss of isolation. So what principle do we use to address this in security? The answer is the same principle, but with different implementations that include different terminology, technology, and processes.

Translated into security terms, loss of isolation means "given access." Our fail-safe mechanism here is addressed in the use-control element of the Control Theme. That is, given weapon access, use control seeks to prevent or delay unauthorized nuclear detonation while allowing authorized use. Denial of unauthorized use is implemented by *isolating* access to critical circuits within the weapon and rendering critical components *inoperable* when unauthorized use is detected. You might say that *use-control creates a weaklink.*

Furthermore, the last part of the Control Theme, namely "yet allow timely authorized use," is akin to the second function of the *incompatibility* principle in two ways. First, use-control devices use a code that is *incompatible* with the threat, which is human. For both safety and use control, we have used engineering judgment to decide how to make the enabling signals of our safety and use-control isolating devices incompatible with the threat. Of course, the differences are that for safety we use an unclassified 24-event unique signal and for use-control we employ a shorter, but classified code. Again, these are just different implementations of the same principle.

Secondly, the "yet allow timely authorized use" portion of the Control Theme allows the system to meet its operational requirements without unduly compromising security and use-control just as in the Safety Theme.

To summarize, we have seen how the safety principles form the basis for developing both Safety and Control Themes and how these themes are tailored to maximize system surety consistent with operability requirements. Therefore, these safety principles could be renamed *surety principles* to more adequately reflect their global applicability.

How Independence Is Used in Safety

Because requirements to assure nuclear detonation safety in operational and accident environments are very stringent, multiple safety subsystems have been incorporated into modern nuclear weapon systems to avoid total dependence on a single safety subsystem.

The use of multiple safety subsystems is not specifically dictated by requirements; such use, rather, reflects engineering judgment about how best to achieve expected levels of safety (as in the Walske[2] criteria). The choice to use two or more safety subsystems allows simplifying an individual subsystem's design so that the isolation barrier-weaklink strategy has higher confidence in being ultimately successful (achieving higher reliability for the system).

These advantages come at a price, however. The safety subsystems, whether considered collectively or in pairs, must not be subject to chain-of-events coupling between subsystems or common-mode failures in which both subsystems are damaged or bypassed by the same event. Thus each subsystem must provide its safety function independently of the others; that is, each must serve its purpose even if the other subsystems are defeated, damaged, or fail.

Independence is required if two or more safety subsystems are employed, and as such, must be ranked as a supporting theme to the safety principles. As a practical matter, however, multiple safety subsystems *are* the norm and independence thus becomes critically important. Because its correct implementation requires great care, independence is a very important part of the overall Safety Theme.

Defense-in-Depth versus Independence

Security relies on what is termed "Defense-in-Depth." Once the threat and the target is defined, the designer can design the protection system that best combines elements such as fences, vaults, sensors, procedures, communication devices, and protective force personnel to best achieve expected levels of security for the system. This concept is very similar to the independence concept used in safety. In this case, independent layers of defense are employed to simplify the individual component's design so that the detect-delay-defeat strategy has higher confidence in being ultimately successful (achieving higher reliability of the system).

However, an important difference exists between the concepts of defense-in-depth and independence. For safety, the surety community has determined that two independent safety subsystems are the optimal number to meet the quantitative safety design criteria for abnormal environments, and three are optimal for normal environments. For security,

[2] The Walske criteria is named after Carl Walske, Chairman, Military Liaison Committee based upon his letter to the Atomic Energy Commission, dated 14 March 1968. That letter states that the probability of premature nuclear detonation shall be less than 1E-9 per weapon lifetime in normal environments and less than 1E-6 per accident in abnormal environments.

there is no such standard as the threat definition is ever changing - so protection schemes vary and are as unique as the unique signals themselves.

Passive versus Active Approaches

Nuclear weapon safety allows a *passive* design approach. This means that no active response is required to place the weapon into a safe state–*it starts out in a safe state and will stay safe until either the environment abates or the weapon becomes permanently inoperable.* When weaponizing the physics package, we can design the safety devices to be in an inoperable state until proper authorization is received. This is how modern stronglinks are designed. They remain in a passive, safe position until the enabling unique signal is received.

One might argue that safety uses an active approach in the design of weaklinks. For example, the Mylar in the firing set capacitor must activate or *change state* to short out the capacitor in a fire environment. However, a key concept to consider is that this change-of-state is based on *first-principles.* First principles employ the fundamental laws of nature in the chemical or physical properties of materials to assure predictable response of a designed or engineered device. In other words, "It's going to happen," or we can say the probability of the Mylar melting above its melt temperature is one. Because the weaklink capacitor has used first-principles to implement its safety function, it can be viewed as taking a passive approach.

Let us see if this first-principles law holds true for security and use-control designs that use active approaches. Security and use control both use passive and active approaches, although one could argue that the active method is the dominant approach. For example, in security, the use of fences can be considered passive, but they are only meant to delay an adversary. If these fences have sensors, their function is to detect (active) to allow the initial protective force time to respond. One could argue that the initial response force also fits into the delay bin to allow additional protective forces to respond, and so on, until control (unauthorized access is removed) is re-achieved. All these are active approaches that do not meet the first-principles law in their implementation (no guaranteed successes). **That is why security uses defense-in-depth.** There may not be a first-principles solution to regain control, but this, again, is where use-control comes into the picture.

For use-control, interruption of critical circuits in the weapon uses a passive approach (devices are open until commanded to close), while rendering the weapon inoperable is using an active approach. Because this active approach does not meet the first-principles law, use-control also relies on security and the defense-in-depth concept.

Advanced development in this area might be directed towards developing a first-principles implementation of commanded disablement, or a completely passive approach to disablement. An example of a passive approach to disablement is to deploy the weapon in a pre-disabled state and require active means to reverse the disablement before authorized use can proceed.

Other Related Topics to Consider

Surety and Operability Tradeoffs

Tradeoffs between elements of surety and between surety and operability are inevitable in the development process. Because the tradeoffs have potential impact on the performance of surety and operability functions, it is important to document the reasons behind the decisions and to estimate the residual risks the tradeoffs entail.

Factors driving tradeoffs include forced collocation of hardware, weight and volume constraints, cost and schedule requirements, replacement requirements for limited life components, operability requirements and partitioned organizational responsibilities. An example of a tradeoff between safety and operability is the decision to locate the gas transfer system outside of the exclusion region. The decision was driven largely by the operational need for ease of reservoir replacement. The decision was a tradeoff because the transfer system penetrates the barrier without the use of a stronglink gate. The residual risk is that the penetration forms a potential pathway for energy to bypass the isolation of that exclusion region barrier.

The safety concerns over such tradeoffs and other implementation concerns over performance of safety theme implementations are referred to as "soft spots." It is important to evaluate these concerns in the light of the fundamental principles that are being implemented so that confidence is gained that the safety requirements are being met.

These evaluations need to be expanded to include the other elements of surety and to begin to understand the relationships of all surety elements at the principle level. In this way, tradeoffs may more appropriately give way to better overall surety solutions.

Recapture/Recovery and ARG Operations- Are they related and do they operate under surety principles?

Security also seeks to respond to theft of nuclear weapons or SNM and compromise of classified information stored in nuclear weapons. This situation is analogous to an Accident Response Group (ARG) weapon recovery operation. In these emergency situations, the operation is never normal and the participants must react to the unique factors present. Both operations are attempting to regain *control* first and then return the balance of surety into the system as quickly as possible. After control is obtained, a surety theme is developed to again maximize the surety of the system consistent with operational requirements.

Surety Principles Applicability

I believe that the surety principles used herein have general applicability to improve surety in engineered systems other than nuclear weapons. Development and integration of a customized surety theme for these other systems will be the subject of another paper.

Summary

Table 1 summarizes the relationships among the surety principles and the themes for safety and control developed in this paper. Although this paper did not discuss reliability, a postulated reliability theme using these same principles as a basis is provided for comparison.

Biography

Mr. Perry E. D'Antonio is currently on a special one-year assignment at the Department of Energy's (DOE) Office of Weapons Surety. Prior to this assignment, he managed the System Surety Engineering department at Sandia National Laboratories (SNL). The department develops system safety engineering solutions for nuclear weapons and other industrial high-consequence operations. He holds a Masters Degree in Electrical Engineering from Stanford University. In seventeen years at SNL he has held staff and management positions in weapon systems engineering design and safety assessment, and managed a research program to improve safety technology. He is the SNL representative to the Lockheed-Martin Engineering Process Improvement Center's System Safety Subcouncil. He is a weapons safety expert in the DOE Accident Response Group. Mr. D'Antonio is currently serving as President of the System Safety Society.

Table 1. Surety Principles and Their Implementation in Safety, Control, and Reliability Themes

Surety Principle	Safety Theme	Control Theme	Reliability Theme
Isolation	blocks or diverts normal and abnormal energy in non-use operating and moderate intensity accident environments and prevents inadvertent release of critical information	prevents or delays unauthorized access or use by deceit, hiding, blocking, burying, impeding, recoding, etc.	prevents premature operation and allows reversal of isolation for intended operation (surety principles implementations must not unduly compromise operability)
Inoperability	permanently disables weapon in severe accidents (passive, or first-principles based active approaches)	prevents removal or use by disablement of weapon or its transporter (passive and re-active approaches)	no principle (surety principles implementations must not unduly compromise operability)
Incompatibility	uses types of enabling energy and information unlikely to be duplicated in non-use operating and accident environments (e.g., information unclassified, 24 events)	prevents or delays unauthorized access or use by employing secret codes (classified, <24 digits)	uses types of enabling energy and information unlikely to be duplicated in non-use operating environments but will reliably enable the weapon in intended use environments (surety principles implementations must not unduly compromise operability)
Independence	uses multiple safety subsystems; each safety subsystem must fulfill its function even if the others have been defeated	Defense-in-Depth uses multiple layered security/use control subsystems that may operate synergistically	redundancy uses redundant firing subsystems; each redundant firing subsystem must fulfill its function even if the others have been defeated

Working the Lessons Learned Process

Tonimarie S. Huning
Sandia National Laboratories*
Albuquerque, New Mexico

Paul B. Pattak
PME, Limited
Germantown, Maryland

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

Intentionally left blank

Safety Applications of Computer Based Systems for the Process Industry

Sandro Bologna
ENEA
Rome, Italy

Gustav Dahll
OECD Halden Reactor Project
Halden, Norway

Giovanni Picciolo
ENICHEM
Milan, Italy

Robert Taylor
ITSA
Glumsoe, Denmark

Intentionally left blank

Fail-safe Control for Gas Distribution Systems: The Need for Gas Protection in the Urban Environment

Ian C. Campbell
GPS Gas Protection Systems, Inc.
Maple Ridge, BC, Canada

Abstract

Gas protection systems must be improved and fully deployed to mitigate damage and protect people and buildings. Urban gas protection (UGP), which is very different from gas transmission line protection, has been justified by a variety of risk analyses. This paper considers the mounting risk presented by urban gas distribution and gas appliance systems and specifies the requirements for a high quality, cost justified gas protection system. The possible risks presented by gas distribution systems are very wide, ranging from an unprotected lethal pinhole leak at a corrosion site to multiple unprotected leaks in a firestorm over a city after a major earthquake. The first example is relatively common, and of low national consequence. The second example is of very low probability, but of very high national consequence.

At the user level there are no generally deployed gas protection systems which will automatically detect and automatically shut off the flow of natural gas or propane in the event of a gas danger, however caused. The absence of gas protection for users is a national vulnerability. Gas flow is not automatically interrupted if a building is on fire. Existing protection systems ignore threats from malevolent malefactors, either internal or external. This lack of gas protection is in sharp contrast to the rich history of electric protection. Electric protection systems are layered, coordinated and interlocked. Gas protection systems are not interlocked, simple, possibly flawed, or nonexistent. The generally available seismic protection device — a mechanical seismic valve — violates one of the foundations of electric protection theory, that the protection system operate on the direct risk (e.g. detection of methane), and not on a symptom of a risk (e.g. the vibration of the valve).

Improved gas protection systems are increasingly necessary as the causes of gas leaks and problems are becoming more threatening and as the population becomes more aware of the dangers, and as mitigation becomes a necessity for business, governments and the insurance industry. Urban gas protection will be become common as the legal risks of non-protection become recognized and new types of legal actions become possible. These new legal actions will flow from recognition that good gas protection systems are now being installed due to improvements in gas sensor and gas protection technology.

Introduction

The degrading of gas infrastructure is continuing in all countries. It is a growing, underestimated, multidimensional threat for the following reasons: first, older appliances become more risky as they pass 8000 operations or ten years in operation. Second, new furnaces may contain new sources of risks due to light weight, complexity, computer control, and economic pressures to reduce cost and vibration. Third, black iron pipes that are vulnerable to corrosion, shifting earth, or disasters like hurricanes or earthquakes supply most appliances. Alternatively, copper piping may be vulnerable to long term sulfur corrosion. In both cases, inspection standards are sometimes arbitrary and ineffective. Fourth, existing protection systems ignore threats from malevolent malefactors, either internal or external. Finally, it is outrageous that natural gas is allowed to flow freely into a burning building with no mechanism in place to automatically interrupt it. Clearly, the threat from unprotected gasses is much greater than any one act or event.

This paper summarizes some electric protection principles and contrasts these with gas protection activities and illustrates that some electric protection principles are valid for gas protection.

The Japanese and American gas fires which followed their most recent earthquakes give us examples of the major consequences of a lack of adequate gas protection. Several reasons for these failures are presented, with technically achievable alternatives. A recent Canadian gas explosion, which killed six people and injured over 20, is described and analyzed, and suggestions are made which may have reduced the tragedy.

Finally, some possible methods of economic justification are presented.

The Need for Better Gas Protection Systems

Good gas protection systems must handle all types of gas risks, however caused. By starting start with a focus on earthquake effects, as they are better documented, the foundational principles of gas protection can be discerned and are also applicable to other forms of gas risks.

Richard N. Wright, Director, Building and Fire Research Laboratory, US NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, testified before the House Committee on Science Subcommittee on Basic Research, October 24, 1995. In these hearings, he referred to the Northridge and Kobe earthquakes as "moderate," and reported on the two significant issues related to gas and fires as follows:

1. Lifeline systems, i.e., water supply and sewers, gas and liquid fuels, electric power, transportation, and telecommunication systems, are public works and utilities systems that support most human activities: individual, family, economic, political, and cultural. Disruption in services of lifelines can be devastating, as demonstrated by the aftermath of the Northridge and Kobe earthquakes.

2. Fires following earthquakes are another major hazard, particularly in urban settings such as Kobe and many major cities located in seismic regions in the United States. Failures of lifelines, such as natural gas, electric power, and water supply, both cause fires and inhibit their suppression.

The full testimony is available at on the Web at www.nist.gov/testimony/rwearth.htm.

Let us keep Mr. Wright's assessment in mind as we take a critical look at the state of gas protection.

There are no generally deployed protection systems that will automatically shut off the flow of natural gas in the event of a gas danger, however caused

There are very few gas protection systems certified for use in normal buildings in North America. These systems automatically interrupt the flow of natural gas in the event of a gas leak, or equipment malfunction -- for example a failure that generates carbon monoxide. This is true because there are very few valves and systems certified by the relevant North American authorities, American Gas Association, the Canadian Gas Association, and their wholly owned testing facilities, International Approval Services. Other North American certifying agencies report very few such systems approved. However, these devices are more common in other parts of the world, especially Europe. In North America, however, sophisticated gas protection systems only monitor and protect gas transmission lines, in contrast to a complete lack of good protection at the user level. Many underground mines and chemical industries have complex gas control and monitoring systems.

The Absence of Urban Gas Protection is a National Vulnerability

Good protection for major gas transmission lines is not a sufficient national response to all the risks presented by gas distribution across the country. In particular, existing gas protection does not address the people using gas systems. Very old and very young people are especially vulnerable but other vulnerabilities are very significant. User level protection is justified for police stations, fire halls, hospitals, emergency centers, key port facilities, key air ports, key telecommunication facilities, and other strategic assets at the corporate or national level.

This lack of gas protection is in sharp contrast to the rich history of electric protection

Electric utilities have sophisticated organizations that apply complex electric protection systems at high voltages, similar to the gas protection systems deployed by gas transmission companies. Electric protection systems use a rich array of specially designed systems, for example, over voltage, under voltage, over-current, undercurrent, reverse flow, ground current, harmonic current, differential current, under-frequency, over-frequency, and many others. This electric protection extends seamlessly down the system to the end user.

Electric protection systems are layered and coordinated

No one type of device can protect the electric system and the most cost-effective way to provide protection is through the use of a hierarchical, coordinated set of specific protections. All buildings are protected under this coordinated electric protection system, using appropriate protection technology out of a large array of possibilities. In almost all cases, the exact threat is monitored, and protection action is initiated when the risk is clearly identified. Most importantly, electric protection is mandated.

Gas protection systems are simple or nonexistent

In North America almost no buildings have automatic gas protection. Gas protection is not mandated. Some buildings use seismic valves in an attempt to provide gas protection, but this technology is open to question, as this paper will illustrate. Japan is reported to use both seismic and overflow protection devices.

Gas overflow devices do not offer good protection

Overflow devices automatically shut off gas flow in the event of excess flow, much as over-current relays detect over flows of electric energy. But just as over current devices cannot fully protect an electric system, gas overflow devices cannot fully protect a gas system. The reason is simple; the gas failures were often cracks at the threads of pipes, or at corrosion sites. There is seldom a failure that shears, or cleanly cuts, the pipe. The gas, therefore, often leaks at a slow but lethal pace, a rate of flow that is lower than the protection set point. Therefore, the protection device is ineffectual unless the failed pipe has a large hole, something that just does not often happen. Conversely, seismic valves operate to shutoff gas flow without any risk, in most cases. These valves operate if there MAY be a risk, and this false operation will happen at the exact time when false operation is most inconvenient, during an emergency when all available services will be most needed.

Seismic valves do not offer good gas protection

The generally available gas protection device, a seismic valve, violates one of the foundations of electric protection theory, that the protection system operate on the direct risk (i.e. detection of methane).

Seismic vales operate on a symptom of a risk, i.e. the movement of the valve. The seismic device used to interrupt gas lines is triggered by ground movement, which itself is not a direct threat. If seismic devices were to be widely deployed, it is possible that a large earthquake would shut down almost all buildings in a city. In North America an experienced team is required to "turn on" each building after checking all pipes for leaks, even though the probability of gas failure is low. There are few such experienced tradesmen. After a few weeks, the teams are tired and then an after shock occurs, shutting down many of the devices that have just been turned on again. It may take several months to turn on all these devices. This is a very serious problem in cold countries. The Northridge earthquake pointed out this problem very clearly. If local maintenance staff do turn on the seismic valve after an emergency, (which in North America is not lawful) they run a risk of missing a gas leak in the confusion that will exist. It is unrealistic to expect calm, repetitive surveillance by inexperienced staff of all gas pipes for several days after an earthquake? It is more realistic to expect all seismic valves to be turned on soon after an earthquake without serious inspections, as has been reported in Japan. So why have them in the first place? For these reasons some gas utilities actively recommend these seismic devices not be installed, and other professional do not recommend installation of these devices.

These types of false shutdowns with ensuing problems, or misoperation, would be considered poor protection design if they occurred in the electric industry.

Gas protection systems can learn from electric protection systems

This paper summarizes some electric protection principles and contrasts these with gas protection activities and illustrates that some electric protection principles are valid for gas protection.

There are some important principles in electric protection. One is to keep the protection system entirely separate from the associated control systems. Another is to keep the protection system simple. Another is to interrupt and secure the system after measuring the exact variable that is the threat, and not some symptom of a threat. Another is to ensure that short-circuited or open-circuited protection wiring will trigger a fail-safe operation. Experience in the electric power industry shows that interrupting service based on a symptom will cause false shutdowns. Human nature being what it is, the protection will often be "jumpered out," and made useless.

Gas protection systems need specifications

Using these principles, good gas protection system would sense the real threats, methane which causes fires and explosions, and carbon monoxide which causes poisoning. A simple, isolated system would automatically shut off the flow of gas, securing the building and people. This system would not be part of any control system; it must be a stand-alone protection system. It should fail-safe; the gas automatically shuts off if self-testing detects a problem.

The threat from uncontrolled gasses is much greater than any one act or event

The natural degradation of natural gas infrastructure is continuing in all countries; it is a growing, multidimensional threat. Here are five causal reasons to substantiate this claim.

First, older appliances become more risky as they pass 8000 operations, or ten years

Appliances must pass operational tests before they can be sold. But these appliances are not designed for an infinite life. In North America, they are often tested for 8000 operations under American Gas Association tests. This is equivalent to about ten years of normal operation. Possibly 50% of gas appliances may be older than ten years and are operating out of their certification regime. They are exploring new territory with each on-off cycle. Is the answer to replace each appliance after ten years? No, but is equally wrong to pretend that gas risks remain the same as the mechanical appliance becomes older. The correct decision is to protect assets against the increased risks posed by old appliances. The protection should be based on good principles, and should operate based on the exact threat, methane or carbon monoxide in many cases.

Second, new furnaces may contain new source of risks due to light weight, complexity, computer control and vibration

Corrosion caused in part by improper installation is a serious modern risk. An additional risk is that gas appliances are being designed tighter to their requirements, as a natural consequence of business competition. Therefore, it is easy to expect more frequent failures of new appliances after the expiration of the gas appliance warranty has expired. What is the threat? Methane and/or carbon monoxide are more lethal than water and/or a tripped circuit breaker, the natural consequence of a hot water tank failure. For the water tank, there is provision to protect the electric system and to control the water after a failure of a hot water tank. Similar protection is needed to protect against gas accidents for gas appliances.

Third, vulnerable pipes supply most appliances

Black iron pipes are inflexible and vulnerable to fracture under building collapse caused by natural disasters like hurricanes or earthquakes. Copper or other pipes are also vulnerable, possibly to corrosion caused by sulfur in natural gas. Although high-pressure piping is welded, and if properly monitored, safe for many years, connections to appliances are by black iron threaded pipe, or by copper.

Black iron, plastic or copper piping all have weaknesses with respect to corrosion, shock, shifting ground soil, floods, earthquakes or other natural disasters. No appliance control system can protect against these failures any more than an electric motor protection system can protect electric distribution lines. Purposeful, hierarchical protection is needed for electric and gas distribution systems.

Fourth, existing protection systems ignore threats from malevolent malefactors, either internal or external

This type of threat is beyond the scope of this paper. However, threats exist at user sites that are not addressed by existing gas distributions systems.

Fifth, gas flows freely into building even when the fire system knows the building is on fire

Finally, natural gas should not be allowed to flow freely into a burning building. It should be automatically interrupted in case of a fire. This interruption should not be at the appliances but outside the building at the service entrance.

Many ordinary citizens of North America falsely believe that natural gas flow is shutoff by the fire alarm system as soon as a fire is detected. In some cases, fire fighters do not start fighting fires until after the gas company has been summoned, and manually turns off the gas. How will gas be shut off in a fire after an earthquake? The clear answer is -- it will not happen unless it happens automatically with a gas shutoff valve.

Major gas fires result from inadequate gas protection systems

The Japanese and American gas fires which followed their earthquakes are us an example of the major consequences of a lack of adequate gas protection. Several reasons for these failures are explored and technically achievable alternatives are offered.

These failures were detailed in a Statement of Richard N. Wright, Director, mentioned earlier in this paper. Here are six of his findings that relate to fire and gas protection after studying the Kobe situation:

1. There is a need to focus on the issue of fire following earthquakes. In Kobe, while there was no firestorm, there were 380 ignitions, and often no water to suppress them. Water purveyors and fire departments should review the vulnerability of water supplies. Recent earthquakes have shown that there is a low probability of maintaining a water system following an earthquake unless systems are designed and constructed, or retrofitted, for earthquake resistance.

2. Consideration should be given to identifying and developing alternate supplies. Similarly, the use of monitoring and control systems should be considered to enable timely cutoff of a broken water system to save water in reservoirs for subsequent fire fighting.

3. An important lesson learned from this earthquake is the need to coordinate the restoration of electric power with an assessment of the state of gas system repair. It appears that premature restoration of electric power in areas of Kobe with leaking gas contributed to additional fires.

4. The difficulty and substantial time required for restoration of gas service in Kobe is an important reminder of the complexities and resources required for the resumption

of gas supply after large-area shutdowns. Restoration of gas can be especially critical in U.S. areas with cold winter weather. It may be advantageous to provide for remote control and other rapid means of isolation of smaller, more manageable areas of the gas system.

5. The extensive damage to vulnerable piping is a very important lesson and a sobering reminder of potential earthquake effects on weak systems. Although threaded steel piping is used rarely in U.S. gas systems, many U.S. systems do use cast iron mains for low-pressure distribution, which are vulnerable to earthquakes.

6. Passive fire protection systems were effective in stopping fire spread. A major earthquake overwhelms the capabilities of fire departments and public service rescue organizations. Homeowner self-help needs to be part of disaster response.

Responsible gas protection systems must respond to these finding with positive, focused action. This protection is especially necessary for threaded black iron pipe, which is usually used inside users' buildings. Clearly any action taken to prevent fires immediately after any natural disaster is critical to reducing demands on water supply, electric operations, and the reduction of risks of a firestorm. The interactions of these water, electricity and gas systems require attention. Improving any one system contributes to the integrity of the others. Conversely, the level of protection in the gas system should not degrade the integrity of the water or electric systems. This requirement calls for a higher standard of gas protection, equal to electric protection.

Neither seismic nor excess flow devices protected Kobe against serious gas fires, and there was little protection in Northridge. The Kobe seismic and overflow devices did not detect the real threat -- a problem guaranteed to occur again, even if seismic valves are used. Some other areas of Japan are reported to have no protection, similar to North America. The lack of protection in Northridge, characteristic of the North American situation, did nothing to prevent serious threats from escalating into real fires and explosions. It is important to apply the key principles of electric protection to gas protection, and perform automatic shutoff of gas flow after detecting hazardous levels of carbon monoxide or methane, or LPG. The protection system should be a simple, stand-alone system, and protect all the buildings and people, not just some appliances. Ideally the protection equipment itself will be fail-safe, and will shut off gas flow unless self-tests are satisfactory.

A recent Canadian gas explosion, which killed six people and injured over 20, may have been avoided

In April 1997 a gas explosion rocked the small community of Quesnel, British Columbia, Canada. The cause is reported to be a leak in the gas distribution line caused by shifting soil. Gas may have leaked out of the line, filtered through the soil, and into an apartment and commercial building. There is confusion about whether gas was smelled, reported or investigated. There is a suggestion that the odorant (which is artificially introduced into the natural gas as a safety measure) had leached out as it passed through the ground. The natural gas, which in its natural state is odorless, colorless and undetectable by humans, gathered until it acquired an ignition point and then exploded.

A gas protection system may have prevented this explosion by alarming and shutting down the flow of natural gas into this building even if the leak was outside the building and upstream of the automatic valve for the following reasons: the visual and audible alarm and subsequent shutoff of gas would have been a very serious signal to occupants, who would have called the gas company and said "we have a gas leak in our building." The building would have been evacuated; the problem would have been investigated sooner. In addition, the gas pilot lights, a main source of ignition for any accumulation of gasses, would have been extinguished possibly giving occupants several more hours to evacuate. This is an example of "good " gas protection theory giving better than expected protection. It is clear that neither overflow nor seismic devices could have given this added protection for an "upstream" leak.

Insurance problems relate directly to gas distribution risks

Canadian insurance sources estimate that a major earthquake will result in over $35 billion in damage for the heavily populated greater Vancouver area of British Columbia. Some experts claim that over six to ten billion dollars of earthquake damage may be caused by secondary fires and explosions, many related to gas. These damage estimates come from the Insurance Bureau of Canada, and were estimated in 1992 by a reinsurance company.

Newspaper reports claim the insurance reserve for earthquake claims is about $4 billion. Therefore, there is public speculation that some organizations that think they are protected may possibly be faced with a bankrupt insurer after a large earthquake.

However, if proper gas protection technology was in place and fire damage is mitigated, the required reserves would be significantly reduced, creating a real amelioration of this insurance problem. Automatic gas shutoffs become more important when it appears that many managers responsible for facility management, and manually shutting off gas valves in an emergency, do not actually know where the gas runs through their building, or where the manual gas shutoff valve is located. This fact indicates they will not be reliable or responsive in a gas emergency.

Automatic gas shutoff will assist recovery of buried persons. Most professional or amateur rescuers will not enter a collapsed building while they smell gas. Therefore automatic gas shutoffs will save lives by allowing rescue operations to be mounted sooner, giving critical assistance when most needed.

Other nations probably face similar problems, and could benefit from similar protection. Lest we forget the enormous costs, the Kobe earthquake is reported to have cost 5300 fatalities, 26,000 injuries, over 200,000 homeless and $200 billion in damage. These figures come from Richard N. Wrights's statement, cited earlier.

These costs are small compared to the 20,000 possible deaths in a significant US earthquake. "Estimating Losses From Future Earthquakes" National Research Council

NATIONAL ACADEMY PRESS D.C. 1989 was prepared for the Federal Emergency Management Agency under contract No. EMW-86G-2366 to the National Academy of Sciences It forecasts the loss of U.S. life in a significant earthquake at 20,000 (Page x of the Preface) and implies that cities outside California may be more vulnerable to damage because they are less prepared. Seattle and Boson are mentioned as two cities in which significant damage may occur. A significant part of these fatalities is related to fire and gas incidents. The report estimates that 70 million U.S. citizens are at risk from serious earthquakes.

The full report is on the Web at
http://www.ul.cs.cmu.edu/books/estimating_losses/esti001.htm

A design goal for gas protection systems is to reduce by 10% of each of these problems, i.e. for a similar, moderate earthquake at Kobe to save $14 billion, 20,000 homeless, and 2,600 injuries and 500 fatalities. It should be possible to extend existing earthquake simulation studies to investigate the design specifications and operational requirements in order to achieve these benefits.

A technically feasible partial solution to these problems is possible

Gas protection, based on the principles presented in this paper, has recently become available. It has been certified for use in North America by the American Gas Association and by the Canadian Gas Association.

Gas protection systems are financially viable

Various government organizations in British Columbia are investigating gas protection on both policy and pilot levels. The province has acknowledged its need to protect its strategic infrastructure against gas threats, especially those related to earthquakes. Fire and police stations, transportation and energy centers, emergency response centers and other government assets were specifically identified as needing protection. The Ministry of Finance, Risk Management Branch, has written a letter advocating the use of gas protection in all government buildings. The Purchasing Commission has issued a standing purchase order to encourage schools, hospitals, and other public bodies to move in the direction of gas protection. A suburban city plans to move to protect all that city's buildings from gas risks. The Corporation of Maple Ridge is continuing a phased plan to protect its buildings against gas threats. The BC Housing Corporation, a social housing agency, has started a pilot project to protect all its buildings.

Types of buildings protected or planned to be protected in the near future include: fire hall, police station, emergency response center, hospital, city hall, operations center, social housing, senior's accommodation. Other building types being investigated include skating rinks (which double as morgues or food distribution centers in community emergency plans), a museum, office buildings, schools, storage facilities and transportation facilities.

Other organizations in the Vancouver area, both public and private, are in process of reevaluating their gas protection needs, and performing risk analyses. These risk assessments may be qualitative, or quantitative. Either approach appears to result in justification if all relevant considerations are covered. On the other hand, a superficial analysis, which underestimates the threats and benefits, will often result in a decision to forego gas protection.

Background to mitigation and some economic justifications

Strategic Buildings should be protected first.
All gas protection applications to this date are to strategic assets. Benefits due to mitigation are most obvious when the most strategic assets are protected. Buildings are considered strategic because of the operations conducted inside the building, and not only because of the value of the building itself. This is quite different from an insurance viewpoint, which often considers replacement value. Financial and economic operations are often very valuable and need to be protected from interruption in operations, especially in an emergency.

A seismic upgrade does not give invulnerability.
One urban gas protection system was justified during a seismic upgrade to a fire hall. Seismic upgrades to older buildings are common in earthquake areas. After a building has been strengthened the owners may falsely believe they are relatively invulnerable to earthquake damage to a certain severity, and structural appear to engineers may imply this. This is wrong because almost all seismic upgrades ignore the gas danger, and only provide structural strengthening. For a very modest additional investment the gas risk can, and should, be mitigated so the owners of the buildings achieve relative invulnerability from earthquake damage and not just protection from structural failure. Full service mechanical engineers may be able to recommend both structural and gas protection.

Buildings built to modern seismic standards do not include protection from gas risk.
An urban gas protection system was justified for construction of a new fire hall, which included the most modern seismic codes. The owners required gas protection in addition to structural protection.

Old buildings that cannot receive structural upgrades may benefit from gas protection.
A series of fire halls that cannot be seismically upgraded because of budget restrictions is being considered for gas protection. This alternative is much more cost effective than structural strengthening, and provides a real benefit. This benefit may be within budget constraints.

Seismic protection replaced by gas protection.
A hospital has recommended that its seismic valve protection be replaced by gas protection. The risks to elderly patients and staff were better mitigated by gas protection than by seismic protection and the incremental costs were considered relatively small.

Gas protection was justified for a social housing project.
Legal liability issues played a part in justifying gas protection for a series of social housing projects.

Other justifications.

Most justifications to date have been qualitative, and not quantitative. Quantitative analyses are available and show advantageous benefit/cost ratios for most, but not all, buildings.

Appendix A is an example of a checklist useful for conducting a Financial Viability for Urban Gas Protection.

Financial justification appears easier in moderate sized organizations, although the objective risks appear higher in larger organizations and the benefit/cost ratios seem much more attractive. Fuzzy corporate commitment to spending money on safety and risk management, unwillingness by middle management to take risks (ironically) with a "new" technology and social shirking appear to be factors in this resistance by larger organizations.

Future real time monitoring is planned for earthquake damage and mitigation.

Gas protection can be enhanced by long distance monitoring of gas valve operations. If all automatically operated gas valves signal their operation to satellites, earthquake damage to natural gas systems could be monitored as it is detected. This damage may be a sensitive reflection of all serious earthquake damage, and may assist in deploying many resources as rescue operations begin. This type of exception monitoring can be relatively inexpensive; perhaps as little as $5 per month per point. At such an inexpensive rate, cost justification may be easy. It could include water monitoring also.

An inexpensive, battery operated radio could receive emergency reports, directly from and to each municipality from Mexico to Alaska, for example. Each municipality could decide whether to offer or request assistance based on this direct data, which would be obtained independently of local telephone or electric power. Some municipalities view this possibility as valuable and exciting.

This monitoring will be useful in coordinating gas and electric operations during the recovery phase after an earthquake, and could even be used to shutdown remotely entire section of a gas distribution system if a fire storm is threatened or in progress. At certain times of the year, and in dry locations, this option could possibly save thousands of lives.

Conclusions

User oriented gas protection systems must be improved or gas related tragedies will become more frequent. Eventually gas protection will become mandatory, as electric protection is mandatory, and for much the same reasons. In particular, it will become less acceptable for the public to be exposed to gas risks because they are in a building without gas protection. Currently, such a situation is unthinkable with respect to electric protection where unprotected buildings are declared unsafe in all modern jurisdictions.

Further work is needed to confirm and refine the numbers quoted in this report, and to estimate the benefit to society of the protection and monitoring concepts identified in this paper.

The trend to improved gas protection systems will continue as gas leaks and problems are becoming more threatening and as the population becomes more aware of the dangers, and as mitigation becomes a necessity for business, governments and the insurance industry. The general population is concerned with personal risk, health and welfare, and the protection of infrastructure. Large organizations are concerned with self-preservation after a catastrophic gas fire or earthquake.

Urban gas protection will be accelerating as the legal risks of non-protection become recognized and new types of legal actions become possible. These new legal actions will flow from recognition that good gas protection systems are now being installed due to improvements in gas sensor and gas protection technology. Consequently organizations without some effort towards gas mitigation and protection may eventually find themselves at legal risk if some gas accident occurs in their facilities.

Appendix A. Financial Viability for Urban Gas Protection

Checklist for analysis.

1. Name of Organization:
   (Note: This should be a Strategic Business Unit with relatively well-defined products and/or services, customers, suppliers and possibly after sales services.)

2. Please describe types of customers:

3. Please describe types of suppliers:

4. Please describe products and/or services, including after sales service.

5. Are you aware of gas fires, explosions or gas poisonings in your industry? If so, briefly describe the damage:

6. What earthquake zone are you in? Do you have a community duty to provide services after an earthquake? Does your organization need seismic upgrading? After upgrading do you think you are relatively invulnerable from earthquake risk?

7. Do you personally know where to turn off the gas in an emergency in the building you are now seated in? who does? Where are the tools to turn the equipment off in each strategic building? Are they locked up? What percentage of the 8760 hours in the year is covered by trained personnel? If they are on duty, how do you know they will be reliable immediately after a serious disaster?

8. Please list your organization's five most strategic business processes
   (Note: usually invoicing and collections are counted as one process for this study)

9. Please list your organizations five most strategic operational assets.

10. Please list any backup processes or assets that are available to continue business operations in the event of severe damage to any of the processes or assets listed in 8 and 9.

11. After a severe natural disaster, or gas leak, what plans does your organization have to ensure continuity of all strategic processes and assets? Do the plans include gas protection? If so, how?

12. How will your business be able to survive a serious gas incident? Do you want to do a quantitative analysis to support your position? If so, phone 1-604-467-2625.

13. If the cost of gas protection is about 10 cents per person per day, or the cost of one cup of coffee for each employee per day, or the cost of two unnecessary copies per

employee per day, how can you NOT justify gas protection as a strategic benefit that will contribute to organizational survival after a gas leak or natural disaster?

Biography

Ian C. Campbell, MBA, P.Eng.
GPS Gas Protection Systems Inc.
11686 Holly Street,
Maple Ridge, BC,V2X 5H1 Canada

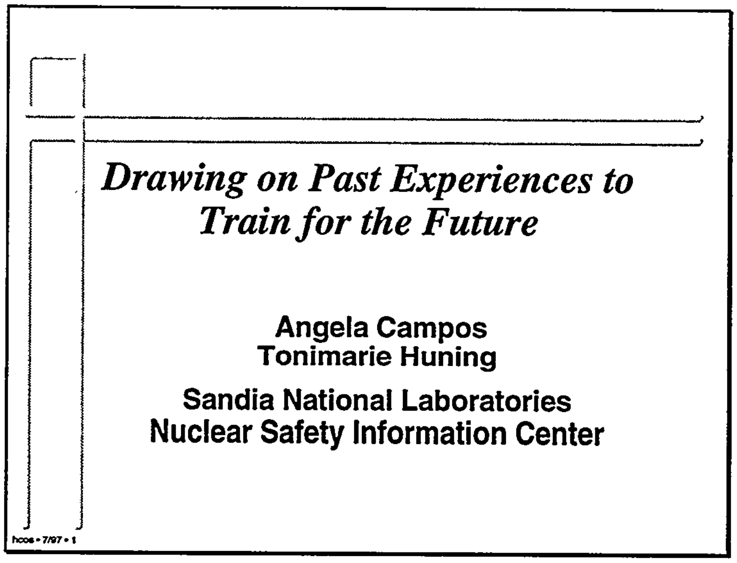
Mr. Campbell is CEO of GPS Gas Protection Systems Inc. He has worked as an Electric Protection Systems Engineer for Canadian General Electric Co. LTD, as Chief Engineer for Lamb Cargate Industries LTD developing gassifiers for the forestry industry, and as VP and Assistant to the President of Lamb Grays Harbor Co, a premier pulp and paper equipment supplier. His MBA is from Harvard University, and he is a registered engineer in Ontario, Canada.

Intentionally left blank

Drawing on Past Experiences to Train for the Future

Angela Campos
Tonimarie Huning
Sandia National Laboratories*
Albuquerque, New Mexico

Slide 1



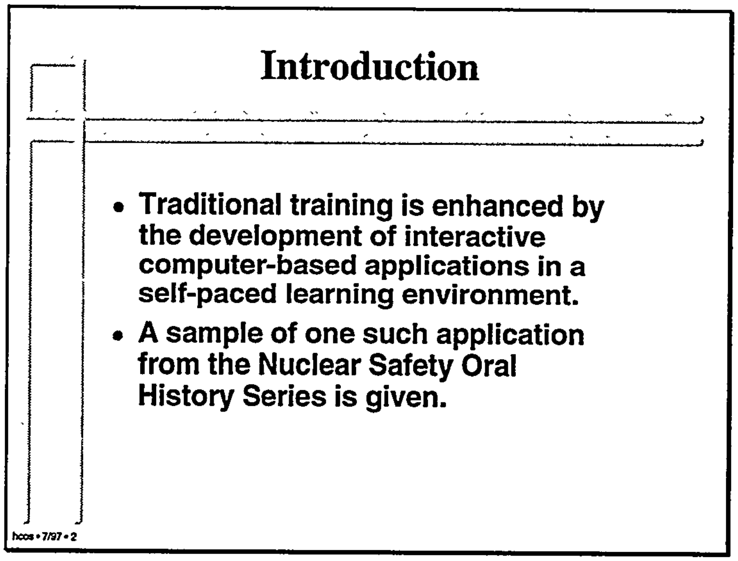
Drawing on Past Experiences to Train for the Future

Angela Campos
Tonimarie Huning

Sandia National Laboratories
Nuclear Safety Information Center

hcos • 7/97 • 1

Slide 2



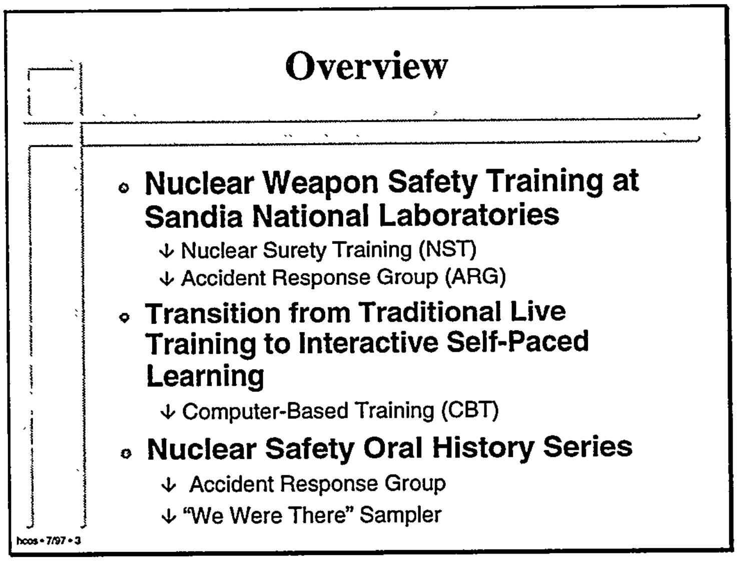
Introduction

- **Traditional training is enhanced by the development of interactive computer-based applications in a self-paced learning environment.**
- **A sample of one such application from the Nuclear Safety Oral History Series is given.**

hcos • 7/97 • 2

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

Slide 3

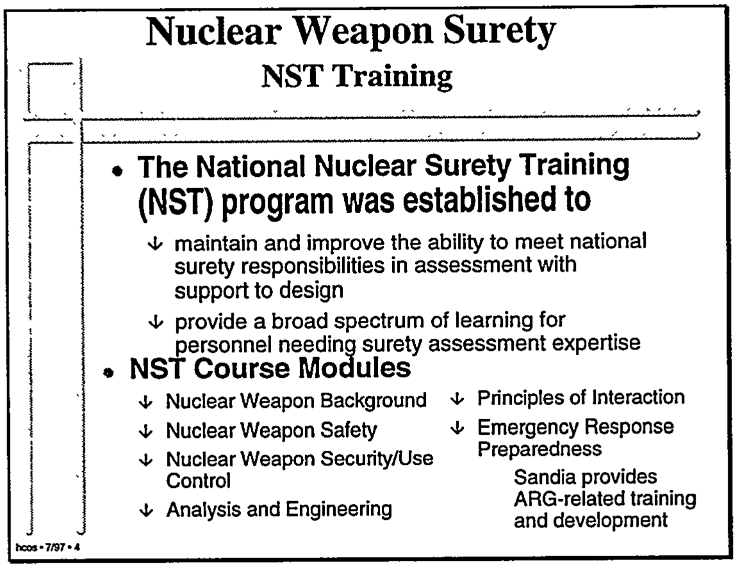


Overview

- Nuclear Weapon Safety Training at Sandia National Laboratories
  - Nuclear Surety Training (NST)
  - Accident Response Group (ARG)
- Transition from Traditional Live Training to Interactive Self-Paced Learning
  - Computer-Based Training (CBT)
- Nuclear Safety Oral History Series
  - Accident Response Group
  - "We Were There" Sampler

hcos • 7/97 • 3

Slide 4



Nuclear Weapon Surety

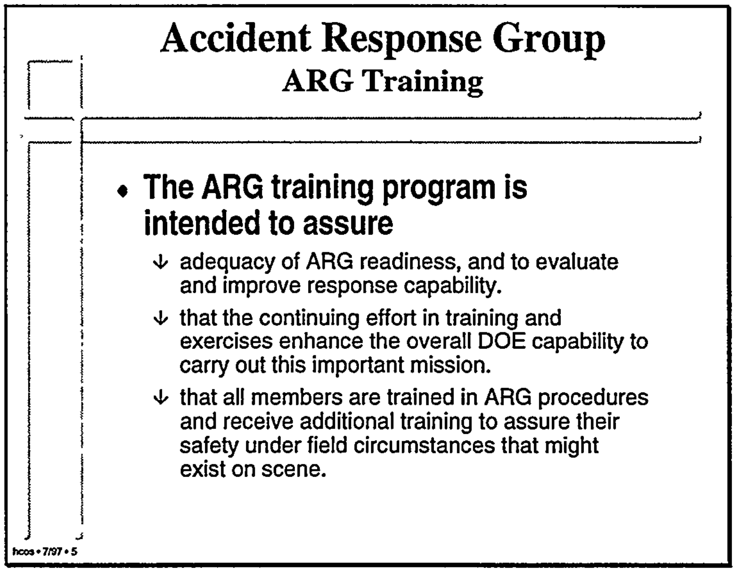
NST Training

- The National Nuclear Surety Training (NST) program was established to
  - maintain and improve the ability to meet national surety responsibilities in assessment with support to design
  - provide a broad spectrum of learning for personnel needing surety assessment expertise
- NST Course Modules
  - Nuclear Weapon Background
  - Nuclear Weapon Safety
  - Nuclear Weapon Security/Use Control
  - Analysis and Engineering
  - Principles of Interaction
  - Emergency Response Preparedness

    Sandia provides ARG-related training and development

hcos • 7/97 • 4

Slide 5



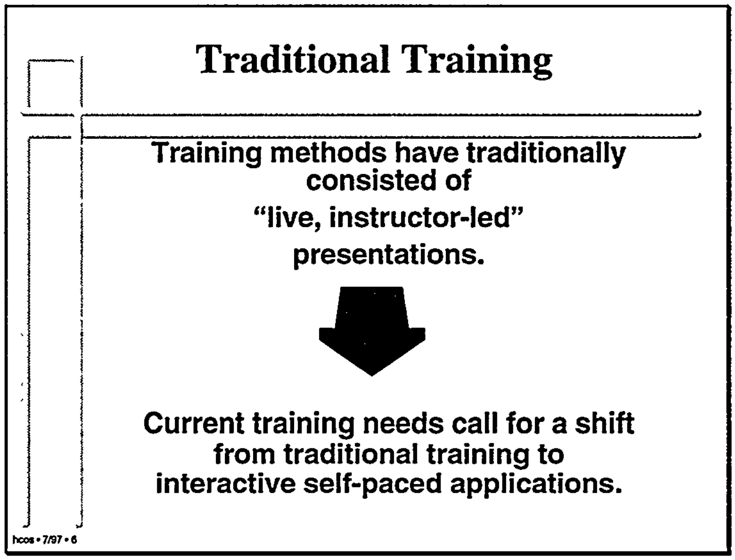
Accident Response Group

ARG Training

- The ARG training program is intended to assure
  - adequacy of ARG readiness, and to evaluate and improve response capability.
  - that the continuing effort in training and exercises enhance the overall DOE capability to carry out this important mission.
  - that all members are trained in ARG procedures and receive additional training to assure their safety under field circumstances that might exist on scene.

hcos • 7/97 • 5

Slide 6



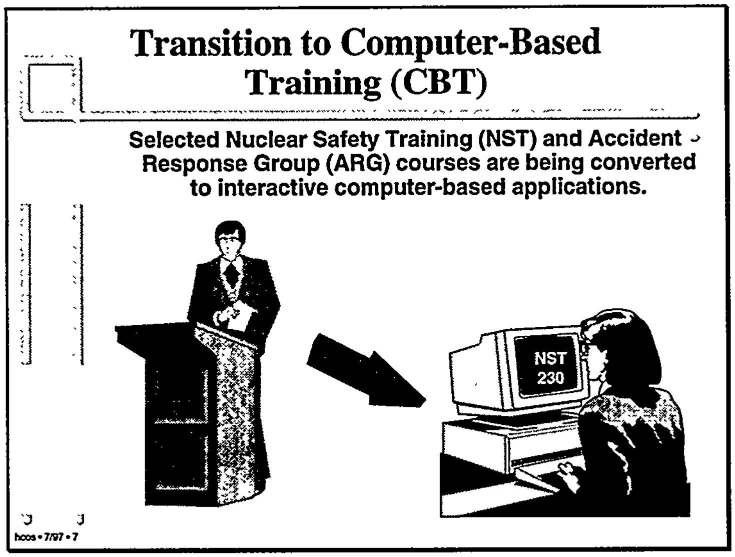
Traditional Training

Training methods have traditionally consisted of "live, instructor-led" presentations.

Current training needs call for a shift from traditional training to interactive self-paced applications.

hcos • 7/97 • 6

Slide 7

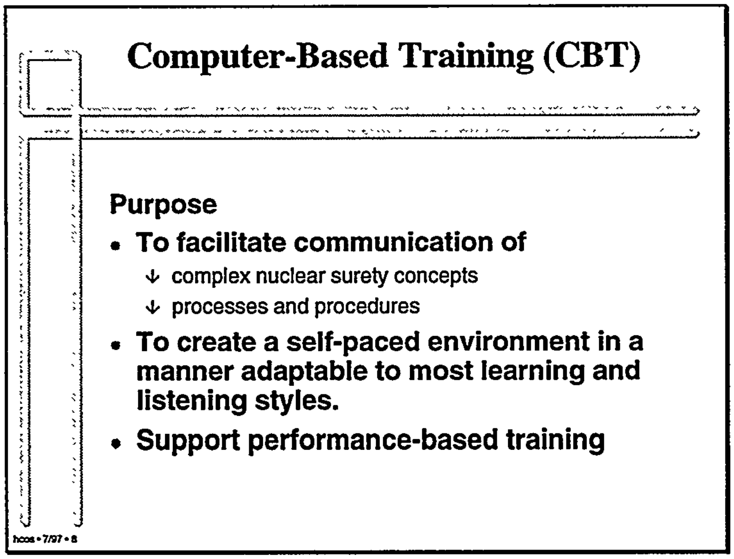


Transition to Computer-Based Training (CBT)

Selected Nuclear Safety Training (NST) and Accident Response Group (ARG) courses are being converted to interactive computer-based applications.

hcos • 7/97 • 7

Slide 8



Computer-Based Training (CBT)

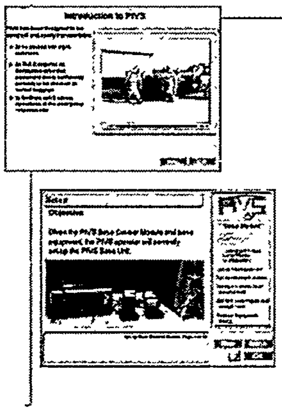
Purpose

- To facilitate communication of
  - complex nuclear surety concepts
  - processes and procedures
- To create a self-paced environment in a manner adaptable to most learning and listening styles.
- Support performance-based training

hcos • 7/97 • 8

Slide 9

Computer-Based Training (CBT)



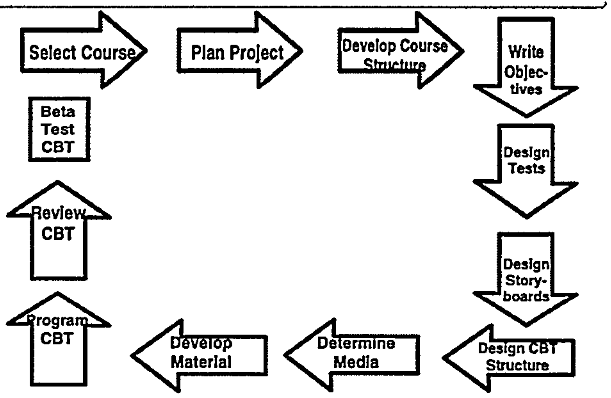
- **The intent of this activity is to**
  - ↓ integrate multimedia tools into capabilities that strengthen our ability to manage and provide nuclear safety information in the most efficient means possible.
  - ↓ incorporate more complex multiple messages into content-rich and logic-based computer applications.

hcos • 7/97 • 9

Slide 10

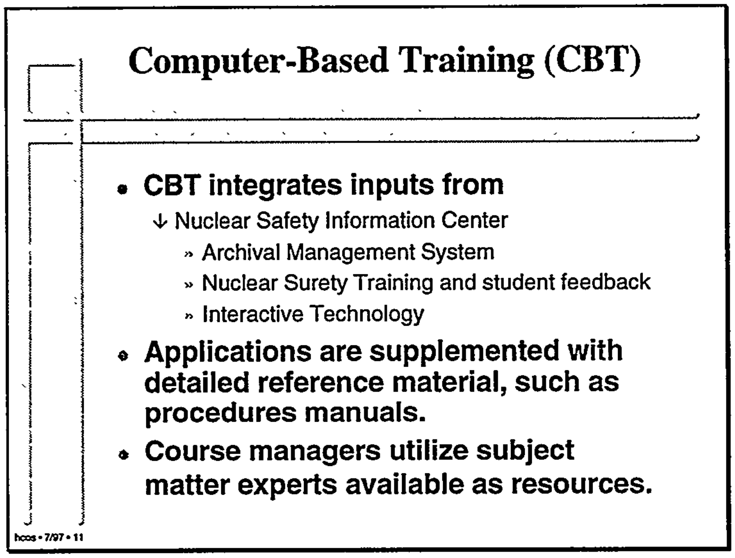
Computer-Based Training (CBT)

The Design Cycle



hcos • 7/97 • 10

Slide 11

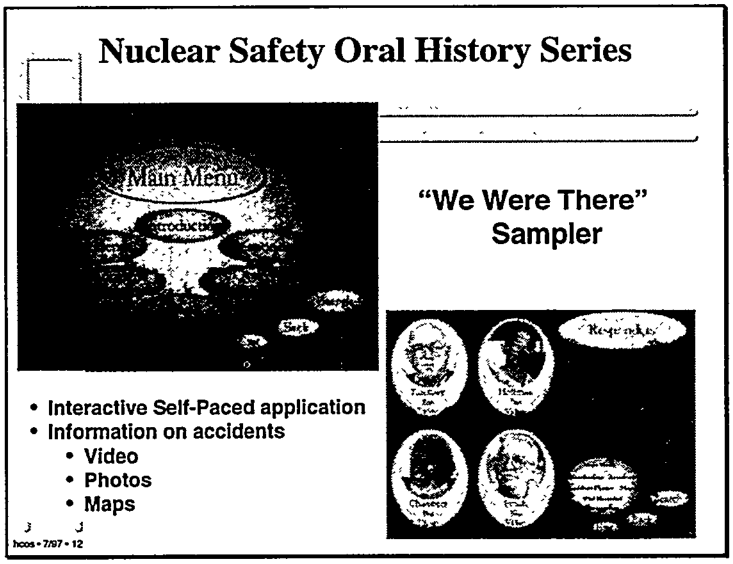


Computer-Based Training (CBT)

- CBT integrates inputs from
  - ↓ Nuclear Safety Information Center
    - » Archival Management System
    - » Nuclear Surety Training and student feedback
    - » Interactive Technology
- Applications are supplemented with detailed reference material, such as procedures manuals.
- Course managers utilize subject matter experts available as resources.

hcos • 7/97 • 11

Slide 12



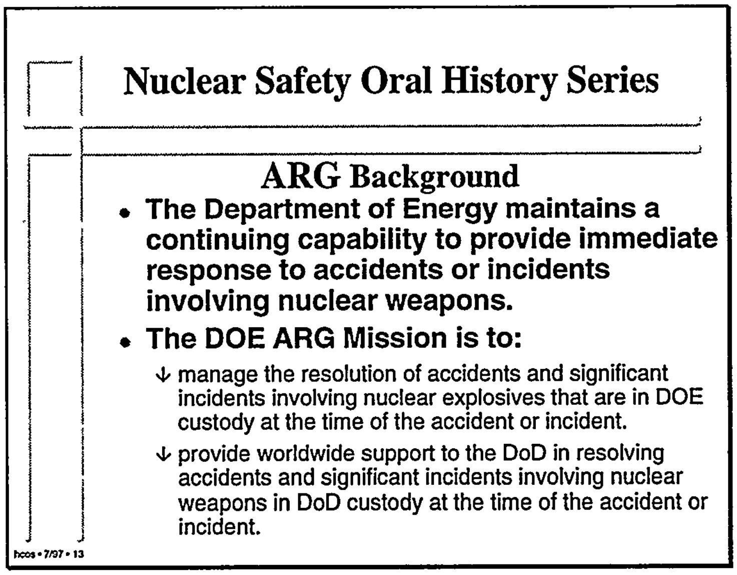
Nuclear Safety Oral History Series

"We Were There"
Sampler

- Interactive Self-Paced application
- Information on accidents
  - Video
  - Photos
  - Maps

hcos • 7/97 • 12

Slide 13



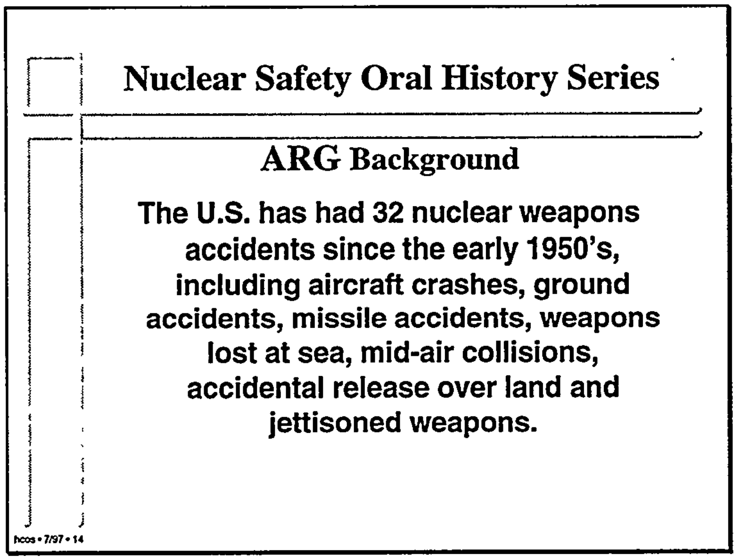
Nuclear Safety Oral History Series

ARG Background

- **The Department of Energy maintains a continuing capability to provide immediate response to accidents or incidents involving nuclear weapons.**
- **The DOE ARG Mission is to:**
  - ↓ manage the resolution of accidents and significant incidents involving nuclear explosives that are in DOE custody at the time of the accident or incident.
  - ↓ provide worldwide support to the DoD in resolving accidents and significant incidents involving nuclear weapons in DoD custody at the time of the accident or incident.

hcos • 7/97 • 13

Slide 14



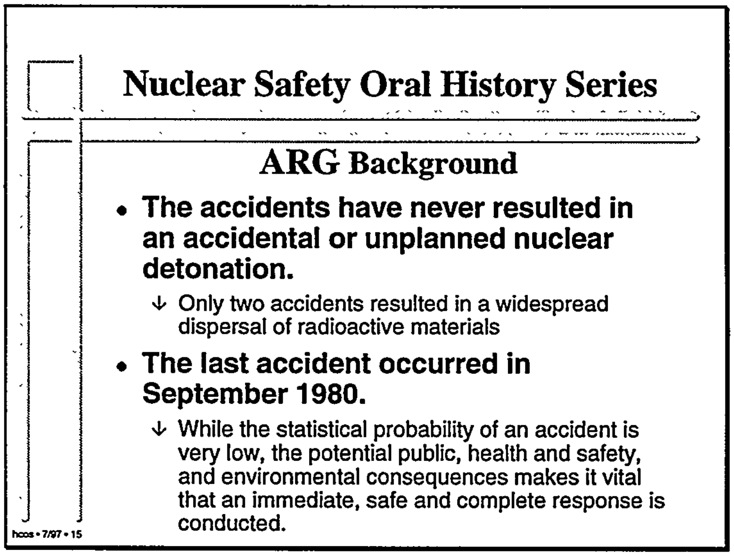
Nuclear Safety Oral History Series

ARG Background

The U.S. has had 32 nuclear weapons accidents since the early 1950's, including aircraft crashes, ground accidents, missile accidents, weapons lost at sea, mid-air collisions, accidental release over land and jettisoned weapons.

hcos • 7/97 • 14

Slide 15



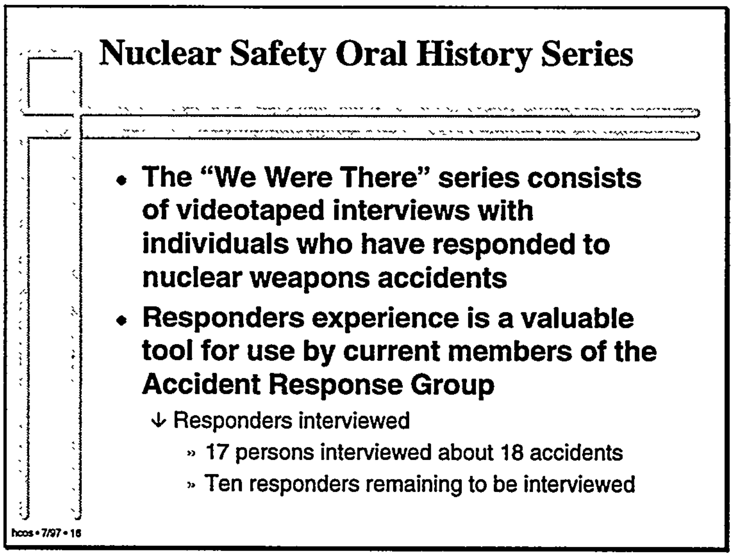
Nuclear Safety Oral History Series

ARG Background

- The accidents have never resulted in an accidental or unplanned nuclear detonation.
  - ↓ Only two accidents resulted in a widespread dispersal of radioactive materials
- The last accident occurred in September 1980.
  - ↓ While the statistical probability of an accident is very low, the potential public, health and safety, and environmental consequences makes it vital that an immediate, safe and complete response is conducted.

hcos • 7/97 • 15

Slide 16

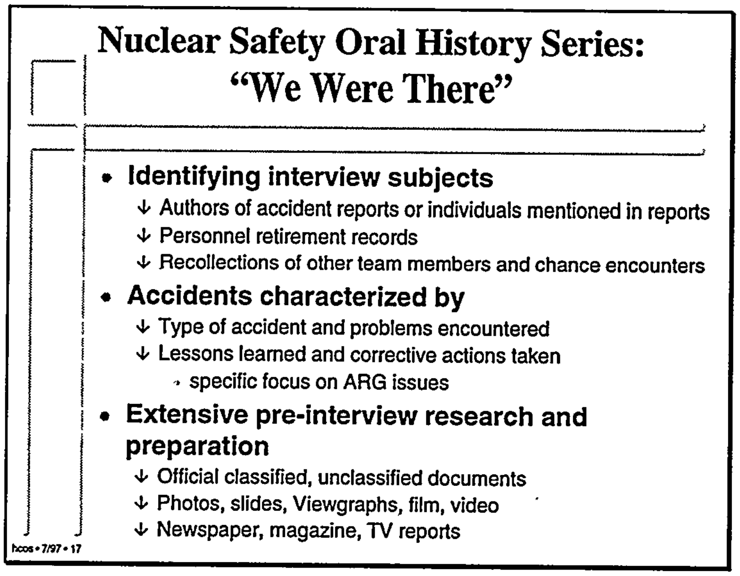


Nuclear Safety Oral History Series

- The “We Were There” series consists of videotaped interviews with individuals who have responded to nuclear weapons accidents
- Responders experience is a valuable tool for use by current members of the Accident Response Group
  - ↓ Responders interviewed
    - » 17 persons interviewed about 18 accidents
    - » Ten responders remaining to be interviewed

hcos • 7/97 • 16

Slide 17

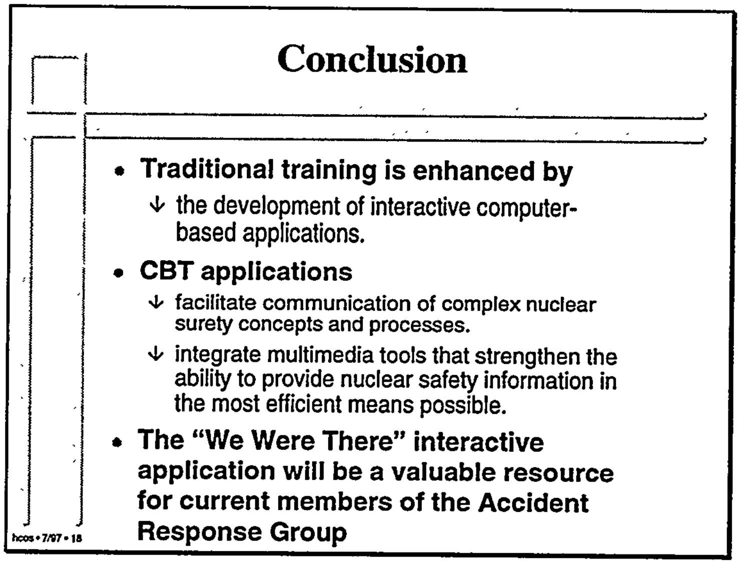


Nuclear Safety Oral History Series: "We Were There"

- Identifying interview subjects
  - Authors of accident reports or individuals mentioned in reports
  - Personnel retirement records
  - Recollections of other team members and chance encounters
- Accidents characterized by
  - Type of accident and problems encountered
  - Lessons learned and corrective actions taken
    - specific focus on ARG issues
- Extensive pre-interview research and preparation
  - Official classified, unclassified documents
  - Photos, slides, Viewgraphs, film, video
  - Newspaper, magazine, TV reports

hcos • 7/97 • 17

Slide 18



Conclusion

- Traditional training is enhanced by
  - the development of interactive computer-based applications.
- CBT applications
  - facilitate communication of complex nuclear surety concepts and processes.
  - integrate multimedia tools that strengthen the ability to provide nuclear safety information in the most efficient means possible.
- The "We Were There" interactive application will be a valuable resource for current members of the Accident Response Group

hcos • 7/97 • 18

Intentionally left blank

HUMAN FACTORS IN SAFETY

Wednesday, July 30, 1997
8:30 a.m. – 12:00 p.m.

Intentionally left blank

Human Aspects of Computer-Related Safety: Limitations, Risks, and Expectations

Peter G. Neumann
SRI International
Menlo Park, California

Intentionally left blank

A Performance-Based Paradigm for Risk Assessment/Management at NASA

James D. Lloyd
National Aeronautics and Space Administration
Washington, DC

Abstract

Modern space systems, such as the Space Shuttle are highly complex. During launch, propulsion systems must channel high amounts of energy, exposing critical components to excessive ranges of temperature over short periods of time. During flight, navigation and environmental control systems must be robust to sustain component failure without compromise to crew safety and to minimize impact on mission success.

NASA uses a comprehensive safety strategy that addresses both hardware and software. From a hardware standpoint, system design strategies include the use of the following:

- Redundancy.
- A thorough understanding of the cause and effect relationships (and the alternatives available to control safety related effects).
- Instrumentation strategies that monitor critical system functions.
- Software designs that minimize the likelihood of an erroneous command that affects flight safety.
- Comprehensive inspection techniques to uncover critical defects on flight hardware.

Increasingly complex spacecraft use extensive software programming to achieve the quick responses that are often needed to accomplish mission objectives or make safety related decisions. NASA's more advanced systems are becoming increasingly dependent on computer technology and use an ever increasing number of lines of code. To assure that an unnecessary increase in the hazards associated with these advanced systems does not occur, NASA has developed a safety standard that will establish a minimum set of software analyses that will be required for space applications. In addition, a far greater emphasis is being placed on the importance of risk assessment and management as a vital element of the program managers and each system engineer's responsibility.

This paper discusses some of the physical and environmental constraints with space systems, presents the key strategies used in minimizing risk through design, test, and instrumentation; and presents an overview of the safety and risk management system that NASA uses to assure mission success.

Introduction

The National Aeronautics and Space Administration (NASA) conducts space operations that have catastrophic consequences if all does not work as planned or designed. Space missions conducted by the United States' Space Shuttle, Russia's MIR and, in the next several years, the international space station, will continue to be perhaps the most visible human space projects to the public. Each of these complex and high-dollar programs represents an extensive national investment, but will serve as valuable resource investments for the nation's future well being, as well as a "departure" point for advancing the world's technology base. The international space station systems, when combined as a joint operation in a few years, will initiate an era when humankind may begin its first steps in exploration of the far reaches of the universe, but during its system engineering development, integration, and assembly will represent one of the most unique challenges presented to humankind in this era.

From a safety standpoint, public expectations for NASA programs, requiring preservation of life in environmental conditions expected to be reasonably close to those here on Earth, can be compared with expectations for protection from nuclear catastrophe that the same public demands from the nuclear industry. In other words, catastrophic failures are not to be tolerated.

NASA's safety program has always been proactive in eliminating or minimizing the effects of catastrophic failures. NASA's policy on safety is that, "Systems shall be designed to preclude the occurrence of a hazard or to negate the effect of the hazard that cannot be eliminated. The level of protection required is a function of hazard severity and can be accomplished by a combination of availability, reliability, maintainability (restorability) and redundancy." Redundancy has always played a large role in NASA's design strategies for complex human-tended spacecraft. The redundancy strategy used provides two-fault or operator-error protection where system loss/damage or personal injury or death could occur.

NASA ensures that this safety policy is properly implemented through a complex process that demands the commitment of engineering, assurance, and management disciplines. Integrating these three elements into a cohesive risk management and control structure continues to be the cornerstone of NASA's success in manned spaceflight.

The Heritage of Safety and Risk Assessment at NASA: Tools

NASA's main tools for assuring a proactive approach to understanding system risk to safety and mission success include deductive reasoning methods such as failure modes and effects analysis/critical items list (FMEA/CIL) and inductive tools such as fault tree analysis. These tools were extensively used in the Apollo program, which took our Astronauts to the moon and returned them to the earth safely in the late 60's and early 70's. These are the same tools that have been used extensively by the defense, commercial, aerospace, and nuclear industries for decades. As many know, the tools are being used increasingly in other industries where failures result in high consequences, such as rapid transit and air traffic control.

Risk identification, analysis, mitigation, and/or acceptance are the elements of the NASA risk management process. Hazards are discerned through a systematic process of inductive and deductive evaluation. Critical hardware is identified through the FMEA. Once a hazard is deemed critical, extreme attention is devoted to assuring that the hardware is properly designed and subsequently produced through an exacting process to assure that the hardware accurately reflects the design specification. The operating environment is the uppermost design-driving requirement in this process.

NASA uses a formal risk assessment approach to supplement the traditional hazard analysis process. The decision (based on all relevant factors) to accept a hazard with its associated risk is a management responsibility, and requires coordination and concurrence by the cognizant safety official and the Program Manager. If there is a lack of concurrence on the decision between management and safety at any level, Safety will elevate the decision to the next Safety, Reliability, Maintainability, and Quality Assurance (SRM&QA) level. Risk assessment analyses generally use the simplest methods that adequately characterize the probability and severity of undesired events. Qualitative methods that characterize hazards and failure modes should be used first. Quantitative methods are used when qualitative methods do not provide an adequate understanding of failure causes, probability of undesired events, or the consequences of hazards or potential failures.

Risk Assessment Code (RAC)

Large numbers of risk factors exist on complex systems such as the Space Shuttle. NASA uses a risk assessment code (RAC) to help focus on those risk factors that require extra attention. A RAC is a numerical expression of risk determined by an evaluation of both the potential severity of a condition and the probability of its occurrence. Similar to the Criticality ranking in the FMEA/CIL process, a severity classification for each risk is assigned according to the following standard definitions:

- Class I - Catastrophic — May cause death.
- Class II - Critical — May cause severe injury or major property damage.
- Class III - Marginal — May cause minor occupational injury or illness or property damage.
- Class IV - Negligible — Probably would not affect personnel safety but is a violation of specific criteria.

Next, a qualitative probability of occurrence estimate is prioritized by the likelihood that an identified hazard will result in a mishap, based on assessment of such factors as location, exposure in terms of cycles or hours of operation, and affected population. This qualitative probability is estimated as follows:

A — Likely to occur immediately.

B — Probably will occur in time.

C — May occur in time.

D — Unlikely to occur.

The Risk Assessment Code Matrix illustrated below in Table 1 is generally used to complete the risk prioritization process.

Table 1. Risk Assessment Code Matrix

Severity Class	Probability Estimates			
	A	B	C	D
I	1	1	2	3
II	1	2	3	4
III	2	3	4	5
IV	3	4	5	6

Design Criteria/Philosophy

In addition to the redundancy strategy and risk management processes, there are several key engineering design criteria that are typically used. For example, the key engineering criteria on the Space Shuttle are:

(1) "Fail safe/fail operational design criteria" that use the redundancy strategies previously discussed.

(2) Conservative design margins where redundancy doesn't make sense (i.e. structures).

(3) A thorough understanding of high energy safety critical components, their nominal performance parameters, and real time monitoring with automatic contingency plans built into the process to eliminate, when considered prudent, the "human in the decision loop."

The judicious use of redundant design strategies requires sufficient understanding of the system design such that common-cause failures cannot impact the two-fault tolerant scheme. For example, where there would be a need for a wire carrying a signal to initiate a servomechanism that would be crucial for crew safety, a backup capability for initiating the same function would not be carried in the same wire bundle. Providing redundant systems or hardware to assure proper function is not always the best solution but always has to be competently prescribed when it is the correct solution.

Useful access to space requires the use of high-energy systems. In such cases, electromechanical components are subject to severe thermal shock and are required to operate at extreme temperatures that challenge the capabilities of both metallic and nonmetallic material science. In assuring the safe operation of critical components, the design engineering department determines the nominal operating conditions with specific attention to temperatures, pressures, and flow rates. Since "time to effect" on a main propulsion system for the Space Shuttle is near instantaneous, supporting software and computer systems use voting logic schemes to make immediate go/no-go decisions based on these performance measures. Virtually every safety critical parameter on the Shuttle Main Engines, External Tank and Orbiter power and control systems is monitored.

The design approach of providing redundancy does present an operational penalty in terms of system availability. In practical terms, not every launch is executed on time because redundant systems may signal a lack of agreement. In recent experience with the Shuttle, as it has become a more mature system and better understood, the "on time" launch record has become remarkable. However, since safety of our human flight systems is paramount, launch delays are the price our nation's premier space program pays when, at the waning moments of a countdown sequence a redundant function goes "off-line" or a monitored critical parameter exceeds limitations (through either false or true excursions) with resultant automatic launch shutdown. Sometimes these shutdowns occur within seconds of the sequence for igniting the solid rocket motors after the liquid engines are already initiated and beginning to "throttle up." As much as this is frustrating and can even be frightening to the launch teams and to an impatient public attuned to and expecting nothing less than success from its Federal government agencies, these forced delays will continue to be visible evidence of NASA's conservative safety conscience at work and will continue to protect the astronauts and the hardware from disastrous consequences.

The international space station is providing a unique and challenging opportunity for the Agency and its international partners (CSA, ESA, NASDA and the newly added RSA) to develop a comprehensive approach to fault mitigation and repair. The impact on system safety of spares criticality, the need for module commonality, extremely limited storage for spares, establishment of proper fault tolerance for life support equipment, philosophy/plans for extended missions in case of failures, safe haven, and dissimilarity of existing international space hardware all must be considered and thoroughly evaluated. Contingency planning must be effectively done with safety as a concurrent partner in the decision-making process. These design processes are at work currently to design and produce hardware that will be placed into orbit in the latter part of the decade. Failure modes and effects and fault tree analysis will serve as the cornerstone for evaluating the risk of this program as well.

Integrating the Process of Safety and Risk Assessment Into the Life Cycle

Now that the key attributes of NASA safety policy have been discussed, let us examine more closely the integrated relationships among Agency management, the assurance discipline, and program management that sustain the safety process for the Shuttle — launch after launch. As articulated in NASA's Strategic Plan, the NASA customers, the top-level decision makers (i.e., the nation's Executive Department and Congress), and the general public are the ultimate resource providers. The Administration and Congress, on behalf of the general public, hold NASA accountable for safety in all aspects of NASA's mission charter, but especially for manned spaceflight. The safety and mission success of NASA's programs are a key operating principle for NASA. To afford a level of confidence in the process for managing the safety and mission success risk, NASA relies on a continuous and comprehensive independent assessment process to assure a sustained level of vigilance, especially for risk associated with manned space flight.

Systems engineering within NASA has become even more challenging in recent years. New programs and projects are generally smaller, more numerous (perhaps), and will have less time allotted for development (cycles are now expected to be less than five years where before cycles were 7-10 years). System engineering management and organization structures have also changed. These are also smaller and less hierarchical. NASA Headquarters once managed many of the programs directly from a central vantage point. That was when large staffs and large budgets were in vogue. This has changed and NASA headquarters is now at nearly half of the staffing it was just 5 years ago. Program authority and accountability is now directly vested in a smaller staff at the field operating center where the decisions and the risk are balance on a direct day-to-day basis. Risk management and decision making is becoming a major driver in assuring the success of these missions. Headquarters' organizations are the purveyors of policy and "enablement" while assuring that the programs are conforming to a set of minimum essential requirements (policy directives) known as the "what's and the why's. Programs are responsible for developing the "how to's."

A new NASA Policy Guideline (NPG) is to be issued this autumn which will relate the top level "what's and why's" for the program management and system engineering community within NASA. This new guideline, NPG 7120.5, NASA Program and Project Management Processes and Requirements, is intended (the document is a draft document and has not been approved by management as yet) the radically change the established life cycle definitions that presently exist and have existed for decades. The NPG is intended to make good on a strategic objective to provide and deliver "world-class" programs and cutting-edge technology through a *revolutionized* NASA. The main themes of NPG 7120.5 will include:

- Process tailoring (allowing program managers great flexibility in applying what used to be required).

- ISO 9000 Compatibility (NASA will no longer specify to manufacturers and suppliers the essence of their quality management processes, these organizations must now be ISO 9000 conformant and third-party certified).

- Aggressive technology commercialization (NASA will increasingly involve commercial entities agreements that will enable the risk for technological advancement to be shared among the commercial entities and not solely by the government (the X-33 and X-34 programs of NASA are a prime example).

- Missions enabled by technology and not the other way around.

- Clear program definition and performance assessment (programs will be monitored for performance using metrics now being derived for cost, schedule, performance, risk, etc.)

- Definitive risk management planning and visible decision making processes.

The objectives of the new guideline are many. These objectives mirror the new strategies of allowing flexibility and tailoring of heretofore considered mandatory requirements. The objectives include many that allow NASA to pursue the "better, faster, cheaper" approach, that many say, was stifled in the past by too many restrictive requirements. Some of these objectives are:

- Establish a process managed approach adaptable to all Programs and Projects including technology development, space and ground systems development, and operations.

- Allow tailoring in Program/Project planning with appropriate levels of insight/oversight required by the risk, criticality, cost, etc. of the particular product or service.

- Build requirements around process products and interacting functions.

- Replace hard lines of Phases A, B, C, D, and E with a flexible nonlinear approach.

- Incorporate interfaces with the other Agency crosscutting processes.

- Encourage innovation- make "better, faster, and cheaper" possible.

It is intended that all future NASA programs will have four major process elements that will replace the present five linear life-cycle element definitions. These processes are program formulation, program approval, program implementation, and program evaluation. Some of these processes coexist at all times (e.g., program evaluation). Figure 1 illustrates this new approach to life cycle processes for NASA.

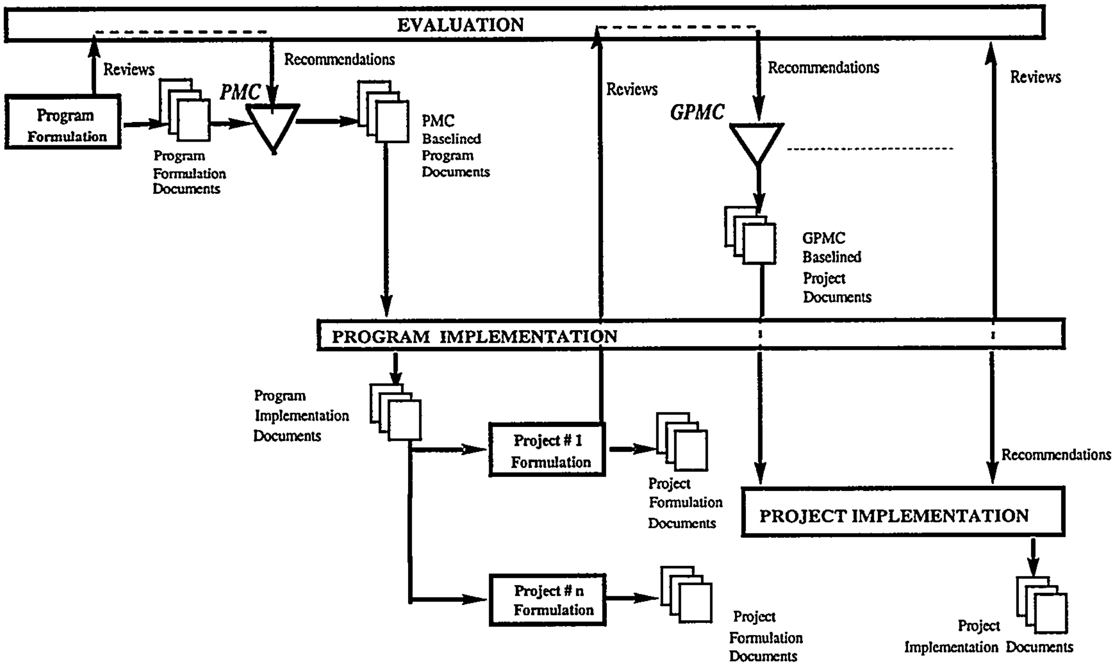

EVALUATION
Reviews
Recommendations
Program Formulation
PMC
Program Formulation Documents
PMC Baselined Program Documents
Reviews
GPMC
Recommendations
Reviews
GPMC Baselined Project Documents
PROGRAM IMPLEMENTATION
Program Implementation Documents
Project # 1 Formulation
Project Formulation Documents
Recommendations
PROJECT IMPLEMENTATION
Project # n Formulation
Project Formulation Documents
Project Implementation Documents

Figure 1. Program/project flow process.

As an element of the new NPG 7120.5, risk management will carry a greater amount of importance. First some definitions to understand these requirements.

(1) Risk to mission success is the probability (qualitative or quantitative) that a program or project will experience undesired consequences such as failure to achieve a needed technological breakthrough, cost overrun, schedule slippage, or safety mishaps.

(2) Risk Management is the identification, assessment, mitigation, and disposition of risks throughout the life of a program or project.

(3) Primary Risk Drivers are undesirable events whose probability is more likely than "remote" and whose consequences could pose a significant threat to mission success. Primary risk drivers typically fall into the following categories:

a. Performance requirements and mission objectives
b. Technology readiness
c. Safety, reliability, maintainability, quality assurance, environmental protection
d. Cost and schedule

Using these definitions NASA plans to invoke the following requirements on all future programs so as to assure that programs begin execution at the outset with the proper foundation and perspective for risk management. These requirements form an essential element and basis for this new approach to programs known as "better, faster, cheaper." These requirements are clear, straightforward and powerful.

e. Risk Management Process. All risks shall be dispositioned (controlled or "retired") before the program/product may enter the operations phase. Each program and project shall follow an orderly risk management process as depicted below. This process shall begin with an analysis of program and project(s) constraints that will shape the risk policy for the program and project(s). Examples are: mission success criteria (primary and secondary); development schedule; budget limits; launch window and launch vehicle availability; international partner participation; legal or environmental concerns; human space flight safety issues; "fail operational/fail safe" requirements; technology readiness; oversight requirements; amount and type of testing; and soon. If an Independent Assessment has been performed, the program or project shall use the risks identified during the assessment as input. An illustration of the risk management and assessment decision process is shown in Figure 2.

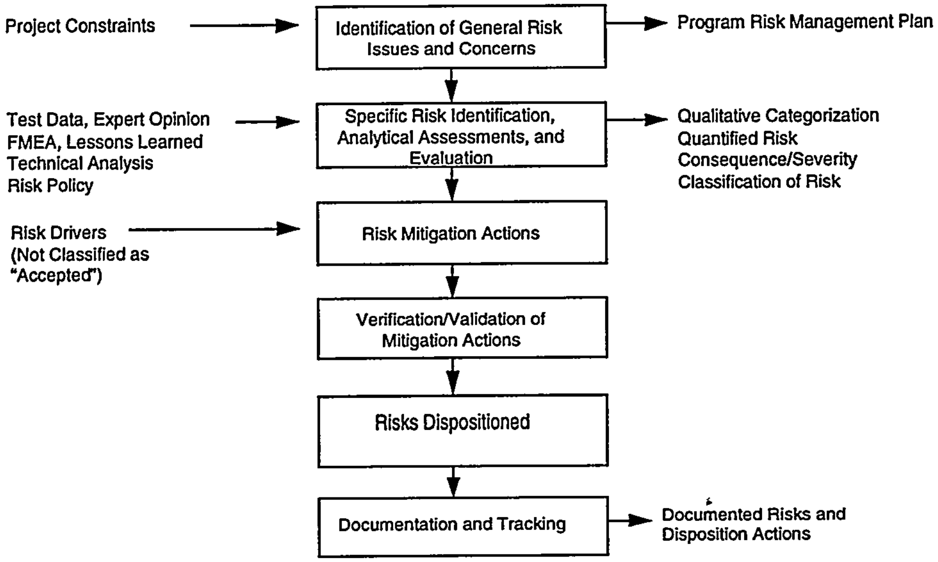

Project Constraints
Identification of General Risk Issues and Concerns
Program Risk Management Plan
Test Data, Expert Opinion
FMEA, Lessons Learned
Technical Analysis
Risk Policy
Specific Risk Identification, Analytical Assessments, and Evaluation
Qualitative Categorization
Quantified Risk
Consequence/Severity
Classification of Risk
Risk Drivers
(Not Classified as "Accepted")
Risk Mitigation Actions
Verification/Validation of Mitigation Actions
Risks Dispositioned
Documentation and Tracking
Documented Risks and Disposition Actions

Figure 2. The risk management flow process.

f. Risk Management Plan Content. A Risk Management Plan is to be developed during the Formulation Phase and executed/maintained during the Implementation Phase. The plan shall include:

(1) Risk management responsibilities, resources, schedules, and milestones
(2) Methodologies, processes, metrics and tools to be used for risk identification, analysis, assessment, and mitigation
(3) Criteria for categorizing or ranking risks according to probability and consequences
(4) Role of risk management with respect to decision-making, formal reviews, and status reporting
(5) Documentation requirements for risk management products and actions

g. Primary Risk Drivers. For each primary risk driver, the program or project shall have the following information:

(1) Description of the risk driver including primary causes and contributors to the risk
(2) Estimate of the probability (qualitative or quantitative) of occurrence together with the uncertainty of the estimate
(3) Primary consequences should the undesired event occur
(4) Significant cost impacts given its occurrence
(5) Significant schedule impacts given its occurrence
(6) Potential mitigation measures
(7) Implemented mitigation measures, if any
(8) Characterization of the risk driver as "acceptable" or "unacceptable" with supporting rationale

h. Continuing Risk Management. Each program and project shall provide an assessment of overall risk. Each project shall maintain an assessment of the readiness to continue into the next phase of its lifecycle. Suitable reserves must be demonstrated.

i. Risk Control/Retirement. Each project must demonstrate throughout the Formulation and Implementation Phases that it has adequately resolved all primary risk drivers. A risk driver will be considered "controlled" or "retired" when any one of the following conditions are satisfied:

(1) Risk mitigation options that reduce the probability of occurrence to "remote" have been planned, implemented, and their effectiveness verified

(2) All reasonable mitigation options (within cost, schedule, and technical constraints) have been instituted, and although the risk driver is determined to be more likely than "remote," it has been judged by the GPMC to be "acceptable"

(3) Reserves are available so that, should the risk actually occur, resources would be available to recover from cost, schedule, and technical impacts

j. Risk Documentation. All risk disposition decisions must be documented and a system for tracking such decisions must be implemented.

In the future NASA will follow these requirements in its programs. In the meantime, NASA will continue to have robust and piercing independent self-assessment and critique. This independent self-assessment process has provided the proper level of oversight and management tension to assure that all are constantly seeking to perform their safety and risk assessment processes with the proper level of review and engineering. The management tension provided consists of many elements that have been designed to operate at many levels of the management organization.

A primary source of external independent assessment is through the Aerospace Safety Advisory Panel (ASAP). The Aerospace Safety Advisory Panel (ASAP) is a group of senior aerospace safety experts assembled from private aerospace industry to advise the NASA Administrator and Congress. The ASAP develops analyses and recommendations on topics assigned by the Administrator relative to impact from demanding schedules, reductions of cost on launch processing, and external assessments of NASA products and processes. This group of senior Aerospace personnel remains abreast of developments not only for the Space Shuttle, but also for the space station and other aeronautical programs that have an impact on safety. One of the key focal points for ASAP (as well as NASA) in the upcoming years will be the integration of international hardware with the station. This will pose many potential safety concerns in the integration of dissimilar programs (from Europe, Japan, Canada and, now, Russia) having various maturity levels and differing design philosophies.

Internal to NASA, the Safety and Mission Assurance (S&MA) organizations at NASA Headquarters and its field centers conduct support programs such as Space Shuttle though both independent assessments and direct project support. The technical assessments serve as a mechanism to advise program and project element management regarding the adequacy of SRM&QA requirements, assure their effective implementation, and identify areas of technical risk. This support to program/project management is the real workhorse of the independent assessment process. Not only do our safety engineers examine an extensive volume of technical details, looking for subtle changes in requirements, launch commit criteria, software discrepancies, changes to the Critical Items List rationale for retention, flight rules and crew procedures, they are also active participants on all flight readiness reviews and are directly involved on every launch decision.

To gain some insight on the magnitude of the task, consider that on the Orbiter project alone the safety organization participates in 36 active problem resolution teams (PRTs) that have typically examined over 1000 problems that have been reported during a typical 12-month period. Table 2 lists these PRTs. The scope of the PRTs ranges from the critical auxiliary power unit to the thermal protection system (i.e. Orbiter Tiles), to the waste control system. This is on a program that is mature and operating on an eight flight per year schedule!

Table 2. Problem Resolution Teams

- Air Data Transducer Assembly (ADTA)
- Antennas
- Auxiliary Power Unit (APU)
- Actuators
- Audio
- Crew Equipment/Pinch
- Display and Controls
- Data Processing System (DPS)
- Drag Chute
- Environmental Control and Life Support System (ECLSS)
- Electrical Power Distribution and Control (EPD&C)
- KU-Band
- Landing/Deceleration
- Logistics/NASA Shuttle Logistics Depot (NSLD)
- Mechanisms
- Mechanical Systems
- Navigation Aids
- Nose Wheel Steering
- Orbital Maneuvering: System/Reaction Control System (OMS/RCS)
- Purge Vent & Drain (PV&D)
- Rate Gyro Assembly (RGA)
- S-Band

Table 2. Problem Resolution Teams

Flood Lights	Star Tracker
Fuel Cells/Power Reactant Storage Distribution (PRSD)	Structures
Hand Controllers	Supply & Waste Water
Hydraulics/Water Spray Boiler (HYD/WSB)	Thermal Protection System/Thermal Control System (TPS/TCS)
Instrumentation	Waste Control System (WCS)

NASA restructured its safety support for Shuttle launches in the years after the Challenger accident, which occurred in January 1986. The safety team support now in place not only provides technical support to the launch team, but also assures accurate technical communication of any issues that might affect the safety of the flight. This safety team support begins long before launch date. To assure technically accurate and effective communication between NASA centers and Headquarters, several Safety review meetings and teleconferences are held to thoroughly examine potential safety related issues or problems prior to each flight. The Pre-launch Assessment Review (PAR) is the key internal safety review, which assures that the Office of Safety and Mission Assurance at NASA Headquarters has insight into the launch risks associated with any upcoming flight. The discussion during the PAR results in a team decision regarding the technical risk associated with the upcoming launch. The PAR reviews provide the technical basis on which the Office of Safety and Mission Assurance will certify risk acceptability during the Launch Minus 2 Day (L-2) review, when the entire launch management team is assembled to make the final decisions on risk affecting a launch.

Mission Safety Evaluation

Since the entire process is both comprehensive and complex, a Mission Safety Evaluation (MSE) Report is prepared for each launch. The MSE is the document that formalizes the risk decision process. The MSE is an OSMA produced document that is prepared for use by the NASA Associate Administrator, Office of Safety and Mission Assurance (OSMA), and the Space Shuttle Program Manager prior to each Space Shuttle flight. The MSE analyses and assesses the safety risk factors that represent a change, or potential change, to the risk "baselined" by the Program Requirements Control Board (PRCB) in the Space Shuttle Hazard Reports The scope and content of the MSE report provides substantial insight as to the nature and scope of NASA management review to assure safety of flight. Both NASA Headquarters and the Manned Spaceflight Centers participate in extensive reviews of factors affecting the safety risk of each Shuttle flight. OSMA provide concurrence with the decision by the Space Shuttle Program Manager in approval of Element Hazard Reports to baseline the program safety risk.

Changes to the risk baseline for the Space Shuttle Program arise from mission unique requirements, mission processing problems, in-flight anomalies, component testing, new analyses, and related risk issues from other launch vehicles undergoing analysis. Problem or issue resolution is evaluated for risk acceptability and items referred to as safety risk factors are listed in the MSE.

OSMA certifies the risk acceptability of the baseline safety risks with changes identified in the MSE before proceeding to the L-2 Review. Any disagreements with the resolution of risk must be resolved satisfactorily before a decision to launch can be made.

The MSE is published on a mission-by-mission basis for use in the Flight Readiness Review (FRR) and is updated for the L-2 Review. For tracking and archival purposes, the MSE is issued in final report format after each Space Shuttle flight.

The MSE provides the Associate Administrator, Office of Safety and Mission Assurance, and the Space Shuttle Program Manager with the NASA Headquarters' Space Flight Safety and Mission Assurance Division position on changes, or potential changes, to the Program safety risk baseline approved in the formal Failure Modes and Effects Analysis/Critical Items List (FMEA/CIL) and Hazard Analysis process. While some changes to the baseline since the previous flight are included to highlight their significance in risk level change, the primary purpose is to ensure that changes which were too late to include in formal changes through the FMEA/CIL and Hazard Analysis process are documented along with the safety position, which includes the acceptance rationale.

The report addresses risk factors that represent a change from previous flights, factors from previous flights that have impact on this flight, and factors that are unique to this flight. Factors listed in the MSE are essentially limited to items that affect, or have the potential to affect, Space Shuttle safety risk factors and have been elevated to the Shuttle Program Manager for discussion or approval. These changes are derived from a variety of sources such as issues, concerns, problems, and anomalies. It is not the intent to scour lower level files for items dispositioned and closed at those levels and report them here; it is assumed that their significance is such that Program Management discussion or approval is not appropriate for them. Items against which there is clearly no safety impact or potential concern will not be reported here, although items that were evaluated at some length and found not to be a concern will be reported as such. It also documents unresolved safety risk factors impacting each flight.

Data gathering is a continuous process. However, collating and focusing MSE data for a specific mission begins prior to the mission Launch Site Flow Review (LSFR) and continues through the flight and return of the Orbiter to the Kennedy Space Center (KSC). The MSE is updated subsequent to the mission to add items identified too late for inclusion in the pre-launch report and to document performance of the anomalous systems for possible future use in safety evaluations.

The content of MSE includes:

- Brief introductory remarks, including purpose, scope, and organization (Section 1).

- A brief mission description, including launch data, crew size, mission duration, launch and landing sites, and other mission- and payload-related information (Section 2).
- A list of unresolved risk factors that could impact flight (Section 3).
- A list of risk factors that are considered resolved for the flight (Section 4).
- A list of In-flight Anomalies (IFAs) that developed during the previous Space Shuttle flight (Section 5).

The unresolved and resolved risk factors, and the in-flight anomalies sections provide the most technical insight. The **unresolved risk factors** are those that could impact the flight. Items in this list require resolution prior to flight. The **resolved risk factors** present a summary of the risk factors that are considered resolved for the flight and therefore are not constraints to flight. The NASA S&MA Community have reviewed all these items. A description of the risk factor, information regarding problem resolution, and rationale for flight are provided for each risk factor. The safety position with respect to resolution is based on findings resulting from System Safety Review Panel (SSRP), Pre-launch Assessment Review (PAR), and Program Requirements Control Board (PRCB) evaluations (or other special panel findings, etc.). It represents the safety assessment arrived at in accordance with actions taken, efforts conducted, and tests/retests and inspections performed to resolve each specific risk factor. The In-flight Anomalies (IFAs) section contains a summary of in-flight anomalies rising from previous missions. In each of these sections, Hazard Reports (HRs) associated with each risk factor in this section are listed beneath the risk factor title. Where there is no "baselined" HR associated with the risk factor, or if the associated HR has been eliminated, none is listed. Hazard closure classification, either Accepted Risk {AR} or Controlled {C}, is included for each HR listed.

Other Risk Decision Supporting Features of the NASA Program

Having described in some detail the established process for evaluating risk for the Shuttle Program, let's discuss other features designed to augment this process and help strengthen the overall knowledge and awareness of risks to space flight. The Safety and Risk Management Division is sponsoring two activities to ensure effective communication of safety issues outside of the day-to-day risk assessment process. These activities are the NASA Safety Reporting System (NSRS) and Safety Lessons Learned.

The NSRS objective is to assure that a mechanism exists by which any person that feels a safety problem exists (whether the problem is real or perceived) can communicate the issue anonymously to NASA. It is a confidential, voluntary, and responsive safety reporting system that provides a direct channel for NASA employees and contractors to notify the NASA Safety and Risk Management Division of safety concerns. The NSRS enables safety personnel to identify safety problems and implement corrective actions independently. The nature of corrective actions may be engineering, manufacturing, administrative, procedural, or operational. Timely information about actual hazards is of the highest priority. The NSRS has been established to collect, evaluate, and communicate such information in a timely and accurate manner. It is intended to supplement, not replace, existing reporting systems. The NSRS has been implemented at all NASA Field Installations and applies to any risk impacting safety for any NASA program. NASA contractors are also encouraged to implement the NSRS at their facilities.

The Safety Lessons Learned Information System (LLIS) is intended to capture a set of corporate knowledge as a continuous improvement process to enhance safety on current and future projects. The safety lessons learned are disseminated to program managers and throughout NASA Field Installations and Headquarters by cognizant personnel to improve understanding of hazards, prevent the occurrence of accidents, and suggest better ways of implementing system safety programs. In addition to contributing appropriate information to the LLIS, safety managers are encouraged to include this information in program, procurement, and Field Installation newsletters to communicate more effectively with management. Lessons learned that indicate the need to revise source documents (e.g., instructions, handbooks, specifications, and standards) are submitted directly to the person that prepared the document. The LLIS is intended to provide a library of lessons learned data for use by Program Managers, design engineers, and safety personnel.

Software Safety Standard: A New Policy for Supporting Effective Risk Management

NASA has published a software safety standard in recognition of the significant contribution to safety risk that software in complex systems now presents. This recently published standard outlines new requirements for assessing software products as a potential source for risk in the development and operation of new complex safety systems. This guidance, NASA Safety Standard (NSS) 1740.13, Software Safety Standard, is intended for any software being developed for any NASA system that, through software control, can cause harm to humans or damage to property. New emphasis has been be placed on using the traditional approaches for identifying risk originating in the software and assuring means for mitigating this risk. New software analysis reports will be required throughout the life cycle of the software to document the completion of these risk assessments. These new planning efforts and analyses are phased throughout the life cycle of the software, and assure safety analysts are involved with the software developers and include the normal phases of:

- Software Safety Planning, including the definition for Verification and Validation and Independent Verification and Validation
- Software Safety Requirements Specification Development
- Software Design
- Software Integration and Acceptance Testing
- Software Maintenance

New analyses that are specified include:

- Software Safety Requirements Analysis
- Software Safety Architectural Design Analysis
- Code Safety Design Analysis
- Software Test Safety Analysis
- Software Change Analysis

Much of this analysis and safety focus has been used in the past for NASA system development; however, this standard, for the first time ever Agency-wide, will be a major step in standardizing terminology and establishing a degree of rigor to the process.

Assuring Safety and Mission Success Within the Constraints of Budget Realities

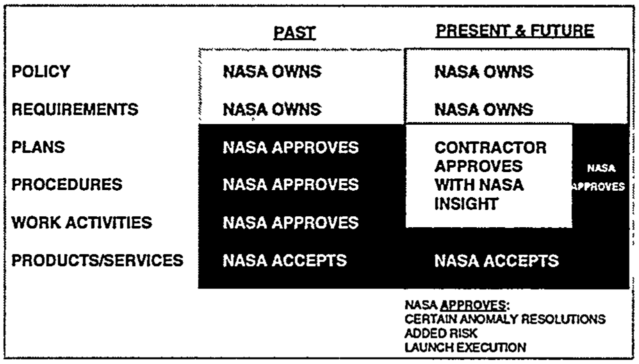
As the NASA missions change and new and more complex programs emerge, NASA must continually adjust the methods and techniques for protecting the resources to which it is entrusted. Responding to the same competitive pressures facing industry worldwide, NASA is also confronted with the challenge for accomplishing scientific endeavors with more efficiency and fewer dollars. As mentioned before, NASA has recently developed a Strategic Plan that provides the framework on which future aerospace ventures will be conducted. This Strategic Plan has been refined over the past several years with both external and internal customers shaping its visions and goals. Included in the Strategic Plan is the strategy to accept appropriate and prudent risk while striving for lower costs, shorter development times, and more frequent missions. This demands that our system engineers not rely so much on robust design approaches as they have done in the past, but more on a better understanding of what these design features provide and at what cost. Risk has become more of a system trade characteristic that has to be "weighed" with other features such as weight, power, cost, schedule, etc. The Office of Safety and Mission Assurance Strategic Plan further states that "We will conduct our programs so that we are recognized as an international leader in safety, quality, and mission assurance activities. We will utilize a systematic and disciplined approach involving advocacy, oversight, and support to the technical risk decision making process."

From NASA's new Strategic Plan, the Office of Safety and Mission Assurance is assessing where improvements can be made, and targeting those areas that will be particularly challenging in the near future. Increasing emphasis on conservative reliability techniques to improve the reliability of redundant elements, identifying and using cost effective and believable probabilistic methods to improve our risk assessment process, and developing new techniques to assure that safety is not compromised in using complex systems with software elements are just a few of the new directions that we visualize for the future to keep NASA and America on the forefront in providing safe and successful access to space.

NASA and Contractor Interaction Under the New Program

While NASA is downsizing and reengineering it is searching for new approaches to monitor the risk and safety posture of its programs. NASA relies more and more on its contractors to independently perform the risk assessment processes. A good example of this process of relying more on contractors can be seen in the transfer of more program accountability to a single flight-processing contractor for the space shuttle. At one time, NASA integrated the efforts of scores of contractors and now this is done by a single contractor. NASA has to develop ways to insure insight is maintained on the effectiveness of these risk management actions. Some of these metrics for insight include incidents and accidents involving both people and property that occur within the control of the contractor.

While still a "partner" with industry, NASA is increasingly reliant on industry to perform the bulk of the risk assessment and safety assessment work to be done. It is expected that any risk that is judged to be "unacceptable" through the thorough and complete risk assessment process will be elevated to NASA for the proper disposition. If this is not done, industry will, to a greater extent, not share the indemnity coverage they enjoy if proper communication of risk were the case. This can be depicted in the following figure, which illustrates the way that NASA and industry will interface, where risk and safety are the criteria.



	PAST	PRESENT & FUTURE	
POLICY	NASA OWNS	NASA OWNS	
REQUIREMENTS	NASA OWNS	NASA OWNS	
PLANS	NASA APPROVES	CONTRACTOR APPROVES WITH NASA INSIGHT	NASA APPROVES
PROCEDURES	NASA APPROVES		
WORK ACTIVITIES	NASA APPROVES		
PRODUCTS/SERVICES	NASA ACCEPTS	NASA ACCEPTS	

NASA APPROVES:
CERTAIN ANOMALY RESOLUTIONS
ADDED RISK
LAUNCH EXECUTION

Figure 3. NASA and industry paradigms for risk management.

What this figure explains is that, in the past, NASA was vitally involved in every aspect of a program's development and consequently was always a direct and contributing party to deciding the level of risk considered acceptable by the program. This involvement was at every level of participation from the development of policy and requirements (proper roles for a governmental unit) but beyond into the development of plans, procedures, work activities and the actual products and services themselves. This was irrespective of the risk consequences. It has been said that this level of involvement stifles the industry and was very costly and ineffective as far as costs and schedule were concerned. In the present and future NASA, NASA will be unable to participate at these levels of involvement and will require more of the decision making to be performed by the supporting contractors. The exception will remain that when risk is high NASA will be more involved in the step-by-step decision process as before.

Passing On "Best Practices:" Translating Experience to the Commercial Sector

NASA is intent on translating its experiences and its knowledge to the commercial sector for the benefit of the American public. In the past this was done more directly, with direct involvement with industry partners. With the organization becoming smaller, more efficient and effective means for conveying partnerships and information have had to be devised. As an example, a recent "push" for aviation safety enhancements by NASA and the Administration has as its goal step-level changes (decreases) in aviation mishap rates by the next two decades. Millions of dollars have been set aside for NASA to help the American aviation industry to achieve these goals. These improvements will focus on not only materials and system level improvements to airframes and power plants for aircraft but also crew resource management improvements through better software and fight controls and better interaction with the environment, the civil airspace, and weather-related factors that are frequently the cause of aviation mishaps.

NASA Safety and Mission Assurance is also attempting to pass along lessons learned and best practices to the industry that are directly associated with NASA. Through the publication of its popular reliability best practices documents (NASA Preferred Practices for Design and Test, NASA Technical Memorandum 4322) and the access to lessons learned through a NASA-only web site, industry can share in the lessons that have proven to be successful for programs.

Further, NASA is now initiating a web-based training effort for its safety and reliability professionals. This web-based training will make available to NASA personnel and associated contractors, training and automated tools for providing experienced-based data and information to its safety and mission assurance practitioners. One of the newest tools that will become available in the next year, will be a Personal Computer/Windows-based quantitative risk assessment model that will assist anyone with the need to quantitatively model a complex system. This model is presently being developed and will shortly be demonstrated to NASA's Administrator who has vocally supported its development. It is a Quantitative Risk Assessment System (QRAS) mathematical model in the form of a PC-based software tool that can be used to calculate the change in the probability of failure of the Space Shuttle as a result of proposed upgrades (at the top level, as well as at intermediate subsystem levels). It will provide to anyone a general capability to analyze any complex system using quantitative risk assessment approaches. When this tool is finalized, it will be available for industry to use in assessing and documenting the risk that is presented for any system that is being designed for NASA. It is our belief that such a tool will allow designers having little risk assessment experience to use their system level understanding of their system to participate in the integration of a complete system risk model of the program they are working. Once the model is assembled certain assumptions can be made and the system design changed based on feedback from the model. A "What if?" (or sensitivity analysis) section will allow users to modify the model (modifications could include replacement of subsystems with what is known or expected from proposed upgraded subsystems, addition/deletion of failure modes, changes to failure probabilities and/or their uncertainty bounds, etc.) and re-run it to obtain change in risk from baseline. A more perfect understanding system-wide change-in-risk would be the outcome.

Summary

NASA is the midst of a revolution in the way it manages its programs and its associated risk. The effects of downsizing, and the need to simplify and streamline its processes are offering opportunities for system engineers to unleash their engineering talents to develop technologies that were unheard of or believed impossible 10 years ago. Along with this newfound pursuit of "better, faster, and cheaper" for system development will come challenges and potential increases in risk. These shifting paradigms bring with them both the opportunity for new and exciting technologies and the risk of catastrophic events never seen before. NASA is busy assuring that the control of risk keeps pace with these events.

Biography

James D. Lloyd
Safety and Risk Management Division
NASA Headquarters
300 E Street, SW
Washington, DC 20546

Mr. Lloyd is presently the Director of the Safety and Risk Management Division in the Office of Safety and Mission Assurance at the Headquarters of the National Aeronautics and Space Administration (NASA). His responsibilities include the development of NASA policy covering safety (including system safety), reliability, maintainability, and risk management as well as the oversight for its implementation organization-wide. Mr. Lloyd has worked at NASA in a number of capacities over the past 10 years. Initially, he participated as a system operations research analyst in the "return to flight" program for the Space Shuttle (after the Challenger accident). He then worked for 5 years in a number of different positions in the Space Station "Freedom" Program, including the position of Director, Product Assurance, just before the program was reorganized as the international space station program.

Prior to his NASA career, he worked as a civilian safety engineer for the United States Army Materiel Command for 18 years participating in the system safety development of many present front line weapons systems, including the Blackhawk and Apache helicopter systems and the Abrams Main Battle Tank and numerous explosives projects and facility developments.

Mr. Lloyd graduated from Union College, Schenectady, New York with a Bachelor of Science degree and from Texas A&M University in College Station, Texas with a Masters of Engineering Degree and is a registered professional engineer.

Public Communications About Nuclear Weapons Accidents: Fanning the Flames or Dampening Doubts?

Hank C. Jenkins-Smith
University of New Mexico
Albuquerque, New Mexico

Intentionally left blank

Human Factors in Proactive and Reactive Safety Studies

P.C. Cacciabue
M. Pedrali
European Commission, Joint Research Centre
21020 Ispra (Va), Italy

Abstract

This paper discusses *reactive* and *proactive* applications of human factors methods for the analysis of complex working environments. It focuses on the crucial issue of consistency between methods employed and data collected in analysis of unwanted occurrences. An example application is shown.

Introduction

The safe operation of complex systems in present technologies demand the elaboration of both reactive measures, by which the lesson of past experience is learned and appropriate feedback is developed, and proactive measures, dedicated to the prevention, detection, protection, recovery, and containment of events that can combine in an accident.

As human factors (HF) is a crucial element for the safety of complex systems, the effectiveness of proactive and reactive measures depends on the accuracy and quality of the HF methods they rely upon (Maurino et al., 1995). In order to be effective, the proactive and reactive measures need to be supported by sound and consolidated theories and methods that, in the case of Human Factors, are based on (1) paradigms/models of operators' behaviour, and (2) instruments allowing accurate examination of operators' working environment, both in nominal conditions and in the case of unwanted occurrences (Wiener and Nagel, 1988). These examinations have to be carried out by also considering the so-called 'organisational factors.'

The consistency and coherence between proactive and reactive measures can be ensured by a core of such methods that may be developed in their support. In this scenario, an essential rule of methodological consistency is the application of *methods* for interpreting (a) the unfolding of real accidents, also defined as the *retrospective approach,* and (b) the generation of possible outcomes deriving from hypothetical initiating events, also defined as the *prospective approach.*

In this paper, the requirements on data structures, the collection of information, and on methods will be further expanded. We will focus on methods that are becoming common practice for the assessment of safety and working environment contexts. An example of such methodological development will also be discussed in some detail.

Proactive-Reactive Measures

The definition of *reactive* and *proactive* measures for accident management and recovery that we will adopt here refer to Reason and can be found in a number of publications (Reason, 1990; Maurino et al., 1995). In brief, *reactive measures* are remedial implications that can only be applied *after* the accident has occurred. They represent the lesson learned from such past experience by devising appropriate feedback and specific actions. *Proactive measures* are applied *before* the occurrence of an accident to assess the safety health of the system.

The common objective of both types of measures is to prevent and eventually control accidents. These goals are reached by developing a number of skills and abilities in the personnel controlling the systems, namely, (1) *awareness* of the risk and hazards, (2) early *detection* of the presence of possible and likely dangers, (3) knowledge means of *protection* for keeping people and the environment from injury, (4) ability to *recover* from off-normal conditions, (5) knowledge of how to *contain* release of dangerous substances or energy, and (6) ability to *escape* from systems out of control.

The main difference between reactive and proactive measures lies in the fact that reactive measures are engendered by the occurrence of an accident while proactive measures are not.

In theory it would be better to develop only proactive measures. However, in practice many safety approaches and methods, originally generated at the research level but not fully expanded, have been fully applied as *reaction* to the outcome of serious accidents. Only later, after an accident, have these measures been further developed into sound methods and, at an even further evolutionary stage, they have been introduced as mandatory measures by safety and regulatory authorities (Figure 1).

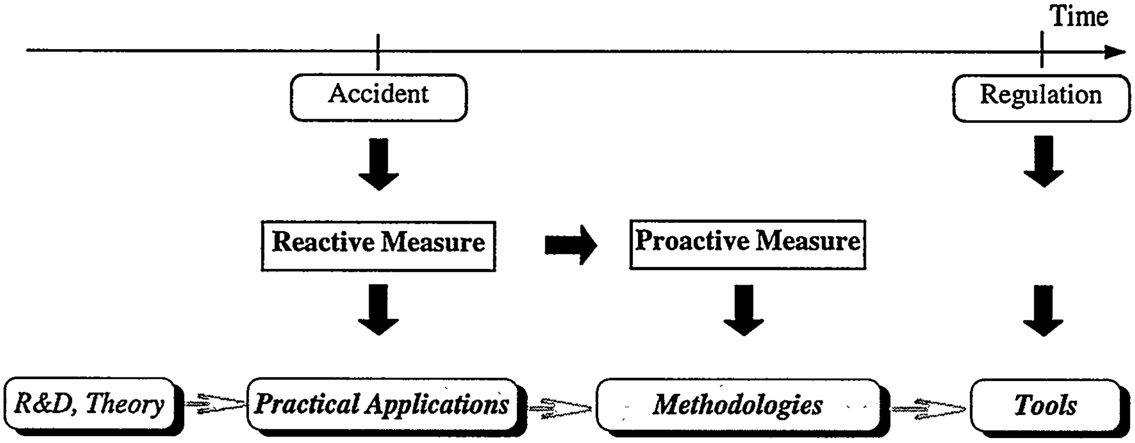


Figure 1. Proactive-Reactive measures and methods for accident analysis and prevention.

Three major examples of such an evolutionary process can be mentioned here: Safety Management Systems for the chemical and process industry, Probabilistic Safety Assessments for nuclear energy production, and Crew Resource Management courses for the aeronautical domain.

The development and use of Safety Management Systems (SMS) for accident prevention in the domain of chemical and process plants, at least in Europe, followed the occurrence of a number of very serious accidents in the late 1970s. One such serious accidents, the Seveso release of dioxin, occurred in Italy and gave paramount importance to the development of SMSs. This method had been already proposed at research level at the time of the accident, but it was not certainly considered essential for the safety assessment of a plant. Hence the development of SMS has been fostered as a reactive measure to prevent future serious accidents of the same nature as the one of Seveso.

Since then, a number of methodological approaches have been developed in consideration of sound theoretical basis and formulations. Thus, proactive measures have been developed (Cacciabue et al., 1994).

Nowadays, the use and implementation of SMSs are regulated by a "directive" of the European Union, which is known as the "Seveso Directive" (Directive 82/501/EEC on Major Accidents Hazards) which requires that all industries subjected to chemical hazards develop an SMS as part of their safety measures. The industrial domain is, in many cases, implementing SMS as a practice and the development state is now entering its final stage. The SMS is becoming a proactive *tool* of standard use, like all other means of compliance of the industry in accordance with safety rules and regulations.

Similar paths of development can be found in the nuclear and aeronautical domains. In the nuclear energy production area, the risk assessment methodology, originally proposed by Rasmussen in the famous report WASH-1400 (US-NRC, 1975) on demand from the insurance companies and as new method for safety analysis, became particularly important after the Three Mile Island accident (a reaction). Afterward, the risk assessment methodology was widely developed, becoming the so-called Probabilistic Safety Assessment (PSA). Presently, it is fully integrated as part of the requirements for certification of operability of nuclear power plants by regulatory bodies in almost all countries worldwide.

Similarly, training of pilots to identify and manage human factors, originally fostered in the US by NASA (Lauber et al., 1979), was brought to the full attention of the aviation safety world by a number of flagrant accidents, such as the Tenerife collision in 1977 and the Washington National Airport accident in 1982. Thereafter, human factors training has been expanded firstly to consideration of pilots as a crew, and thus generating the acronym for human factors training of CRM or Crew Resource Management. CRM has been further extended to cabin assistant, maintenance, and dispatch personnel and now is being adopted also for air traffic control and for the corporate aspects of the companies. Methodological and theoretical aspects of human factors training are fully developed and assimilated by all major airlines and are common practice (Wiener et al., 1993). At the regulatory level, while in the US the CRM is a compulsory requirement, in Europe, the

European Joint Aviation Authorities, (JAA,) has introduced this is a requirement beginning in 1998, though the usual practice of human factors training by CRM is already practically adopted in all European countries.

With reference to Figure 1 and in consideration of the above discussion, it can be argued that the principal objective of research and development institutions covers the period that goes from the initial study of methods and theories and then continues beyond the reactive phase to support the further development of proactive measures by formalising the methods in closed forms that allow production, at commercial level, of 'tools' by industry.

Therefore, the main objective of research institutions lies mainly in the completion and development of proactive measures by devising sound theories and appropriate methods. This concept will be further developed in the next section.

Prospective-Retrospectives Approaches

As previously discussed, a number of methods and theories sustain proactive and reactive measures. In practice one could broadly group these theories into two major categories: *prospective approaches* and *retrospective approaches.*

Retrospective approaches consists of the analysis of real accidents or observed events by the reconstruction of facts and identification of causes of inappropriate behaviours at all levels of human-machine interactions.

Prospective approaches correspond to methods for the prediction of an accident either by postulating the sequence of interactions from an initiating event or by evaluating the safety state of the system.

These definitions of prospective and retrospective methods should not lead to misunderstanding or confusion with proactive and reactive measures, as the former methods represent *means* of compliance or theories to ascertain or assess safety, while proactive and reactive measures are *ends* derived either by the need to avoid repetition or anticipate serious accidents or unwanted occurrences. This difference is subtle but needs to be well understood as not to engender confusion.

As an example, in the case of an accident, the lessons can be learned in two different ways: (1) reactively, by demanding the development of appropriate measures to avoid the repetition of a similar situation (end = avoid repetition by preventing), and
(2) retrospectively, by studying, through an appropriate "root cause analysis" approach, the reasons and factors that lead to the accident (means = theoretical approach for root cause analysis).

In summary, retrospective and prospective methods can either be part of a reactive or a proactive measure, as long as they are properly considered in relation to the objective of the remedial implications (measure) for which they are applied.

To further develop the concept of prospective and retrospective methods we will shortly discuss how they can be developed and what should be their objectives. Moreover, the discussion has so far been kept at a high level, purposely avoiding a focus both on a specific area of safety analysis and on a domain of application.

In the following discussion, as we will detail more the methodological methods supporting proactive studies, we will need to focus firstly on an area, and then on a domain of application. We have chosen to consider the human factors area and the domain of aviation safety, as these suit better our expertise and present context of research work.

Theories and Methods

The literature on human factors, over the last 20 years, is very rich in well-funded methods based on theoretical asserts and practical observations developed by specialists in engineering, cognitive sciences, psychology, and sociology to support methodological development of prospective and retrospective studies (Pew et al., 1977; Rouse, 1980; Rasmussen, 1986; Broadbent et al., 1989; Reason, 1990).

The most modern approaches are oriented towards the consideration of the effects of the whole organisation and socio-technical environment on the behaviour, which is thus a consequence of a number of concurrent internal and external causes, rather than the outcome of individual characteristics (ICAO, 1993; Westrum, 1995).

A paradigm, or model of reference, is necessary for representing how these causes interact and influence human behaviour. In general, a "system" composed of humans and machines can be described by *three levels* of dependencies and interactions (Figure 2):

1. The *defences*, barriers and safeguards, that are planned and designed to ultimately prevent, detect, protect, recover, and contain operational hazards. These are the automatic protection and control systems as well as the human operators themselves.

2. The *workplaces*, with their environmental and psychological contributors to individual behaviour. These factors relate to the task, to the immediate working environment (the context) and to people's mental and physical state.

3. The *organisation*, which is ultimately responsible for defining the policies regulating the design, management, maintenance, training, communication, and so on, and guiding philosophies related to safety, i.e. of the "safety culture" of the whole system (Degani and Wiener, 1994).

The methods developed for retrospective and prospective approaches utilise models and analyses of information and data as shown in Figure 2.

In particular, the lesson that we have learned from the evaluation of real working situations and contextual events, i.e., retrospective analysis, is instrumental to the development of prospective approaches. These analyses deal with the collection and structuring of information useful for "speculative" assessment of hypothetical configurations of the human machine system for which safety has to be assessed.

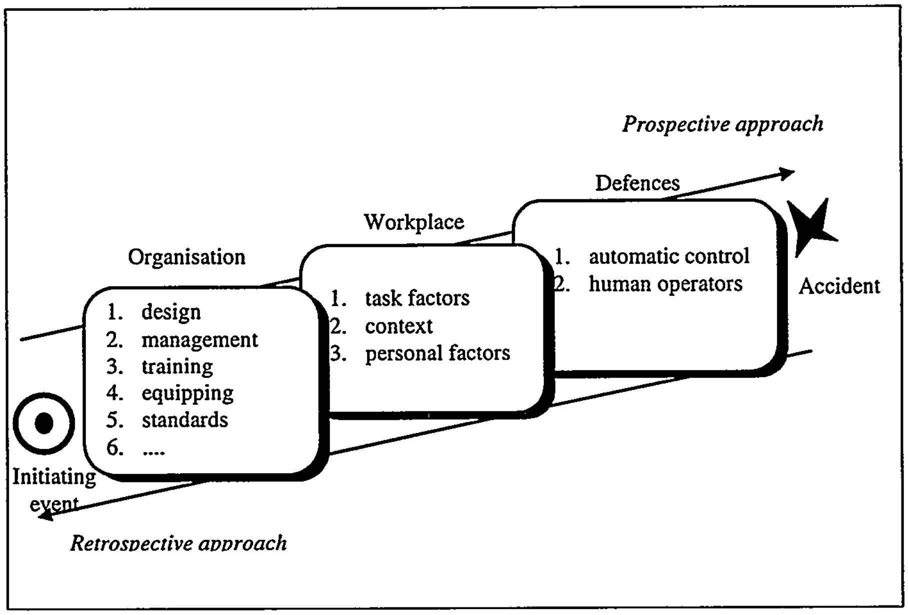


Figure 2. Levels of human interactions.

Data and Information

The ways in which data are collected and analysed in retrospective studies are crucial for the development of prospective approaches. Indeed, when retrospective and prospective approaches are linked by a common model of reference, the output of the latter is strictly dependent from the input given by the former.

In the aviation domain we can find four main sources of data (Figure 3):

1. Data recorded during the human interaction processes, provided by Cockpit Voice Recorders, Flight Data Recorders, and videos of training sessions.

2. Information collected within the working environment and the organisation by field observation.

3. Information collected within the working environment and the organisation by interviews and questionnaires.

4. Information retrieved from the analysis of accident reports and of the contents of mandatory and voluntary reporting systems (ECC-AIRS, NASA-ASRS, etc.).

These data can strongly contribute to create a body of information extremely valuable for understanding the "socio-technical system."

We can look at the first type of data as elements NOT mutually correlated, i.e. they are collected as recorded. The other three types are structured in a convenient way, i.e. they are collected according to formats defined a priori. Indeed, while the former come directly from a real situation and characterise it, the latter are coupled with a representation of this situation.

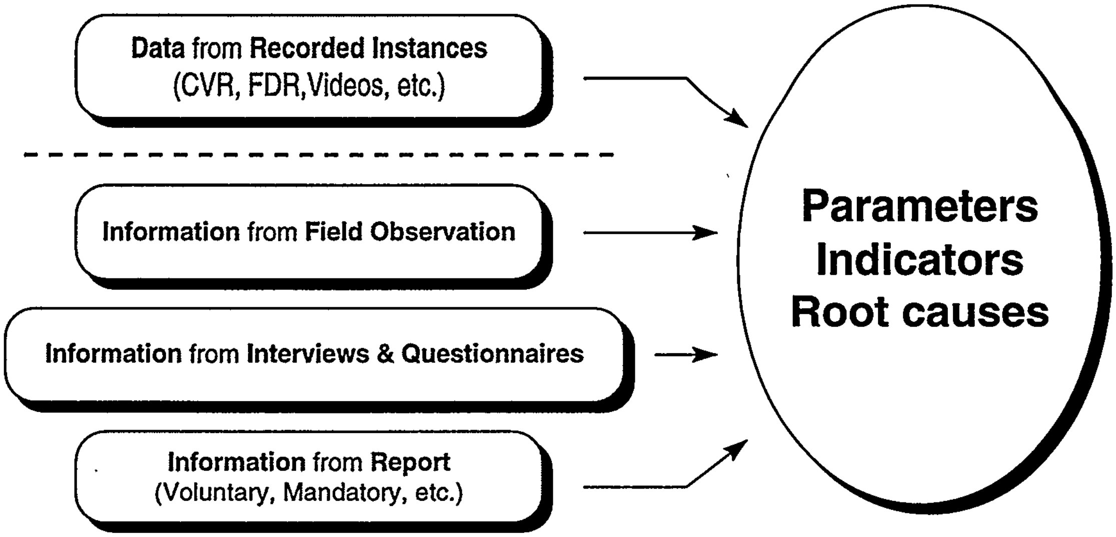

Data from Recorded Instances
(CVR, FDR,Videos, etc.)
Information from Field Observation
Information from Interviews & Questionnaires
Information from Report
(Voluntary, Mandatory, etc.)
Parameters
Indicators
Root causes

Figure 3. Data and information as the origin of parameters and indicators for safety studies.

These data are the outcomes of retrospective approaches that combine root-causes of erroneous behaviours, parameters and indicators associated with these behaviours, indicators of system state, and so on. They will be exploited for prospective approaches such as probabilistic safety assessments and the design of interfaces and procedures.

HERMES: A Method for Human Factors Analysis

At the Joint Research Centre of the European Union in Ispra, we have developed a method for prospective and retrospective human factors analyses named HERMES, which stands for **H**uman **E**rror **R**eliability **M**ethod for **E**vent **S**equences (Cacciabue, 1997). This method is based on a *classification* of human errors that is coupled with a *model of cognition* (Hollnagel and Cacciabue, 1991; Hollnagel, 1993). While the use of a classification scheme is necessary to put event descriptions in a common form, the model provides a basis for the classification. The method ensures that the classification is used in a uniform way.

The reference cognitive model is the SMoC (Simple Model of Cognition). Four cognitive functions outline the process of cognition (Observation, Interpretation, Planning, and Execution) and are connected with each other as schematically represented in Figure 4.

The two fundamental features of the SMoC are (1) the distinction between what can be observed and what can be inferred, and (2) the cyclical nature of human cognition. What can be observed is related to the phases of Execution and Observation, such as the execution of a particular action, or the perception of a signal. What can only be inferred is related to the phases of Planning and Interpretation. Indeed, we can deduce how operators have interpreted a signal or a system state only by observing their behaviour. This cyclical nature means, for instance, that an action can be preceded by a choice (in the planning phase), or by the interpretation of an observed sign, which could be the consequence of a previous action.

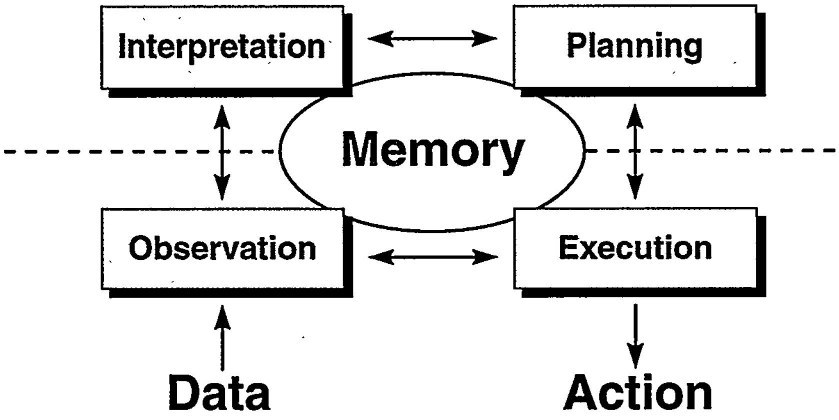


Figure 4. The SMOC model.

The classification of human errors is the "core" of the method. It consists of four tables in relation with the four cognitive functions of the SMoC. Each table contains a set of predefined error categories, typical of a particular function (Execution, Planning, Interpretation, and Observation). There are two fundamentally different ways to consider erroneous actions. One is with regard to their manifestations or **phenotype**, i.e., how they can be observed; the other is with regard to their causes or **genotype** (Hollnagel, 1991). The classification distinguishes between phenotypes and genotypes; these are further classified into **Person-related causes**, PRCs; and **System-related causes**, SRCs. While factors related to cognition and emotional states are classified as PRCs, those that can be attributed to the technological system and to the environment are included in SRCs. Phenotypes are grouped separately; they are the result of an interaction between genotypes and the context. SRCs may trigger or modify a PRC; however, they are not necessarily involved in an erroneous behaviour (PRCs can be the only causes).

In *retrospective applications* of HERMES, classification is used to investigate triggering causes of erroneous actions. The analysis is performed by starting from the phenotype and following back the process of cognition that ended up with the execution of this action. The classification structure allows one to reconstruct the causal chain, from the error manifestation up to its root causes. The causal chain is not linear and we can represent it as a fault tree with the root as the error manifestation (phenotype) and the leaves as its causes (genotypes).

In *prospective applications* of HERMES, the analysis is performed starting with the selection of a set of initiating events and boundary conditions. Then, a modelling architecture for the evaluation and prediction of the human-machine interaction has to be defined. This architecture has to account for the simulation both of human cognitive and behavioural processes (by means of the SMoC model), and of physical plant and working context. The successive step is the definition of data for the predictive calculation of interactions.

These data are retrieved from the previous retrospective analyses and they constitute the actual connecting element between retrospective and prospective analyses in HERMES. Indeed, these data correspond to (a) the System and Person related causes, (b) the Phenotypes of erroneous actions, and (c) the effects of erroneous behaviour at higher levels of cognition, such as inappropriate forms of perception, identification or planning.

Once all these elements of a prospective analysis are defined, the calculation and evaluation of consequences and the safety assessment of the human-machine system can be performed.

Retrospective Approach: Root Cause Analysis

The retrospective use of HERMES is aimed at discovering what errors made by an operator or operators contributed to an incident/accident, and subsequently to support the identification of the possible causes that triggered these errors. The application of the method is therefore accomplished in two phases: Erroneous Action Identification (EAI) and Causal Analysis (CA).

In the first phase (EAI), the investigator makes a chronological reconstruction of the accident/incident and detects those actions that *deviated* from the expected evolution of the events. These actions can be seen as symptoms of a general malfunctioning of human-machine and/or human-environment interaction. They are not necessarily erroneous: they may not be erroneous deviations from a prescribed procedure. The analyst determines it using the following steps: Data Collection, Event Time Line, and Deviation Detection.

In Data Collection, all the available material regarding the accident is gathered; in the Event Time Line, sheets filled-in with the information coming from the previous step provide a time-oriented representation of the accident; in the Deviation Detection, actions not complying with the foreseen procedures are identified. To do this, the investigator compares the real sequence of actions, reconstructed by the Event Time Line, with the procedures that should have been followed. A further screening is subsequently done to discover what are the real errors. These errors, or inappropriate actions, ought to be identified at the end of the EAI; they are the manifestation of erroneous behaviours, that is to say the final result of a cognitive process.

In the second phase (CA), the investigator analyses the erroneous behaviours and ascertains their root causes. This analysis of human actions consists of two steps and is carried out by means of the above-mentioned classification. The errors (manifestations) are classified according to a list of *error modes*; then they are examined by the scheme supported by the classification, allowing a clear distinction between causes and manifestations of inappropriate actions, and between internal and external causes affecting human performances.

The reason for this subdivision is methodological: incorrect actions in context need firstly to be singled out before looking for their causes. The EAI is not only preparatory to the CA, but it is also the main reference when performing the CA.

Reactive Measure: Human Error Analysis in Accident Investigations

The retrospective application of HERMES can be an example of a **reactive measure** when applied in the context of an accident investigation. We applied the method to two aeronautical accidents that involving to a DC9-30 and a A320 (Pedrali et al., 1995). The aim was not to give another interpretation of facts, our interest instead was to understand how the different factors noticed by the official commissions of inquiry could play a role in the pilots' cognitive processes. These processes led the pilots to deviate from the prescribed procedures and to ignore those signs and signals that could have induce them to recover from errors.

From our analyses it came out that the two accidents had very much in common: they both occurred during the approach to landing (ATL) phase, they were both classified as controlled flight into terrain accidents, and in both situations the flight path was lower than expected. However, while in the case of the A320 the incorrect flight path was due to an erroneous evaluation of the vertical speed, in the case of the DC9-30 this discrepancy was due to an erroneous evaluation of the aeroplane altitude. Moreover, the two ATL phases were quite different: a non-precision approach (VOR/DME) for the A320 and a precision one (ILS) for the DC9-30.

Hence, a very accurate analysis was done with respect to SRCs. In particular, while the SRCs were substantially different owing to the working environment (CRT screens, flight management system, and autopilot modes), they show similarities in terms of crew co-operation, and communication within and outside the cockpit. As far as PRCs were concerned, it is important to note that in both accidents *time compression* and *work overload* were responsible for faulty planning that ended up in errors. It also turned out that these PRCs were triggered by SRCs in relation with the procedure. PRCs related to the training (*lack of training* and *long interval since learning*) influenced the pilots' cognition at the level of planning, interpretation, and observation as well. Omissions were very often due to causes that arose at the planning phase and whose effects have directly affected the execution phase; other phenotypes showed a more complex nature.

The analyses of these two accidents revealed that SRCs are, as usual, less complex to deal with than PRCs. While the former can be often solved by technological improvements, the latter can be tackled with training.

Proactive Measure: Video Analysis of Human Errors in Training

As stated before, reactive and proactive measures are ends and are dissociated from the methods (retrospective and prospective) they are supported by. This explains why we can use the same method both as a reactive measure and as a proactive measure.

If we refer to Figure 1, we realise how the same method, originally conceived at the research level but not fully expanded, can be applied as a *reaction* to the outcome of serious accidents. However, the method can be successfully adopted as a proactive measure after further development and by its implementation as a tool.

HERMES, applied retrospectively, followed this path: on the basis of its previous applications for the analysis of human error in accident investigation (reactive measure), it has become a tool for the analysis of human errors in debriefings after simulator sessions.

We ameliorated the classification and implemented it in a software tool, named DAVID (Dynamic Analysis of Video in Incident stuDies), developed for *video analysis* of human errors. The idea is to support the expert in the organisation of data concerning errors and in the investigation of error causes. The tool is therefore composed of two modules: a data Organiser and an Analyser (Pedrali and Bastide, 1996).

- By means of the data Organiser, the expert examines the video recording of an event and detects errors. However, all the data concerning these errors need to be arranged conveniently in order to make apparent the information that can be useful for the causal analysis. For this purpose, the Organiser interface provides a ten-column table where the analyst can input error characteristics.
- By means of the Analyser, the analyst can graphically trace back the erroneous cognitive process. The interface is basically structured in two parts: the left part is devoted to the identification of genotypes, while the right part displays the reconstruction of the causal chain as a fault tree. Since the architecture of the classification is totally transparent to the expert, the use of the Analyser is rather simple. At the beginning of each error analysis, the expert classifies the human errors according to a list of phenotypes. The selected category becomes the *root element* of the fault tree and it is placed in the 'account of events.' Causes are proposed on the left-hand side of the interface, the selected categories are added below the root element, and they become the *leaves* of the fault tree. The expert can comment on the chosen categories and demand for their explanation (Figure 5).

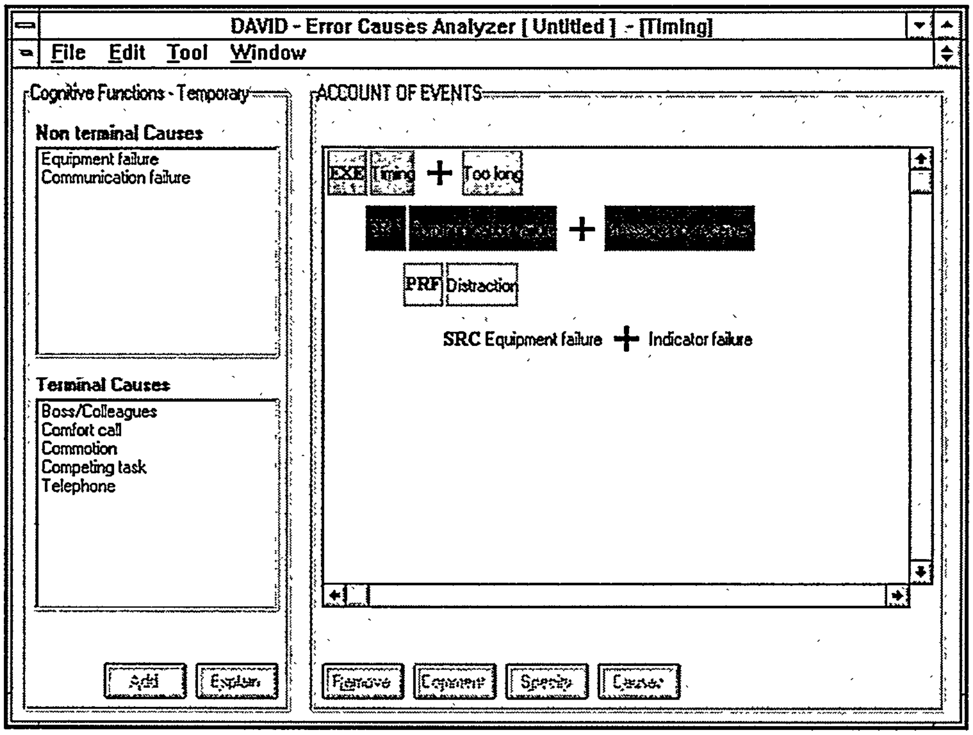
We integrated DAVID in a multimedia environment, whose architecture was conceived together with the tool. This environment relies on a Selector for the realisation of video scenarios and on a relational Database for the storage of the analysis results.

We applied DAVID to the video analysis of errors performed during non-precision approaches carried out in a full A340 flight simulator. The two-pilot crew (Captain and First Officer) made several approaches over two different airports (New York-JFK and

Toulouse-Blagnac). After the simulations, the First Officer detected errors made and analysed them by means of DAVID. What is of interest in the results we obtained is a first validation of DAVID as a tool for debriefing crew after simulator session (Pedrali and Bastide, 1997).

The acknowledged advantage in this type of analysis is the reconstruction of the causal chain of an error in the cognitive process, made by the people involved (auto-confrontation). It is extremely useful for the improvement of human-machine interactions, discovering that some kind of causes exert their influence in a particular phase of the cognitive process. Moreover, ascertaining that some kind of errors are more frequent in certain working conditions can be extremely important in accident/incident prevention. For these reasons, application of our approach in the domain of operator training is envisaged as a proactive measure.

From the point of view of data structures, we can see the interest of an integrated approach such as HERMES that combines analyses of real and simulated events. Although the context of an accident might be different from a simulation, we can discover relations and analogies between errors performed following the same procedures. Capitalizing on these data coming from different sources is of fundamental importance, and guarantees the importance of proactive approaches based on the same method used for reactive approaches.


DAVID - Error Causes Analyzer [Untitled] - [Timing]
File
Edit
Tool
Window
Cognitive Functions - Temporary
ACCOUNT OF EVENTS
Add
Explain
Remove
Comment
Specify
Cancel

Non terminal Causes

Equipment failure
Communication failure

Terminal Causes

Boss/Colleagues
Comfort call
Commotion
Competing task
Telephone

EXE Timing + Too long

PRF Distraction

SRC Equipment failure + Indicator failure

Figure 5. User interface of DAVID analyzer.

Conclusion

This paper has discussed problems and issues of proactive and reactive safety measures associated with human factors.

The question debated concerned methods and theories sustaining such safety measures. In particular, a number of issues related to these methods have been examined, namely, the meaning of prospective and retrospective analysis, the importance of data and information retrieval, and the use of these for the development of valuable safety proactive measures.

The theoretical standpoint that derives from the discussion on safety measures, methods and theories, has resulted in the elaboration of a method called HERMES that can be applied in retrospective and prospective studies of accidents, both as a proactive and reactive safety measure.

The development of HERMES is quite well advanced and its application to real situations has been attempted both as a reactive and proactive measure, derived from the (retrospective) study of the root causes of real accidents and simulations in the aviation domain. A number of other laboratory and theoretical applications of HERMES have also been carried out, though they have not been discussed in this paper, with reasonable success.

The method is considered mature for an application as a prospective approach to a real working context and the opportunity of carrying out such an operation is presently being exploited in the domain of thermo-electrical energy production. The results of such an application will certainly help in further refining the theory and model contained in HERMES and will contribute to making the approach more realistic and manageable in practice.

Acknowledgements

The authors wish to thank Monica Bacchi for her contributions to the development of the methods and studies and for the support in the preparation of this paper.

References

Broadbent D.E., Baddeley A., Reason J.T., (Eds.), (1989). *Human Factors in Hazardous Situations*, Proc. of a Royal Society Discussion Meeting 28-29 June 1989, Clarendon Press, Oxford.

Cacciabue P.C., Gerbaulet I., Mitchison N., (Eds.), (1994). Safety Management Systems in the Process Industry. **EUR 15743 EN**, European Commission, Brussels, Belgium.

Cacciabue, P.C., (1997). A Methodology for Human Factors Analysis for System Engineering: Theory and applications. *IEEE-System Man and Cybernetics,* **27** (3), pp.325-339.

Degani, A., Wiener, E.L., (1994). Philosophy, policies, procedures and practice: The four "P"s of flight deck operations. In N. Johnston, N. McDonald & R. Fuller (Eds.). *Aviation Psychology in Practice,* pp. 68-87. Avebury Technical, Aldershot, UK, 1994.

Hollnagel E., Cacciabue P. C., (1991). Cognitive Modelling in System Simulation. Proceedings of Third European Conference on Cognitive Science Approaches to Process Control, Cardiff, UK, September 2-6.

Hollnagel, E. (1991), The Phenotype of Erroneous Actions: Implications for HCI Design, in G.R.S. Weir & J.L. Alty (Eds.), *Human Computer Interaction and the Complex Systems*, Academic Press, pp. 73-121.

Hollnagel E., (1993). *Human Reliability Analysis: Context and Control.* Academic Press, London, UK.

ICAO, (1993). Human Factors Digest No. 10, Human Factors, Management and Organizations. Circular 247-AN/148.

Lauber, J. K., White, M. D., Cooper, G. E. (Eds.) (1979). Resource Management on the Flight Deck. NASA Conf. Publication 2120, NASA Ames Research Center, Moffet Field CA, US.

Maurino, D. E., Reason, J., Johnston, N., Lee, R. B., (1995). *Beyond Aviation Human Factors.* Avebury Aviation, Aldershot, UK.

Pedrali, M., Cojazzi, G, Cacciabue P.C., (1995). A methodology for retrospective analyses of accidents involving human factors, 7th International Conference on Aviation Psychology. Columbus, Ohio.

Pedrali, M., Bastide, R. (1996), DAVID: A Multimedia Tool for Accident Investigation, in M.A. Sasse, R.J. Cunningham, R.L. Winder (Eds.) "People and Computer XI, Proceedings of HCI '96," Springer, pp. 349-368.

Pedrali, M., Bastide, R., (1997). Can we trace back cognitive processes on root cause analysis? HCI International '97. 7th Intern. Conference on Human-Computer Interaction, 24-29 August, 1997, San Francisco, US.

Pew R.W., Baron S., Feehrer C.E., Miller D.C., (1977). Critical Review and Analysis of Performance Models Applicable to Man-Machine-Systems Evaluation, BBN Report No. 3446, Cambridge, MA. 1977.

Rasmussen J., (1986). *Information processing and human-machine interaction.* North-Holland, NY.

Reason, J. T., (1990). *Human error.* Cambridge University Press, Cambridge, UK.

Rouse W. B., (1980). *Systems Engineering Models of Human-Machine Interaction,* North Holland, Oxford.

US-NRC, (1975). Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. **WASH-1400** (NUREG-75/014), U.S. National Regulatory Commission, Washington, US.

Wiener E. L., Nagel D. C., (Eds.), (1988). *Human Factors in Aviation.* Academic Press, San Diego, CA.

Wiener E. L., Kanki B. G., Helmreich R. L., (Eds.), (1993). *Cockpit Resource Management.* Academic Press, San Diego, CA.

Westrum R., (1995). Organisational dynamics and safety. In McDonald, N., Johnston, N., & Fuller, R. (Eds.) *Applications of Psychology to the Aviation System.* Proceedings of the 21st Conference of the European Association of Aviation Psychology, pp. 75-80. Avebury Aviation, Aldershot, UK.

Biography

Pietro Carlo Cacciabue, Ph.D., M.Sc.
European Commission, Joint Research Centre
Institute for Systems, Informatics and Safety
TP 210
21020 Ispra (Va), Italy

Dr. Cacciabue is a senior scientist of the Institute for Systems, Informatics and Safety. His Ph.D. in Nuclear Engineering is from the Politecnico di Milano (Italy) and his M.Sc. in Nuclear Engineering is from the Politecnico di Torino (Italy). He is also Director of the International Association for Probabilistic Safety Assessment and Management. He is an expert in probabilistic safety and reliability assessment, safety analysis, and simulation of complex systems and human factors.

Mauro Pedrali, Ph.D., M.Sc.
European Commission, Joint Research Centre
Institute for Systems, Informatics and Safety
TP 210
21020 Ispra (Va), Italy

Dr. Pedrali is human factors researcher of the Institute for Systems, Informatics and Safety. His Ph.D. in Computer Science is from the University of Toulouse 1 (France) and his M.Sc. in Aeronautical Engineering from the Politecnico di Milano (Italy). Since 1992 he has been working in the domain of accident investigation by contributing to the development of a method for root cause analysis of human errors and implementing it in a software tool to be used during debriefing after simulators sessions.

Rapid Transit Control Center Operations: A Human Factors Approach

Kurt F. Walecki
Booz·Allen & Hamilton, Inc.
Los Angeles, California

Abstract

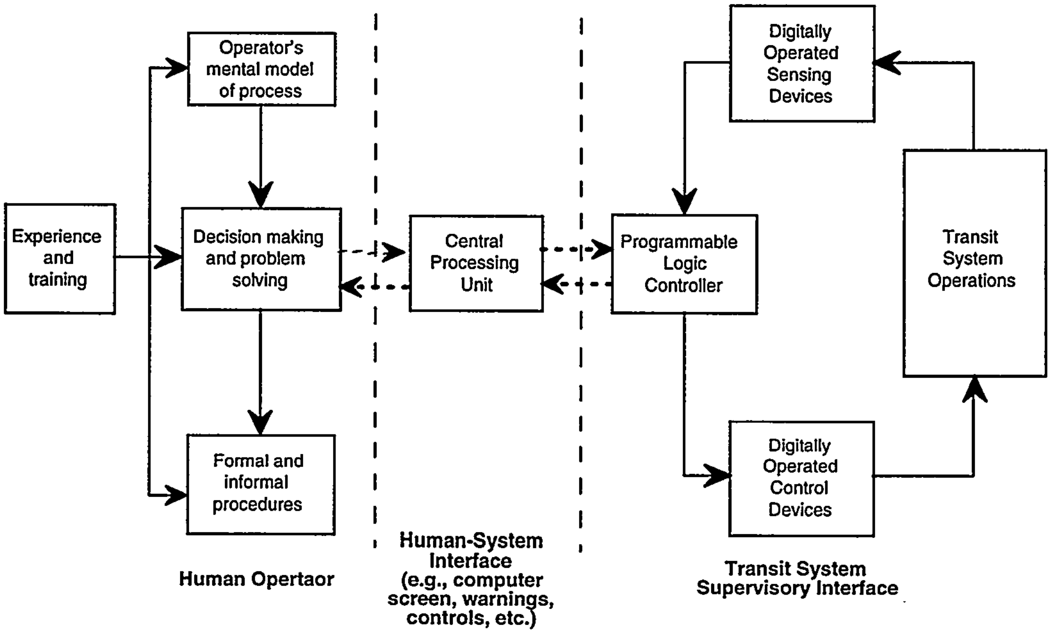
The central network of present rapid transit systems is the operations control center. This operations center is responsible for the control and monitoring of critical subsystems required to ensure public safety. As the technology of transportation systems increases in the future, the ultimate control responsibility will shift from the train operator to the central control operator via advanced supervisory train control systems. This increase in workload and responsibilities to the central control operator will place an ever-increasing strain on the human-machine interface.

The potential high consequence (i.e., patron safety, public finance, and social perception) associated with public rapid transit operation is significantly correlated with the transit property's knowledge and ability to address human-factors issues. Human error causation can be attributed to numerous human-factors issues, both micro and macro in scope. A human factors assessment of an operations control center should utilize the most current human factors methodologies. As the human factors issues are uncovered, recommendations to operation control center managers can be made and be ready for facility implementation. This paper will present a systematic approach to assess human factors related issues to a typical operations control center of a transit system.

Introduction

The technological revolution has reached the rail transit industry, providing numerous advancements in train control, train protection, and safety systems monitoring. These advancements however, continued to rely on the human element as the core component. With the introduction of advanced Supervisory Control And Data Acquisition (SCADA), the role of the operator is changing from an on-board train operator to a centralized, external system supervisor. Physical detachment from the operating transit system, additional tasks, and expanded complex control equipment combine to increase the complexity and responsibility of this position (see Figure 1).

The increased workload applied to the transit operator has, in concurrence, placed extreme importance on the selection process of the Operations Control Center (OCC) operator. Additionally, with many transit systems in the process of implementing



Operator's mental model of process
Experience and training
Decision making and problem solving
Formal and informal procedures
Human Opertaor
Central Processing Unit
Human-System Interface (e.g., computer screen, warnings, controls, etc.)
Digitally Operated Sensing Devices
Programmable Logic Controller
Digitally Operated Control Devices
Transit System Operations
Transit System Supervisory Interface

Figure 1. OCC Operators role in a modern transit system.

Automated Train Control Systems (ATCS), the OCC operator will become even more burdened with responsibility. This increased workload inherently lends itself to increased human error and decreased worker job satisfaction. Therefore, the importance of matching the OCC operator personnel to the new transit control environment is significantly increased.

Standard OCC operator selection is often accomplished in the same manner as other employee types (e.g., clerical, management, etc.) through standard interview processes. However, the OCC operator position is very complex, with specific responsibilities and significant public consequence with a potential for some risk. The selection of the OCC operator should be comprehensive and reliable in its methodology.

The OCC operator selection process should apply a systematic approach that considers desired candidate attributes and are applicable to all applicants in an unbiased and objective manner. Defining the traits and criteria for the OCC operator job form the foundation of the selection process. These traits or aptitudes are uncovered through task and link analyses of the OCC. Once defined, a structured testing and evaluation of the candidates can then be performed. Additionally, personnel training and training criteria must be considered when determining the approach for the operator selection process.

Selection Criteria

The Law of Requisite Variety (Ashby, 1956) states that complex systems require complex operators. The complexity of a system must be dealt with in some way, design, machine, or operator. Additionally, since the human factors element is usually not considered during the design stage, the operator must adapt to potential human factors design deficiencies. Operation of the transit system combined with potential OCC design issues requires an operator that is both vigilant and self-sufficient. The traits and mental attributes of an OCC operator are the basis for no other ability to understand the transit system from a remote location. These assessments include defining the optimum operator mental model and performing both a task and link analysis.

Mental Model

The mental model is an important factor when understanding and verifying the desired OCC operator aptitudes and traits. Any operator, regardless of the level of complexity of the system, must possess a mental model of that system (Francis and Wonham, 1976). According to Meshkati (1991), "Mental models provide the foundation of which operator experience and learning are based while engaged in OCC monitoring and supervision." A well-defined operational mental model allows the operator to concentrate on the critical tasks while ignoring inconsequential decisions. Systems Engineer, Dr. Jens Rasmussen (Rasmussen, 1983), has created a mental framework that provides understanding of the operator-system interface of complex automated systems. Known as the Rasmussen Model of Cognitive Control, or SRK, this model encompasses three basic steps which the OCC operator can understand and use to act on the system, as seen in Table 1 below.

Table 1. Three Levels of Rasmussen's SRK Mental Model

Level of System Understanding	Operator's Traits of System Comprehension
Skill Based Behavior	• Actions are based on simple tasks Perform tasks without conscious thought, e.g., normal track allocation.
Rule Based Behavior	• Actions are based on rules or procedures • Perform these tasks through using mental sequences, or stored rules Rules are learned from actual "Rules and Procedures" and experience, e.g., track work performed during revenue operation.
Knowledge Based Behavior	• Requires complete understanding of system • Comprehension of the transit systems state from the OCC through controls and warnings • Requires analysis of the system state with calculated risk, adaptation, and prediction Operator as decision-maker and improviser, e.g., initiation of emergency ventilation and the OCC command does not work, requiring manual improvisation.

Figure 2 provides a graphical representation of Rasmussen's SRK model. This figure demonstrates the levels of operator cognitive control of the system. The three levels use different thought processes to act on the system's state. The greater the complexity of the transit system's state, the higher the level of required cognitive control. If all systems are performing properly during normal operations, then the operator must simply monitor the

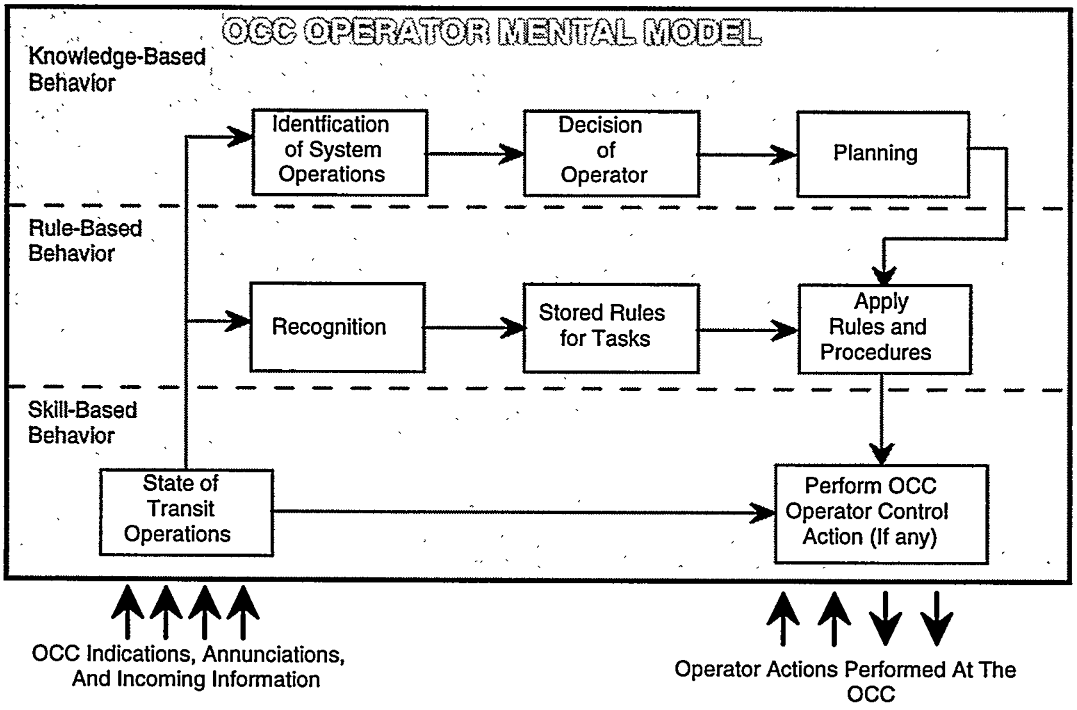

OCC OPERATOR MENTAL MODEL
Knowledge-Based Behavior
Identification of System Operations
Decision of Operator
Planning
Rule-Based Behavior
Recognition
Stored Rules for Tasks
Apply Rules and Procedures
Skill-Based Behavior
State of Transit Operations
Perform OCC Operator Control Action (If any)
OCC Indications, Annunciations, And Incoming Information
Operator Actions Performed At The OCC

Figure 2. SRK mental model of OCC operator and transit system.

supervisory systems, a skill- or rule-based level task. However, if a system is not in normal operation or an emergency arises (e.g., vehicle breakdown, fire, etc.) then the operator must improvise and make decisions that effect the system, using knowledge-based thinking.

Operator Selection

As technological advancements are incorporated in transit systems (e.g., SCADA, ATCS, etc.) the criteria for OCC operator selection must also be upgraded. The evolving transit environment and objectives of the operator will require different traits (i.e., vigilance, well-defined mental model of transit system) and training requirements. The previous section, which described selection criteria, is the basis of the actual selection process. The selection process for the OCC operator must consider many facets of personality as well as applicable transferable experience. The methods to assess ones ability to perform the demands of the OCC operator job can be measured through numerous tests, surveys, and interviews. Figure 3 demonstrates a thorough, unbiased, and reliable operator selection process. This process, though more time consuming than a standard interview-based selection process, would result in selecting an operator best fit for the OCC position.

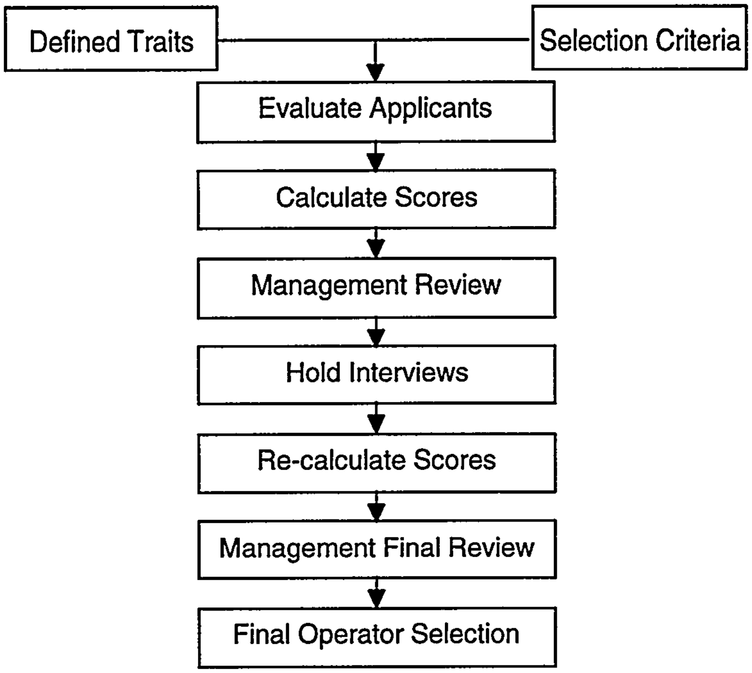


Figure 3. OCC operator personnel selection process flow diagram.

Desired OCC Operator Traits

Desired traits used selecting the OCC Operator will include some of the following characteristics:

1. Ability to solve complex problems.
2. Extensive experience with the existing transit systems.
3. Ability to follow comprehensive rules and procedures.
4. Aptitude for deductive and inductive logical thinking.
5. Possess the temperament needed to handle the demands of OCC operation:

   - Remain vigilant during normal operations, monitoring the system
   - Possess an advanced mental model capable of sustaining "Knowledge-Based Thinking"
   - Apply this mental model directly, reliably, and quickly during emergency situations

6. Past experience with computer based supervisory systems.
7. Ability to communicate clear and concise actions (e.g., deadhead moves, emergency response actions, etc.).

Testing

The selection of OCC operator candidates should include some tests that can assess a candidate's basic thinking ability and personality type. Testing for thinking ability (e.g., Ability and Aptitude Tests or Minnesota Paper Form Board, etc.) can demonstrate a candidates ability to understand a problem, logically break it down, and arrive at a solution. Personality tests (e.g., Guilford-Zimmerman Temperament Survey, etc.) can assess a candidates ability to cope with numerous stressors (e.g., alarms, warnings, annunciations, etc.). The test results provide the selection committee with a accurate measurement of a candidate's ability to logically diagnose system problems, specifically during emergencies. These tests should be unbiased and applied to the all applicants for consistency and testing validity. Specific issues regarding testing methods include:

- All applicants are asked the same questions.
- All questions are related to the job.
- The scoring of the responses are the same for all applicants.
- The tests are accurate in predicting job-related criteria.

Interview

The interview is a standard technique that is commonly used throughout all industries. This type of experience elicitation is proficient at assessing ones direct understanding of OCC background. Additionally, the interview allows working peers as well as management an opportunity to observe the candidate's ability to communicate his or her thoughts and ideas in "real-time." This can be useful since any future operator will be communicating with all types of transit personnel or passengers (e.g., maintenance employees, traction power team, vehicle operators, etc.).

Micro Human Factors

As human factors issues are uncovered, recommendations for improving OCC operator performance can be incorporated in the facility design and management approach. This paper will present a systematic approach to assess human factors-related issues for a typical transit system OCC. Figure 4 illustrates the general relationship between micro and macro human factors issues.

The OCC operator's primary responsibility is to monitor system status as presented on the SCADA terminal. This role as "system monitor" has created a working environment that requires vigilance during normal system operation and critical incident response actions during emergencies. To be effective, the interface between the SCADA system and OCC operator requires an efficient and coherent workstation. Factors that contribute to the usability of OCC workstations include:

- Video Display Terminals (VDTs)
- Overhead Screen Displays

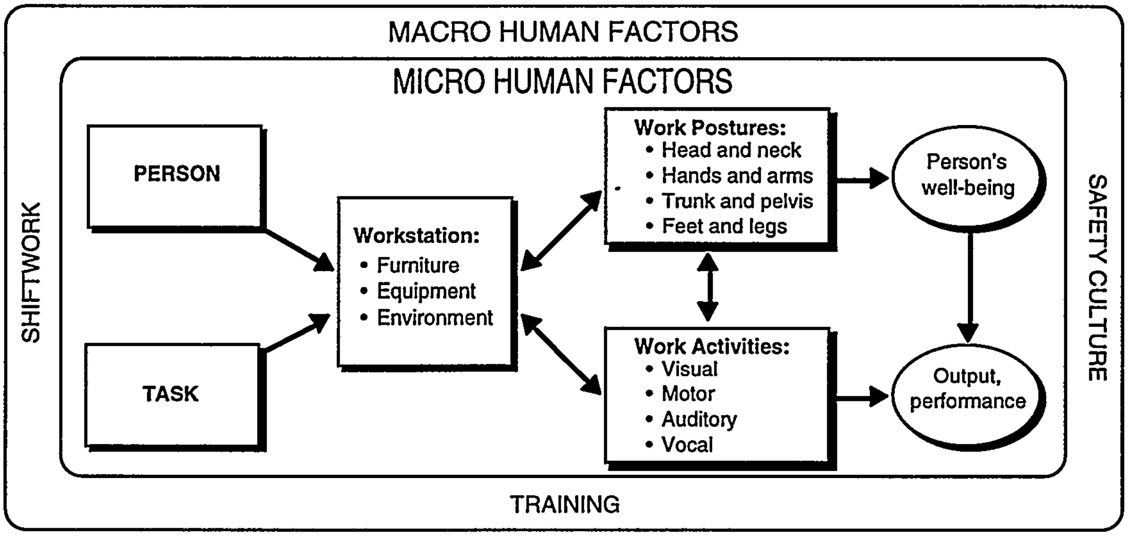


Figure 4. Human factors interaction diagram.

- Keyboard
- Chair Design

Table 2 identifies equipment and issues that may reduce the effectiveness of the OCC operator. When assessing the OCC workstation, one should consider factors that contribute to the degradation of human performance. The design and setup of OCC workstations can significantly impact the reliability and safety of the rail system.

An OCC human factors assessment should utilize the most current human factors methodologies including:

- Human Factors Standards
- Task Analysis
- Link Analysis
- Organizational Assessments

Task Analysis

A task analysis is the initial step in defining the criteria used to select an OCC operator. The purpose of task analysis is to provide a very detailed definition of the OCC required operator skills, system design deficiencies, and issues that would require specific training focus. Task analysis defines the actions that should be performed by the operator and the operator-machine interfaces (e.g., controls, warnings, equipment, etc.) that may accompany such tasks. Job factors are then determined, allowing procedures, personnel selection, training requirements, and evaluation of the existing system to be defined. Task analysis is the heart of the OCC operator personnel selection process assessment. The process for developing a task analysis is outlined in Table 3.

Table 2. Human Factors Considerations for Workstation Design

Equipment	Considerations
Video Display Terminal (VDT)	• Location of the screen should allow the operator to look straight ahead or slightly down. • Screen should be at right angles to the operator. • Screen color and contrast should be adjustable. • Operator should be between 18 to 28 inches from the screen. • Reduction of all glare and reflection.
Overhead Screen Display	• Use a high-resolution monitor or overhead projector. • Adjust color so that it is compatible to the operator's mental model of the control and warning hardware. • Adjust brightness and contrast levels to reduce operator fatigue. • Reduce blinking and numerous warnings, leaving these for only most important issues.
Keyboard	• Adjust height and distance in conjunction with operator's anthropometry, this may require installation of a lower keyboard tray. • Tilt the keyboard so that operators forearms are level and the wrists are nearly horizontal, when using the keyboard. • Use wrist pads. • Adjust chair armrests to support the forearms.
Chair	• Is the chair adjustable, if so, has this feature been used? • Adjust backrest to support lumbar. • Lower chair until feet are flat on the floor and there is little or no pressure on the back of the thighs. If operator is too low for proper view of the control area, raise chair and provide a footrest. • Provide a chair with a large seat pan and cushioned with a firm non-slide fabric.
Workstation	• Provide task lighting that is below the operator's line of sight to avoid direct light. • Task lighting should provide enough light to perform hard-copy tasks. • Allow the workstation to be adjustable to the operator population, within financial feasibility. • Provide unobstructed legroom to allow free operator movement. • Provide sufficient desk space necessary for hard-copy tasks.

Table 3. Task Analysis Procedure Checklist

Step	Task
1	Identify all tasks that must be performed in order to accomplish OCC operations.
2	Break tasks down into detailed steps that are required to accomplish the task.
3	Analyze each step to determine the following critical factors: • Instruments/warnings that initiate an action • Information and decisions required of the operator • Actions required • Feedback information • Potential errors or stressors • Criterion for successfully completing a task
4	Determine criticality and difficulty of task.
5	Identify training requirements unique to this task.

This human factors assessment technique, for example, might find the following:

- The primary task of the central control operator is to monitor train movement.
- Concurrently, the operator is required to monitor critical safety and security subsystems.
- Subsystems eventually require emergency response management.

Link Analysis

Link analysis is a human factors technique that assists the evaluation of OCC operations. The link analysis defines physical tasks and equipment that the operator interfaces with on a consistent basis. Once an interface frequency list is defined, operator selection criteria can be adapted to focus on those candidates that have experience with pertinent equipment. Additionally, the link analysis will define training requirements of highly used equipment and also focus on that equipment that is not used but is critical to transit system safety and reliability (e.g., fire suppression system, intrusion detection, seismic sensors, flood level indicators, etc.). Common relationships used in human factors are:

- Comparison of display/control requirements with control room inventory.
- Control room survey to identify deviations from accepted human factors principles.
- Selection and assessment of human engineering discrepancies to determine which discrepancies are significant.
- Selection and prioritization of design improvements.

- Determination of the relative frequency of an operator going from one task element to another.
- Frequency of communications.
- Operator perceptual and decision-making capabilities.
- The relative importance of each factor (emergency vs. non-critical action).

Macro Factors Issues

Public rail transit is more than just a collection of its systems and subsystems; it is a reflection of the structure, management, procedures, and culture of the organizations that create and operate them. Public transit rail systems tend to place the onus of an accident on human errors or equipment failures without recognizing the organizational and managerial factors that impact the root causes of accidents. The causes of rail system accidents are typically rooted in the management and organization structure. Potential macro human factors issues that may impact operator effectiveness include:

- Training
- Shiftwork design
- Safety culture

The results of the task analysis described earlier in this paper provide valuable input for the development of an effective training program. Task analysis is an integral part of the instructional development process. This human factors assessment technique provides OCC management with the information needed to devise a comprehensive training approach. Tasks, priorities, emergency response actions, and the control interface are the foundation for the training program of a safe and efficient OCC operation.

Shiftwork

Present public rail transit systems require OCC operators to perform on a 24-hour, 7-day-a-week, 365-day a year schedule. Therefore, normal operations or maintenance procedures require that these operators remain vigilant during every moment that they perform their tasks. Hence shiftwork, or the scheduling of operators to be on duty at all times, requires specialized planning and coordination of the shift length, shift rotation, and vacation days.

Shift Length

Various shiftwork studies regarding OCC operators from a multitude of applicable industrial sectors, including rail operations, have come to some conclusive findings regarding shift length and shift rotation. Shown in Table 4 and Table 5 are the two most common shift lengths used by OCC operators.

Table 4. Eight Hour Shift Length Factors

Advantages	Disadvantages
Improved operator learning performance, increased cognitive ability.	Decrease in operator productivity.
Operator fatigue is less susceptible to performance decrement, and operator error.	Potential operator job dissatisfaction due to lack of large blocks of vacation time.
Risk of operator error is minimally affected.	Increased absenteeism due to job dissatisfaction.

Table 5. Twelve Hour Shift Length Factors

Advantages	Disadvantages
Increase in productivity compared to the eight-hour shift.	Significant decrement in operator mental performance towards end of shift.
Operator stress is reduced due to the longer blocks of free time.	Significant decrease in hand-eye coordination.
Increased job satisfaction (larger vacation blocks).	Increased sleepiness and fatigue.
Reduced of operator absenteeism.	Follow-up studies have found no significant performance adaptation over time.

Shift Rotation

Operators that are required to perform shiftwork can be scheduled so that their shifts start at varying times relative to their past shift start points. An operator shift can be "rotated" forward or backwards. This rotation can affect the internal clock (circadian rhythm) of each individual operator.

Forward Rotation - Forward rotation shifts (i.e., from an 8 a.m. start time to a 4 p.m. start time) allows the operator time to adapt to the new schedule. Thus, the risk of error is minimized.

Backward Rotation - Backward rotating shifts (i.e., from an 8 a.m. start time to a 12 a.m. start time) do not allow the adaptation of the operator's internal clock (circadian rhythm) to adjust. This maladjustment can be directly correlated to decrement in operator performance and increased mental fatigue.

Safety Culture

Safety, culture is the general approach to human factors and safety that is reflected in management and workers attitudes and beliefs. Major accidents often stem from an inappropriate or dysfunctional safety culture that may be characterized by overconfidence and complacency, disregard for safety, and flawed resolution of conflicting goals. It is considered acceptable practice that the genesis of a design should include human factors input. However, including human factors analysis at the design stage may require extensive upper management support to insure such analyses are adequately performed and their results are incorporated into the design. The benefits of a healthy safety culture may not be immediately noticeable, but a rail-transit organization that encourages appropriate attitudes toward human factors and safety, will receive long term benefits through improved productivity and reduced accidents.

Training

Additional safety systems, line extensions into other transit corridors, and software changes, will require the OCC operator to perform training. Likewise, the training program must be previously setup (based on task and link analysis findings) so that the selection process can hire an operator with a compatible amount of knowledge and transit operations experience. These human factors assessment techniques provide the OCC with the information needed to prepare a comprehensive training approach.

The process of training the OCC operators should require a systematic approach to instruction that emphasizes:

- Goals and objectives
- Transition from old OCC equipment to updated equipment or software
- Transfer of past transit experience and control to the OCC system
- Training improvement
- Supervisory equipment training strategies including: planning, teaching, monitoring, intervening, and learning about the SCADA system.

There are five basic phases to consider when using a systematic approach to OCC training. These are outlined in Table 6.

Simulator Training

OCC simulator training should be incorporated into all applicable OCC training programs. Equivalent equipment should be provided in order to attain compatibility between the simulator system and the actual OCC control equipment. Several benefits of training with a simulator include:

Table 6. OCC Operator Training Plan Process

Phase	Method
Analysis	Analysis of the system, its required tasks, human-machine interface, and managerial expectations.
Design	Design the training to encompass the analysis stage as well as existing knowledge and desired instructional goal.
Develop	Develop the training around the OCC and its operators, this should include feedback from the operators and specifically relate back to the task analysis.
Implement	Implementation of the training program. To acquire organizational support, both operators and management must be involved.
Evaluate	Evaluate the existing program. This stage should be continuously performed to train the operators on any changes in hardware, software, or procedures.

- An opportunity to practice SOPs and EOPs without risk to the transit system.
- An opportunity to train at higher levels of skill than would be afforded in a reasonable time by on-the-job training.
- Reduction of accidents.
- Provide annual refresher training without disrupting transit service.
- Allow operators to experience new system additions or additional future corridors.
- Provide an environment in which errors and poor performance are tolerated and feedback can be given.
- Allow removal of distractions so that the operator can learn the basic skills in the best conditions.
- Isolate tasks that require further learning without having to endure all other tasks.
- More cost effective than training on real equipment.

Conclusion

The methodology outlined in this paper will help transit system managers select OCC operators. The process for selecting OCC operators should include:

- A task analysis to identify all tasks to be performed.
- A link analysis to identify operator-OCC equipment interfaces.
- Defined OCC operator desired traits and attributes.
- OCC-specific testing methods.
- Simulator training requirements.

The human factors approach to selecting OCC operators and training requirements will provide transit properties with a safer and more reliable transit system.

References

Ashby, W. R., (1956). An Introduction to Cybernetics. John Wiley, New York.

Clymer, A. B., (1985) Simulate Your Way to Safety. Hydrocarbon Processing. (Dec).

Fleger, S. A., and McWilliams, M. R. (1995). Control Room Human Factors Assessment at a Bulgarian Nuclear Power Plant. Proceedings of the Human Factors Society 39th Annual Meeting (pp. 1043-1047). Santa Monica, CA: Human Factors Society.

Francis, C. M. and Wonham, J. G., (1976). The Efficient Organization Centralizes in Order to Decentralize. Organizational Dynamics. 5(4): 3-14.

Meshkati, N., (1991). Integration of Workstation, Job, and Team Structure Design in Complex Human-Machine Systems: A Framework. International Journal of Industrial Ergonomics. 7 (1991) 111-122.

Rasmussen, J., (1983). Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models. IEEE Transactions on Systems, Man, and Cybernetics. 13(3): 257-266.

Walecki, K. F., (1996). Human Factors Assessment of the Operations Control Center. Proceedings of the American Public Transit Association 1996 Rapid Transit Conference, June 1996. Washington DC: APTA.

Biography

Kurt F. Walecki AHFP
Booz·Allen & Hamilton
523 West Sixth Street, Suite 650
Los Angeles, CA 90014

Mr. Walecki provides system safety and human factors support at Booz·Allen & Hamilton primarily for transportation modes. Before working for Booz·Allen he was Principle Ergonomist and Safety Advisor for Irwin Industries, a refinery contractor in the LA Basin. His education includes a Master of Science in Human Factors from the University of Southern California and a Bachelor of Science in Industrial Psychology from the California Polytechnic University at San Luis Obispo. He is a member of the Human Factors and Ergonomics Society.

Human Factors Issues in High Consequence Systems

Jerry M. Childs
BDM International
Albuquerque, New Mexico

Abstract

This paper sets forth the need for the application of human factors tools in the design and implementation of emerging high consequence operational systems. It focuses on the need to consider human performance in conjunction with these new technology-based systems. Several concepts and tools are described for ensuring that human performance issues are addressed early and often in the systems-acquisition cycle.

Introduction

Technology-based tools can enhance system performance if used correctly by managers, operators, and maintainers. However, world-class organizations are known by their people - not their technology (Childs, Courtright, and Murphy, 1990). When Microsoft is mentioned, we may more readily think of Bill Gates and his software engineering staff than Windows 95 or Excel. Southwest Airlines may elicit visions of Herb Kelleher and the employee 'family' rather than ticketless travel or flight-management systems. So, technology cannot eliminate human-in-the-loop performance issues. In fact, technology has increased the need for designs that apply principles of human performance (Sarter and Woods, 1995; Meister, 1996). Totally automated systems have been known to fail, requiring manual interventions. Semi-automated systems may give misleading data or lack information to facilitate operator decision making. High consequence operations involving nuclear materials, air transportation, weapons systems, and command and control systems linked to national security pose an even greater need to focus on human factors because of the potentially disastrous human-mediated consequences of systems failure.

Human Performance and Technology

Over the past 20 years, two trends have emerged that dramatically impact human performance in systems operations. First, the cost-intensiveness of implementing technology-based systems has shifted dramatically from hardware/software to human performance (Figure 1). Most current supervisory control systems are reliant on effective human performance to maintain high levels of effectiveness and safety (Childs, 1992). This is exemplified by military, airline, and air traffic control initiatives to design and implement systems that are more compatible with the perceptual, learning, and motivational capabilities of users.

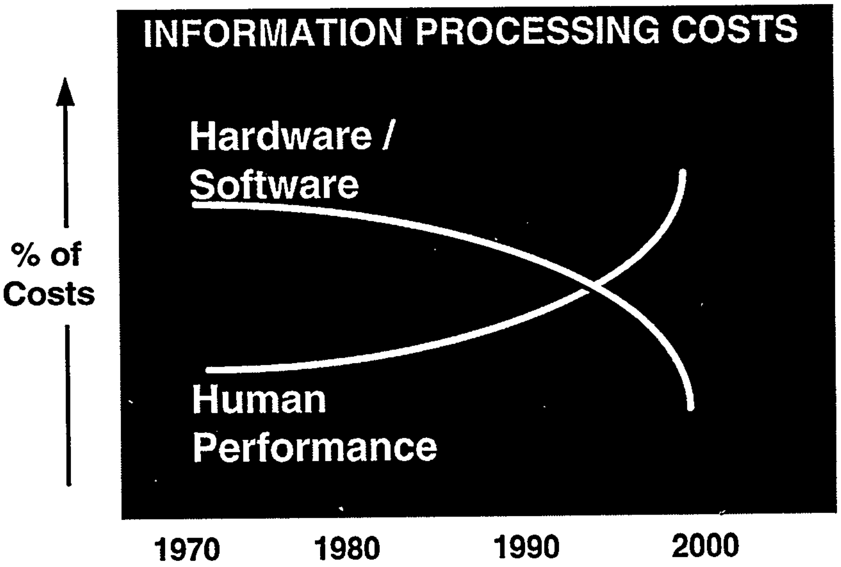


Figure 1. Human performance vs. technology costs.

The second trend is related to system reliability. While the reliability of technology has experienced a steady increase, human performance reliability has remained fairly constant, lagging behind technology and creating a gap in our ability to effectively operate and manage newer automated systems. For example, for nearly 30 years, human performance errors have accounted as causal or contributing factors for at least 70% of all aviation accidents and incidents. This is in spite of the implementation of automated flight control, navigation, and management systems, digital voice recognition systems, alert and warning systems, and other advanced technology.

Need for Function Allocation

For any emerging high-consequence system, work functions should be assigned to people and technology based on the strengths and vulnerabilities of each (Figure 2). System designers have moved away from function analyses and allocations in emerging technology-based systems. This is ironic since these newer systems pose an even greater need for such efforts than conventional systems that were implemented 30 years ago. Generally, people are more adaptive than computer-mediated systems, and despite outcomes from Kasparov verses IBM Big Blue chess matches, are better suited to judgments and decision making based on experience. People are able to use inductive and deductive reasoning based on very intangible data. Technology should be used to gather, process, store, collate, and compute information rapidly and efficiently. Technology tends to be more reliable and uniform in task and job execution than humans who are more prone to be adversely affected by environmental stressors, and thus, more subject to performance variability.

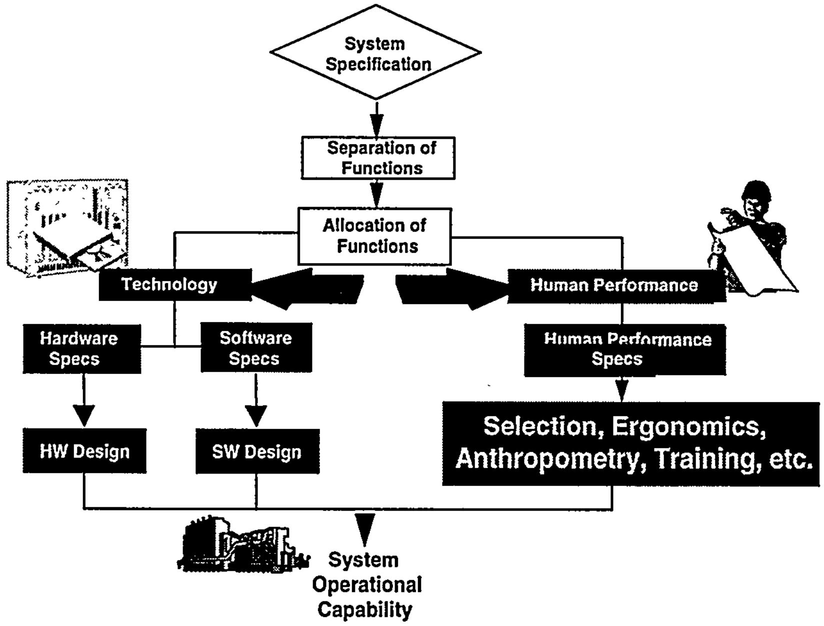


Figure 2. The Function Allocation Process.

Target Audience Identification

Another frequently overlooked, yet critical activity concerns definition of the target audience group for the new system. Human factors in high consequence operations should be linked to the performance and experience characteristics of system operators, managers, maintainers as well as other users. Data are required on their background, skills, experience, motivatiòn, aptitudes, and learning styles. Systems management skills are important to job success as are situation awareness and decision making skills. Components of an effective target audience analysis are shown in Figure 3.

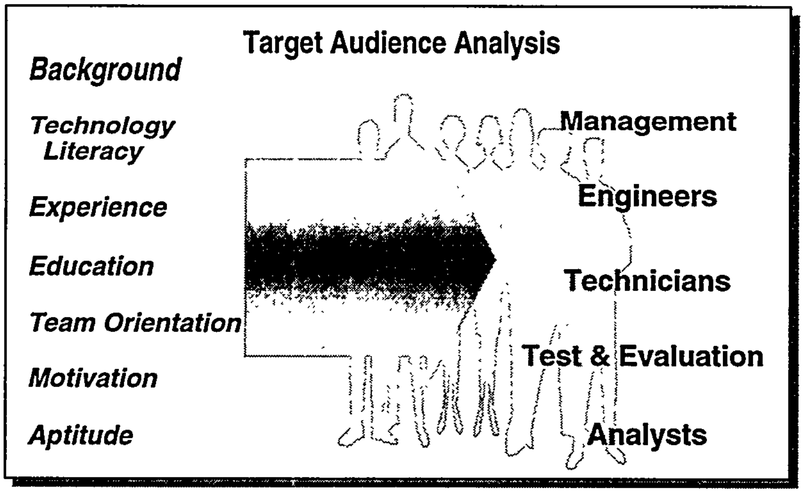


Figure 3. Target Audience Analysis Components.

Effective Human Engineering

The effectiveness of operational systems depends upon the safe and proficient performance of operators and maintainers. Training plays an important role in achieving this goal. However, the fielded systems should be human engineered to provide:

- User-oriented controls.
- Displays that are user-legible and that are functionally integrated with the control systems.
- Operating status information that is easy to access, interpret and act upon.
- Workspace that is designed to minimize performance error.
- A safe, comfortable working environment.

Effective human engineering at least partially mitigates the need for redesign and 'train-arounds' required to optimize post-implementation human performance. Experience has shown that addressing human engineering issues early and continuously in system design can reduce human performance error, improve productivity, increase morale, and prevent catastrophic loss in the fielded systems. The human-technology interface is shown in Figure 4.

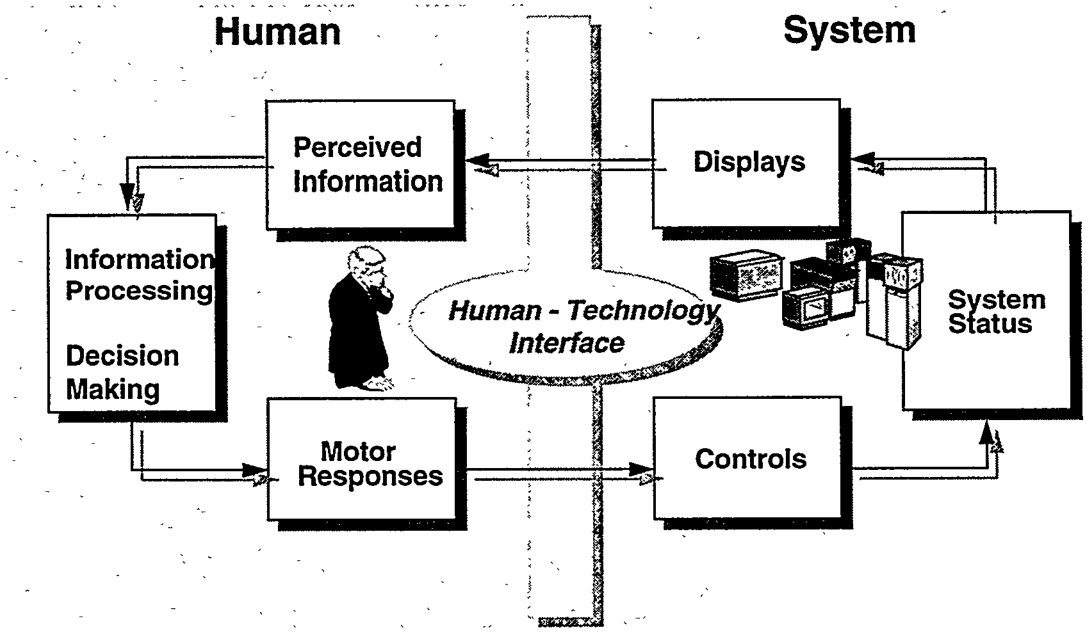


Figure 4. Human-technology interface.

Note that the interface is a closed loop. Humans affect system performance through control inputs resulting from perception, information processing, and decision making. System outputs then are displayed which lead to further human performance modifications to yield desired system states. This interface is responsible for the integrity and effectiveness of operational systems. When the interface is adversely affected, system performance suffers and safety compromises may result.

Human Performance Factors in System Design

Human performance factors that should be addressed in the design of systems as well as the modification of existing systems are shown in Figure 5 (adapted from National Transportation Safety Board, 1983). Recruiting and selection of people to staff critical job functions should take into consideration these factors and their interrelationships.

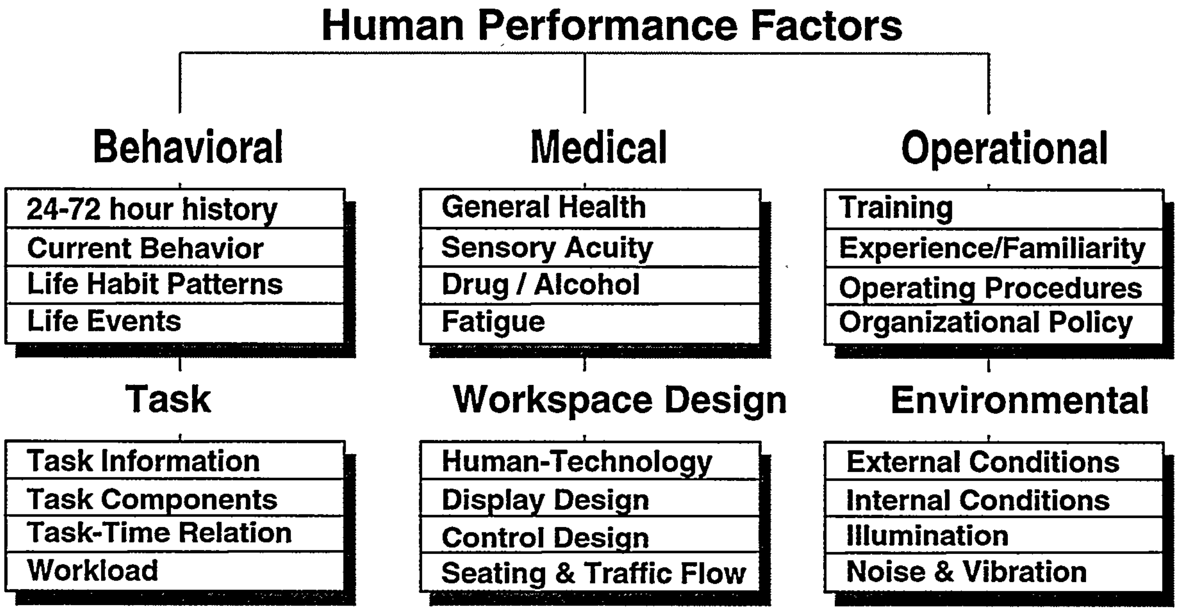


Figure 5 Human performance factors affecting system effectiveness (adapted from NTSB, 1983).

Human Engineering Activities in High Consequence Systems

Four human factors measurement domains that are of particular interest for high consequence operations are:

- Mode Awareness
- Situation Awareness
- Resource Management
- Automation With and Without Manual Override Capabilities

Human engineering of high consequence systems can involve any or all of the following tasks within those domains:

1. *Anthropometry and Usability* - Design of operator workspace to accommodate the full range of size, control reach, viewing angles and distances of the projected operators and maintainers of the system. Design for Maintainability (DFM) concepts may be employed. A broad range of automated anthropometric tools (O'Brien, 1996)

is available to assess the effects of system component size and placement on human usability during the design phase. This prevents costly modifications to the system after implementation.

2. *Control and Display Design Inputs* - System controls should be easy to reach, operate, and program (Van Cott and Kinkade, 1972). They should be logically compatible with displays that depict the information resulting from control and programming inputs. Screens should be uncluttered and display normal and off-normal condition data that are easy to interpret. Displayed information should be consistent with users' expectations and experience. User culture and experience should be considered in display design. Color, size, and shape coding can be used to facilitate control access and use. There should be little or no lag in display response to control inputs. Human factors design principles should be applied to the selection and use of screen colors and graphics. This will enhance operator processing and use of information. Symbology should be easy to interpret. Figure/background contrast should be sufficient to enable operators to easily interpret displayed information within the range of ambient illumination expected for unit operations. Screen glare should be minimized and screens should swivel to accommodate desired viewing angles. Standard human factors engineering guidelines such as those contained in MIL-STD 1472 D can be used to enhance usability and safety.

3. *Workspace Design for Control Stations* - Workspace within system control stations should permit operators to move freely whether seated or standing, should enable them to view and access needed information on demand, and should minimize ambient noise, heat, cold, vibration, humidity, dust, and other adverse conditions (McCormick and Sanders, 1982). Operator clothing worn in very cold conditions should permit operators to accurately enter information on computer keyboards and touch screens. Adequate ventilation should be provided for operations in hot, humid conditions.

4. *Alarm and Warning Systems* - Visual and auditory warning systems should enable operators to easily detect and quickly respond to off normal and emergency conditions (Weiner and Nagel, 1988). Sensory modes used for alarms should signal undesirable trends in temperature, pressure, fuel flow, and system capacities. Containers and other system components should be clearly marked and the content and format of safety labels and markings should follow military standards or best commercial practices.

5. *Lighting, Noise, Vibration, Temperature, and Ventilation Concerns* - Facilities used to house critical operating systems should be adequately lighted and ventilated for operator access and use (McCormick, 1976). This includes the workspace surrounding hazardous materials, holding tanks, conversion units, rail cars, etc . Tests should be conducted to ensure that operators can see and hear all critical sources of unit operating information throughout the workspace. Protective clothing worn outside control rooms should permit easy access to, and use of, all controls and support equipment. Ambient noise - both intermittent and continuous - should be

attenuated to within acceptable auditory limits. Job areas should be free of excessive vibration and should be adequately ventilated.

6. *Communication Issues* - Operators and maintainers should be capable of communicating verbally either face-to-face or electronically, as required. Effective written communication also should be included in status and operating reports, memos, and other correspondence. Work planning and scheduling should be a vital part of the communication process as should change of shifts. Ear protection that may be necessary to attenuate ambient noise will need to be easily removable to allow clear voice communications. Listening skills should be cultivated for team-based operations. The importance of effective crew communications in the crash of an Avianca B-707 can be assessed by reviewing Orasanu (1995) and the NTSB report (NTSB, 1991) of the accident.

7. *Information Access and Retrieval* - Operators and maintainers should be able to quickly access and retrieve critical operating and maintenance data. Data entry should be minimal and aggregated to present system performance trends and summaries on demand. Information should be displayable to users in both electronic and manual formats. Information display modes should be selectable by operators. Back-up displays should be available in the event of power outages.

8. *Human-Computer Dialogue* - Information displayed should not require decoding and recoding for operator interpretation. Dialogue by graphical schematics and other conceptual representations of the system structure. Operators should be provided within and across various human-computer interfaces should be consistent in format and procedure. Operators should not be required to maintain an excessive amount of information in short-term memory and memory aids should be provided where possible. User navigation through the system interface should be aided with frequent and rapid feedback and automatic error detection and correction, where possible.

   Mental workload should be minimized by automating computational processes and providing critical systems status data on demand (Kantowitz and Casper, 1988). Decision aiding should be embedded into the system control software. Design considerations should include the incorporation of a manual override capability, with appropriate error checking and query, for automated control functions. Some degree of user-tailoring of the human-computer interface should be possible to accommodate individual differences. Training should address the above human-computer issues as well.

9. *Attention and Vigilance* - The professional literature on operator attention and vigilance indicates that people do not maintain high levels of vigilance for detecting and responding to critical operational signals over extended time periods. In fact, depending on task and signal complexity and the monotony of the work setting, proficiency can be expected to drop well below 80% after one hour on duty (in some instances, signal detection has dropped below 50%). Thus, for systems requiring extended monitoring tasks, visual, auditory, and other external cues will likely be necessary to sustain operator performance over 8-10 hour shifts. As operating data

become available, methods for maintaining operator vigilance should be designed to enhance attention.

10. *Work-Rest Cycles* - Operator work-rest cycles over calendar time need to be addressed to ensure optimal productivity and morale and to reduce the effects of cumulative fatigue, especially in hazardous operating environments.

Human Factors Evaluation

To effectively measure and assess human performance in advanced technology systems, we must address the concept of desired performance. That is, we must first determine the desired process and outcomes of human-in-the-loop performance. This generally is accomplished by gathering operational and mission data from subject matter experts (SMEs) or from job and task analyses. After desired performance is defined, we must measure the actual performance at designated sampling points within the operational or simulated setting. If desired performance matches actual performance (plus or minus an agreed-upon tolerance limit), no intervention is required. However, if the two measurements do not match, any of several interventions may be necessary. As shown in Figure 6, these may include human engineering, anthropometry, training, job redesign, or recruitment/selection revisions.

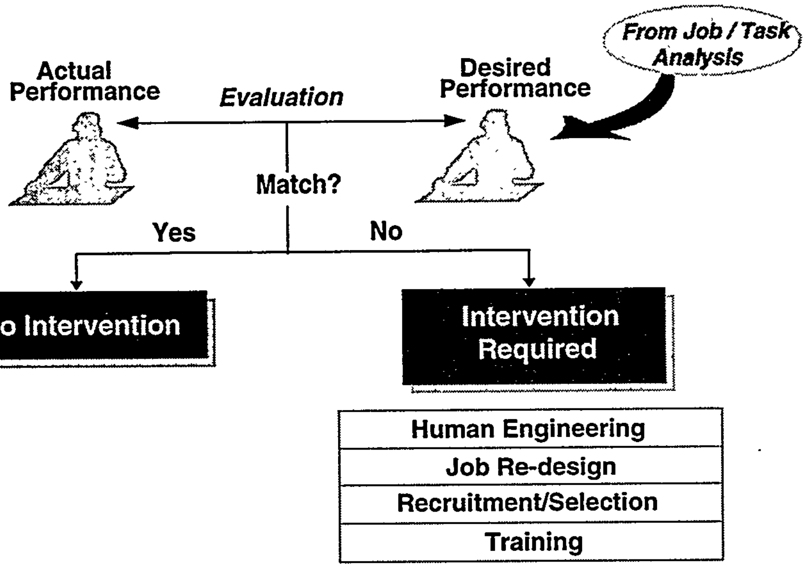


Figure 6. Actual verses desired performance assessment.

Human Performance Demands Imposed By New Technology

Following are some the factors associated with emerging technology that require us to focus on human performance characteristics:

- New digital color displays and symbology
- Cognitive and information processing demands
- Supervisory control for distributed architectures
- Attention and decision making in dynamic operations
- Increased situation and mode awareness by operators
- Electronic maintenance methods
- Systems and software management requirements

New Automation Calls For New Approaches

Human-in-the-Loop Scenario-Based Simulations can be used to identify system design needs and to correct human engineering deficiencies (Swezey, Streufert, Satish, and Siem, 1997). Scenarios can be constructed for many operational settings that impose time-based and event-based work requirements and constraints. Subjects can interact realistically with the simulations to determine the operational safety, effectiveness, and efficiency of the system prior to its implementation. A process for developing and implementing scenario-based simulations is shown in Figure 7. Work requirements and/or steps for each of the major development phases are identified to the right of each phase block.

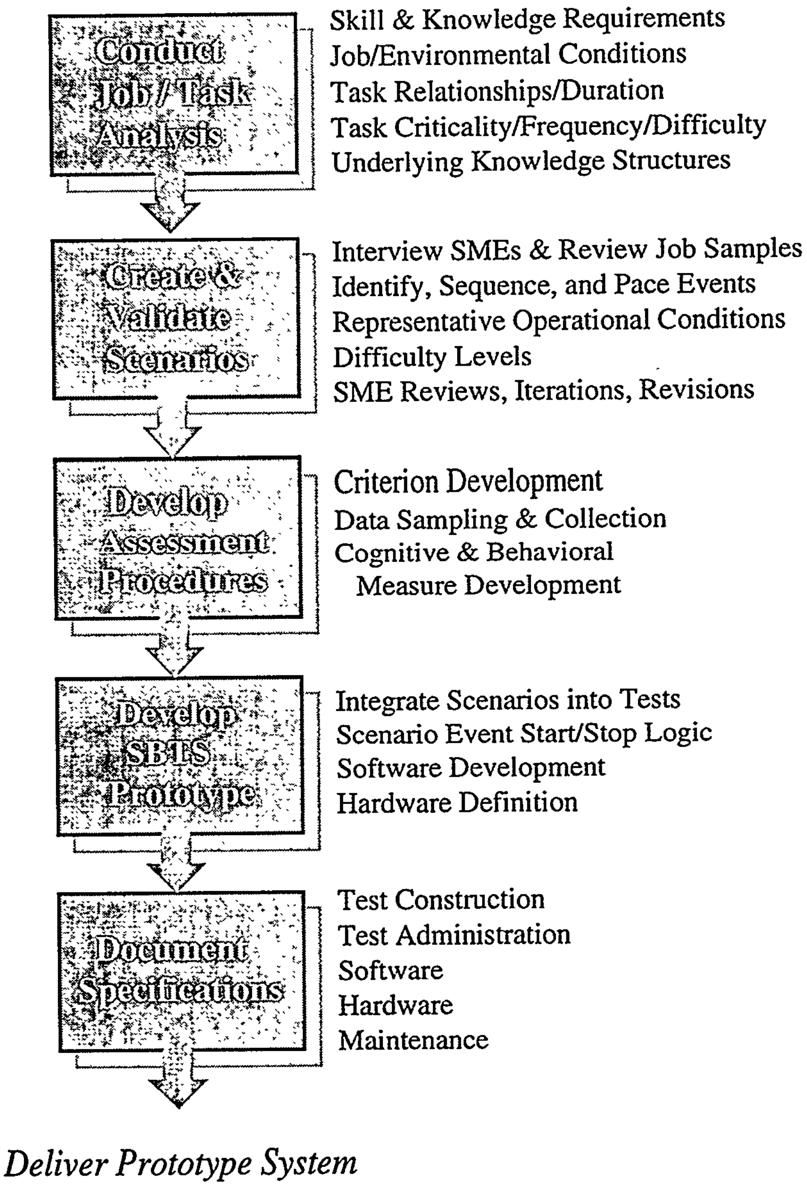

Conduct Job/Task Analysis
Skill & Knowledge Requirements
Job/Environmental Conditions
Task Relationships/Duration
Task Criticality/Frequency/Difficulty
Underlying Knowledge Structures
Create & Validate Scenarios
Interview SMEs & Review Job Samples
Identify, Sequence, and Pace Events
Representative Operational Conditions
Difficulty Levels
SME Reviews, Iterations, Revisions
Develop Assessment Procedures
Criterion Development
Data Sampling & Collection
Cognitive & Behavioral
Measure Development
Develop SBTS Prototype
Integrate Scenarios into Tests
Scenario Event Start/Stop Logic
Software Development
Hardware Definition
Document Specifications
Test Construction
Test Administration
Software
Hardware
Maintenance
Deliver Prototype System

Figure 7. Scenario-based simulation development.

References

Childs, J.M., J.F. Courtright, and W.A. Murphy. (1990) *Manufacturing Training Development and Evaluation - A Critical Element of Manufacturing Management Strategy,* Presented at the International Manufacturing Technology Conference, Society for Manufacturing Engineers, Chicago, IL.

Childs, J.M. (1992) Team Building and Training in the Design for Manufacturability. Volume 6, *Design for Manufacturability Handbook Series,* Dearborn, MI, Society for Manufacturing Engineers.

Kantowitz, B.H. and P.A. Casper. (1988) Human Workload in Aviation. in Wiener, E.L and D.C. Nagel (eds.) *Human Factors in Aviation.* Academic Press, Inc., San Diego, CA.

McCormick, E.J. and M. Sanders. (1982) *Human Factors in Engineering and Design.* McGraw Hill, New York, NY.

Meister, D. (1996) Human Factors Test and Evaluation in the Twenty-First Century. in O'Brien , T.G. and S.G. Charlton (eds.), *Handbook of Human Factors Testing and Evaluation.* Lawrence Erlbaum Assoc., Mahweh, NJ.

Military Standard , MIL-STD-1472. (1983) *Human engineering design criteria for military systems, equipment, and facilities. Washington,* DC.

National Transportation Safety Board. (1983) *Accident Investigation of human performance factors.* Washington, DC.

National Transportation Safety Board. (1991) *Aircraft Accident Report - Avianca, The Airline of Colombia, Boeing 707-321B, HK2016, Fuel Exhaustion, Cove Neck, New York, January 25, 1990,* (NTSB/AAR-91-04, Washington, DC.

O'Brien, T.G. (1996). Anthropometry, Workspace, and Environmental Test and Evaluation. in O'Brien , T.G. and S.G. Charlton (eds.), *Handbook of Human Factors Testing and Evaluation.* Lawrence Erlbaum Assoc., Mahweh, NJ.

Orasanu, J. (1995). Evaluating Team Situation Awareness Through Communication. in Garland, D.J.and Endsley, M.R. (eds.), *Proceedings from the Experimental Analysis and Measurement of Situation Awareness Conference*, pps 283-288, Daytona Beach, FL.

Sarter, N.B., and Woods, D.D. (1995) How in the world did we ever get into that mode? Mode error and awareness in supervisory control. *Human Factors,* 37(1), 5-19.

Swezey, R.W., S. Streufert, U. Satish, & F.R. Siem. (1997) *Preliminary development of a computer-based team performance assessment device (TPAD).* InterScience America, Inc., Leesburg, VA (submitted to USAF Armstrong Laboratory under Contract No. F41624-96-C-5010).

Van Kott, H.P., and R. Kinkade. (1972) Human Engineering Guide to Equipment Design. Washington, DC: American Institutes for Research. Government Publication.

Wiener, E.L. and D.C. Nagel. (1988) *Human Factors in Aviation.* Academic Press, Inc., San Diego, CA.

Biography

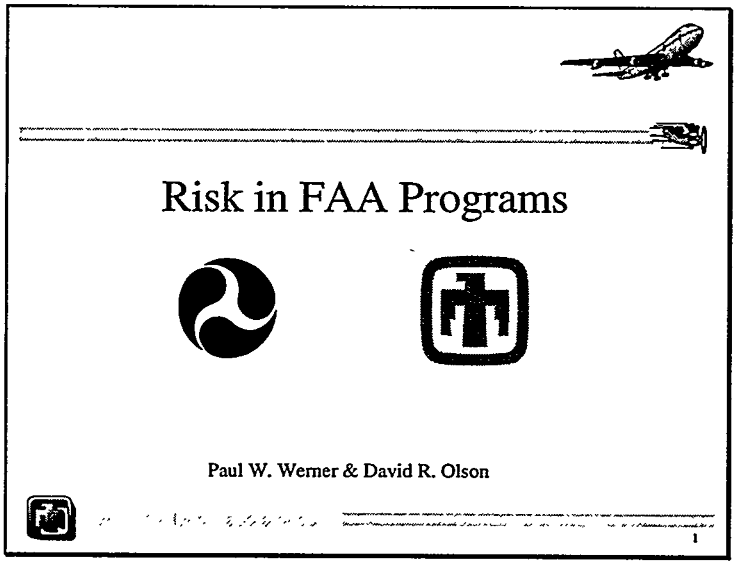
Jerry M. Childs, PhD
BDM International
1801 Randolph Road SE
Albuquerque, NM 87106

Dr. Childs is Director, Performance Engineering for BDM. He has 22 years experience in the development and management of human engineering and training systems programs sponsored by the government and commercial sectors. He was formerly Manager, Commercial Applications, with Hughes Training Inc. and Program Manager with Seville Research Corporation. He holds a PhD in Engineering Psychology from Texas Tech University.

Risk in FAA Programs

Paul F. Werner
David R. Olson
Sandia National Laboratories*
Albuquerque, New Mexico

Slide 1

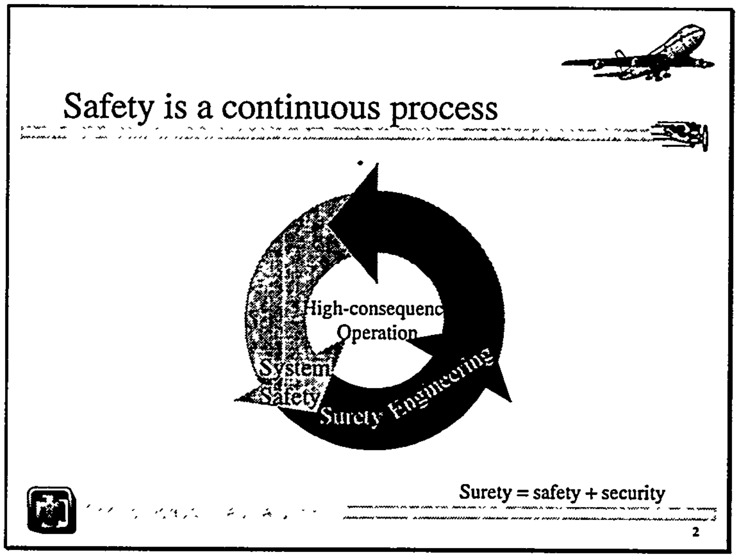


Risk in FAA Programs

Paul W. Werner & David R. Olson

1

Slide 2



Safety is a continuous process

High-consequence Operation

System Safety

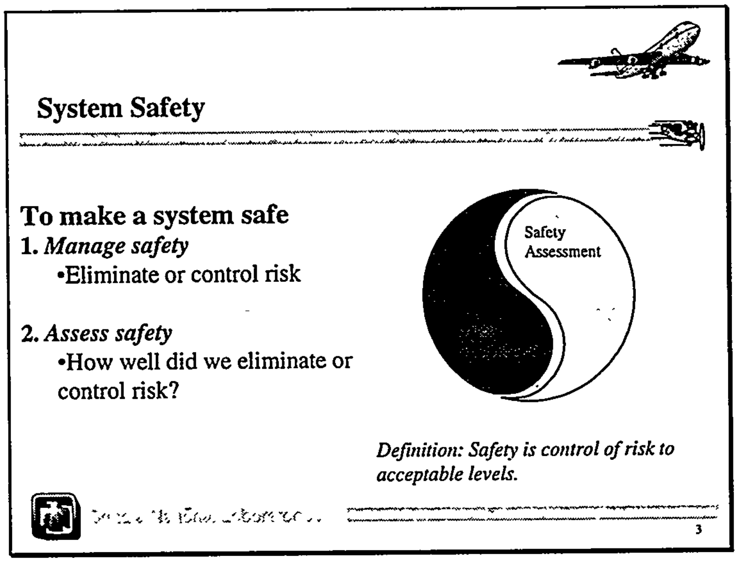
Surety Engineering

Surety = safety + security

2

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

Slide 3



System Safety

To make a system safe

1. ***Manage safety***

- Eliminate or control risk

2. ***Assess safety***

- How well did we eliminate or control risk?

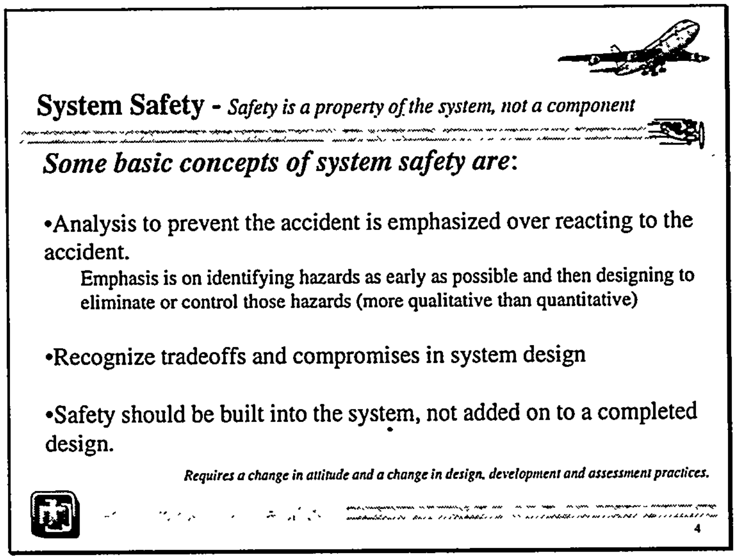
Safety Assessment

Definition: Safety is control of risk to acceptable levels.

[illegible]

3

Slide 4



System Safety - *Safety is a property of the system, not a component*

Some basic concepts of system safety are:

- Analysis to prevent the accident is emphasized over reacting to the accident.

  Emphasis is on identifying hazards as early as possible and then designing to eliminate or control those hazards (more qualitative than quantitative)

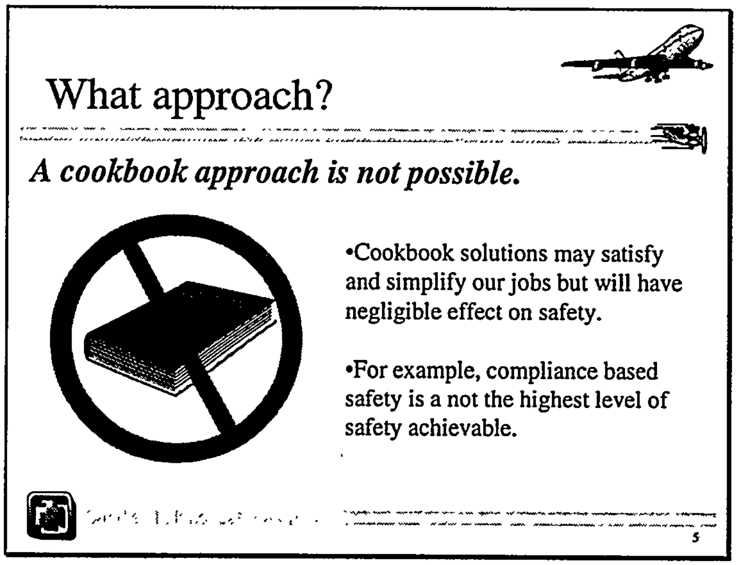
- Recognize tradeoffs and compromises in system design

- Safety should be built into the system, not added on to a completed design.

Requires a change in attitude and a change in design, development and assessment practices.

4

Slide 5

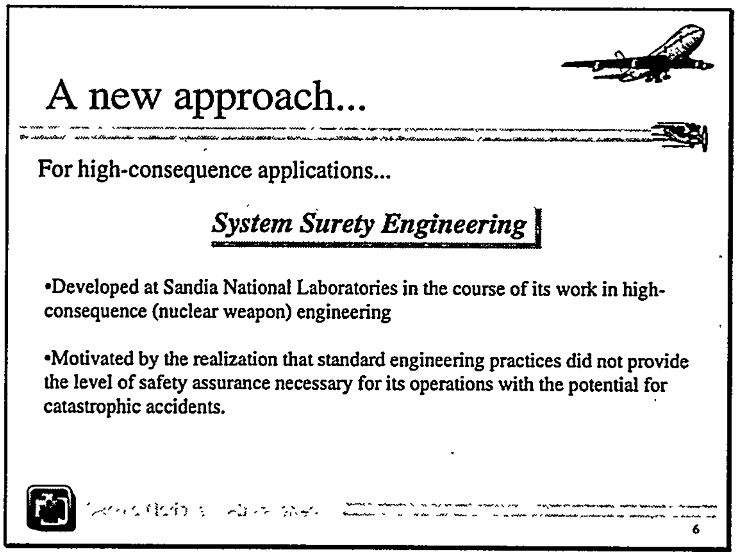


What approach?

A cookbook approach is not possible.

- Cookbook solutions may satisfy and simplify our jobs but will have negligible effect on safety.
- For example, compliance based safety is a not the highest level of safety achievable.

Slide 6



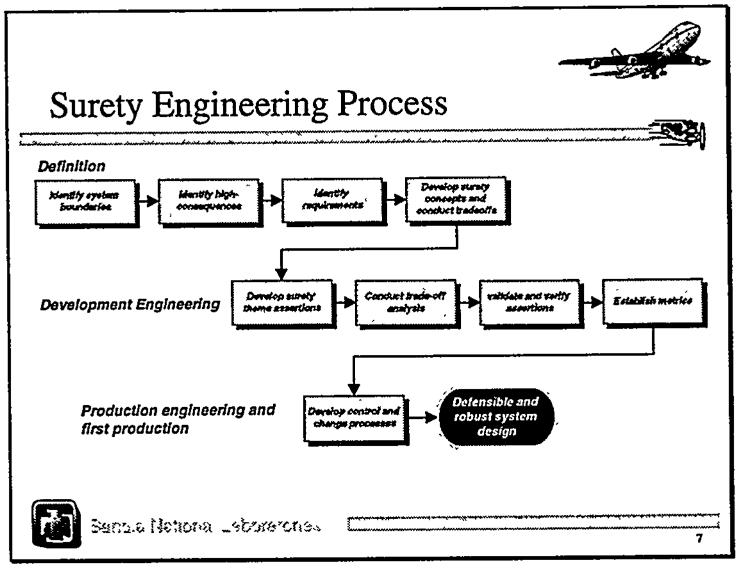
A new approach...

For high-consequence applications...

System Surety Engineering

- Developed at Sandia National Laboratories in the course of its work in high-consequence (nuclear weapon) engineering
- Motivated by the realization that standard engineering practices did not provide the level of safety assurance necessary for its operations with the potential for catastrophic accidents.

Slide 7



Surety Engineering Process

Definition

Identify system boundaries → Identify high-consequences → Identify requirements → Develop surety concepts and conduct tradeoffs

Development Engineering

Develop surety theme assertions → Conduct trade-off analysis → validate and verify assertions → Establish metrics

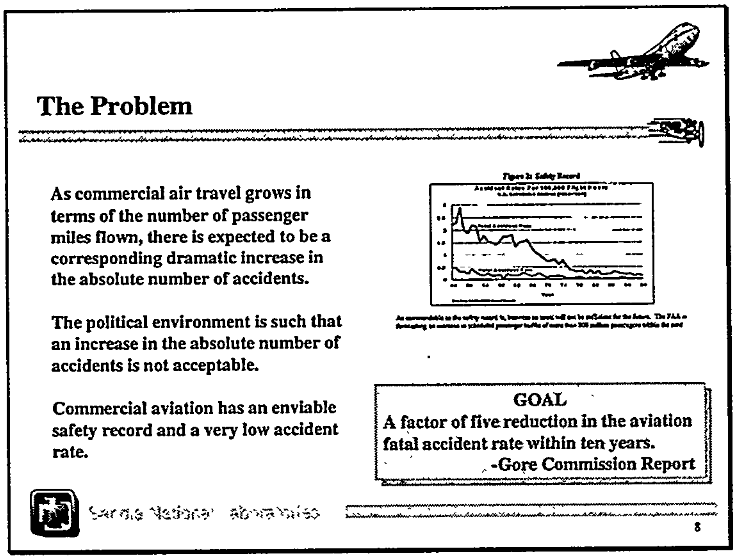
Production engineering and first production

Develop control and change processes → Defensible and robust system design

Sandia National Laboratories

7

Slide 8



The Problem

As commercial air travel grows in terms of the number of passenger miles flown, there is expected to be a corresponding dramatic increase in the absolute number of accidents.

The political environment is such that an increase in the absolute number of accidents is not acceptable.

Commercial aviation has an enviable safety record and a very low accident rate.

Figure 2: Safety Record

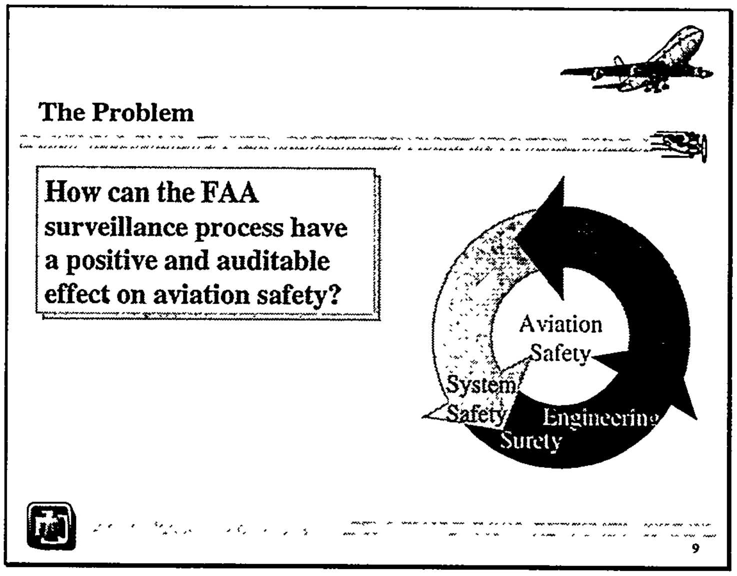
As commendable as the safety record is, however, [illegible] will not be sufficient for the future. The FAA is forecasting an increase in scheduled passenger traffic of more than 300 million passengers within the next

GOAL
A factor of five reduction in the aviation fatal accident rate within ten years.
-Gore Commission Report

Sandia National Laboratories

8

Slide 9



The Problem

How can the FAA surveillance process have a positive and auditable effect on aviation safety?

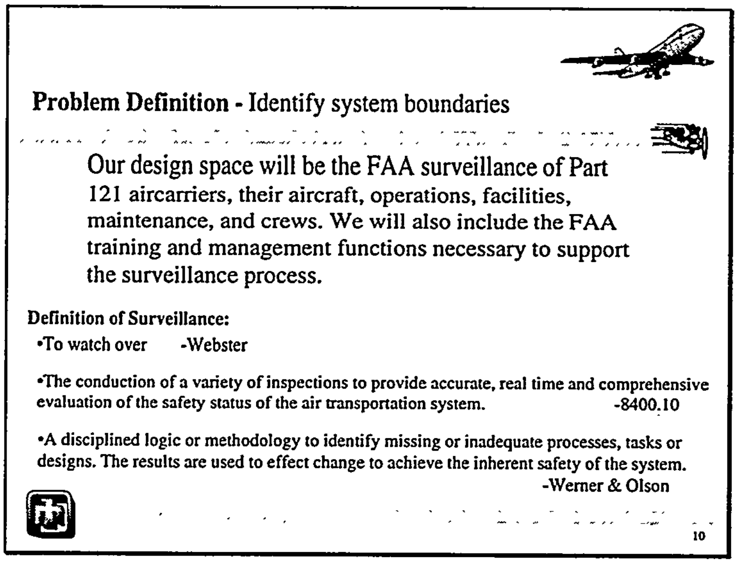
Aviation Safety

System Safety

Engineering Surety

9

Slide 10



Problem Definition - Identify system boundaries

Our design space will be the FAA surveillance of Part 121 aircarriers, their aircraft, operations, facilities, maintenance, and crews. We will also include the FAA training and management functions necessary to support the surveillance process.

Definition of Surveillance:

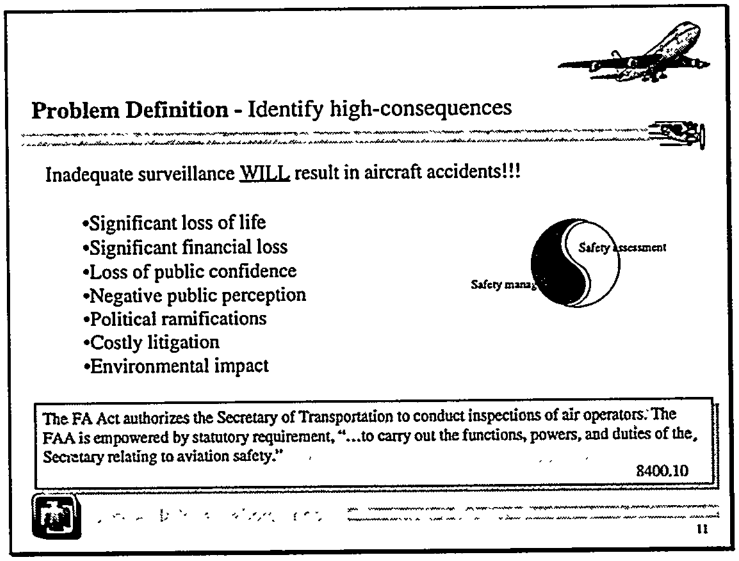
•To watch over -Webster

•The conduction of a variety of inspections to provide accurate, real time and comprehensive evaluation of the safety status of the air transportation system. -8400.10

•A disciplined logic or methodology to identify missing or inadequate processes, tasks or designs. The results are used to effect change to achieve the inherent safety of the system. -Werner & Olson

10

Slide 11



Problem Definition - Identify high-consequences

Inadequate surveillance WILL result in aircraft accidents!!!

- •Significant loss of life
- •Significant financial loss
- •Loss of public confidence
- •Negative public perception
- •Political ramifications
- •Costly litigation
- •Environmental impact

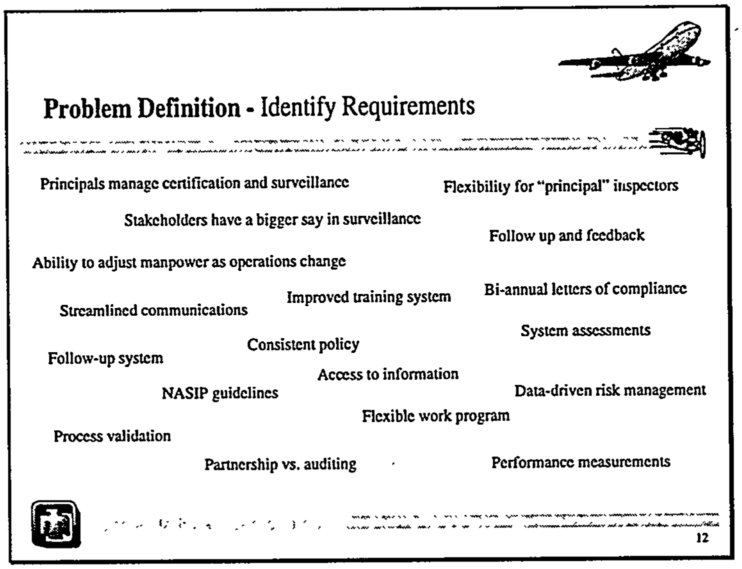
Safety assessment
Safety manag

The FA Act authorizes the Secretary of Transportation to conduct inspections of air operators. The FAA is empowered by statutory requirement, "...to carry out the functions, powers, and duties of the, Secretary relating to aviation safety."

8400.10

11

Slide 12



Problem Definition - Identify Requirements

Principals manage certification and surveillance

Flexibility for "principal" inspectors

Stakeholders have a bigger say in surveillance

Follow up and feedback

Ability to adjust manpower as operations change

Improved training system

Bi-annual letters of compliance

Streamlined communications

System assessments

Consistent policy

Follow-up system

Access to information

NASIP guidelines

Data-driven risk management

Flexible work program

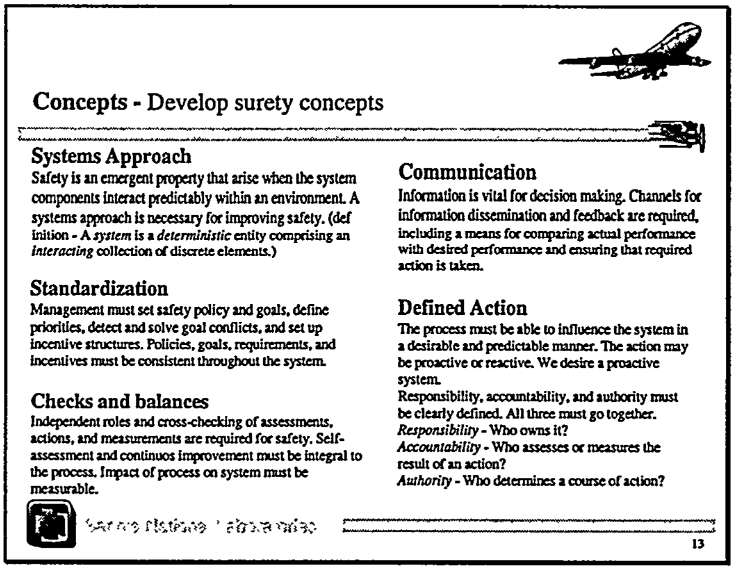
Process validation

Partnership vs. auditing

Performance measurements

12

Slide 13



Concepts - Develop surety concepts

Systems Approach

Safety is an emergent property that arise when the system components interact predictably within an environment. A systems approach is necessary for improving safety. (definition - A *system* is a *deterministic* entity comprising an *interacting* collection of discrete elements.)

Standardization

Management must set safety policy and goals, define priorities, detect and solve goal conflicts, and set up incentive structures. Policies, goals, requirements, and incentives must be consistent throughout the system.

Checks and balances

Independent roles and cross-checking of assessments, actions, and measurements are required for safety. Self-assessment and continuos improvement must be integral to the process. Impact of process on system must be measurable.

Communication

Information is vital for decision making. Channels for information dissemination and feedback are required, including a means for comparing actual performance with desired performance and ensuring that required action is taken.

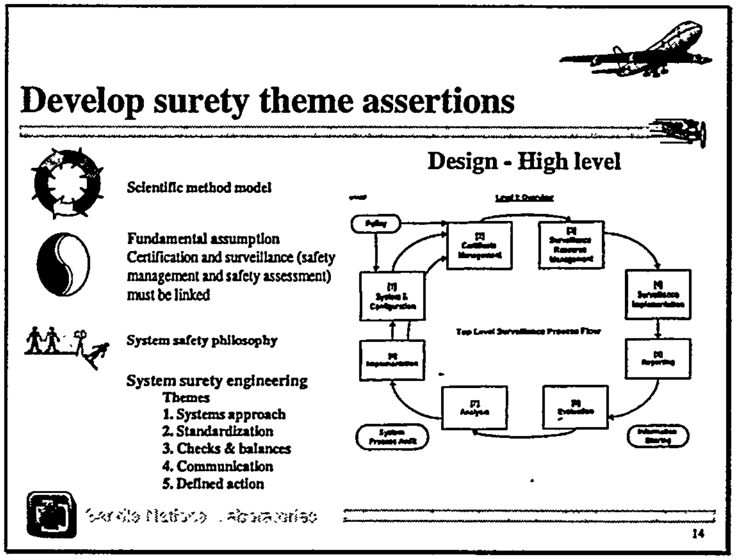
Defined Action

The process must be able to influence the system in a desirable and predictable manner. The action may be proactive or reactive. We desire a proactive system.
Responsibility, accountability, and authority must be clearly defined. All three must go together.
Responsibility - Who owns it?
Accountability - Who assesses or measures the result of an action?
Authority - Who determines a course of action?

Sandia National Laboratories

13

Slide 14



Develop surety theme assertions

Scientific method model

Fundamental assumption
Certification and surveillance (safety management and safety assessment) must be linked

System safety philosophy

System surety engineering
Themes
1. Systems approach
2. Standardization
3. Checks & balances
4. Communication
5. Defined action

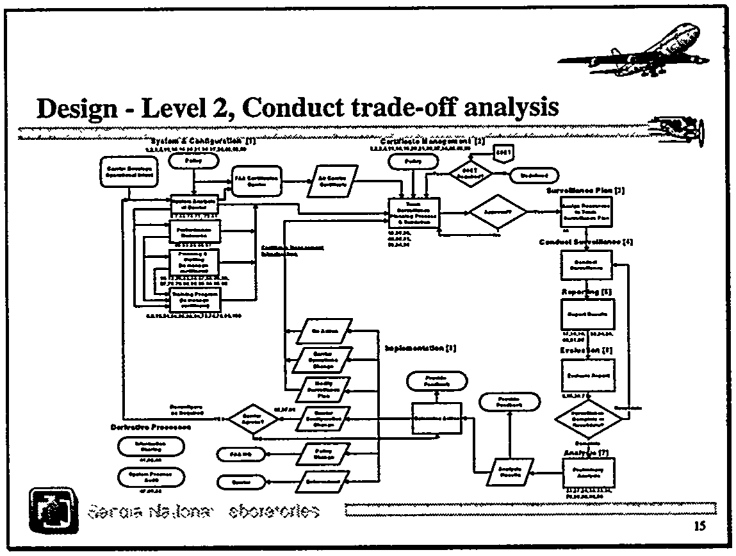
Design - High level

Level 2 Overview
Policy
[2] Certificate Management
[3] Surveillance Resource Management
[1] System & Configuration
[4] Surveillance Implementation
Top Level Surveillance Process Flow
[8] Implementation
[5] Reporting
[7] Analysis
[6] Evaluation
System Process Audit
Information Sharing

Sandia National Laboratories

14

Slide 15

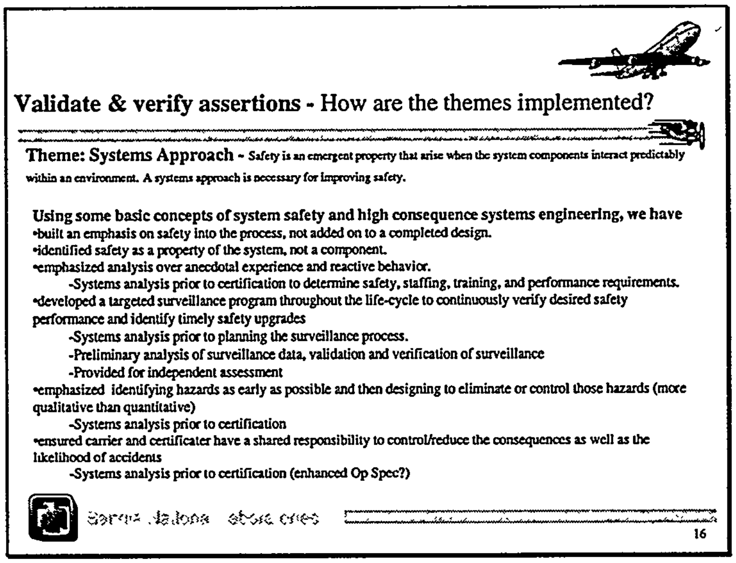


Design - Level 2, Conduct trade-off analysis

Sandia National Laboratories

15

Slide 16



Validate & verify assertions - How are the themes implemented?

Theme: Systems Approach - Safety is an emergent property that arise when the system components interact predictably within an environment. A systems approach is necessary for improving safety.

Using some basic concepts of system safety and high consequence systems engineering, we have

•built an emphasis on safety into the process, not added on to a completed design.

•identified safety as a property of the system, not a component.

•emphasized analysis over anecdotal experience and reactive behavior.

-Systems analysis prior to certification to determine safety, staffing, training, and performance requirements.

•developed a targeted surveillance program throughout the life-cycle to continuously verify desired safety performance and identify timely safety upgrades

-Systems analysis prior to planning the surveillance process.

-Preliminary analysis of surveillance data, validation and verification of surveillance

-Provided for independent assessment

•emphasized identifying hazards as early as possible and then designing to eliminate or control those hazards (more qualitative than quantitative)

-Systems analysis prior to certification

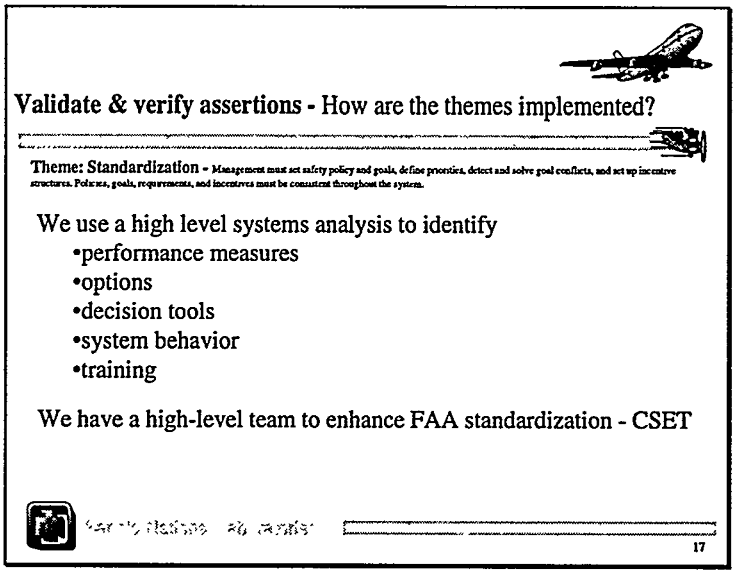
•ensured carrier and certificater have a shared responsibility to control/reduce the consequences as well as the likelihood of accidents

-Systems analysis prior to certification (enhanced Op Spec?)

Sandia National Laboratories

16

Slide 17



Validate & verify assertions - How are the themes implemented?

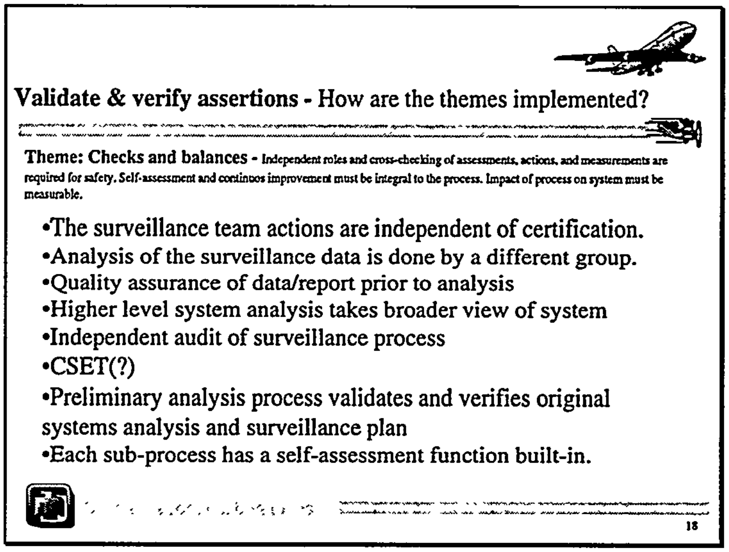
Theme: Standardization - Management must set safety policy and goals, define priorities, detect and solve goal conflicts, and set up incentive structures. Policies, goals, requirements, and incentives must be consistent throughout the system.

We use a high level systems analysis to identify
- performance measures
- options
- decision tools
- system behavior
- training

We have a high-level team to enhance FAA standardization - CSET

17

Slide 18



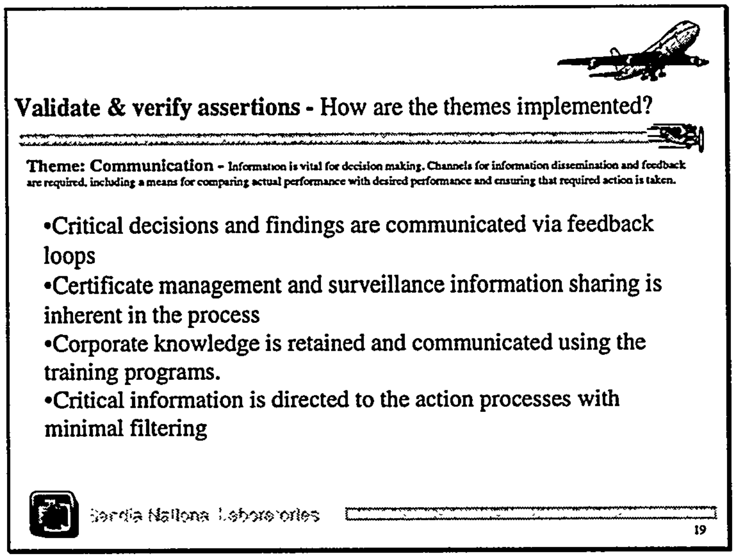
Validate & verify assertions - How are the themes implemented?

Theme: Checks and balances - Independent roles and cross-checking of assessments, actions, and measurements are required for safety. Self-assessment and continoos improvement must be integral to the process. Impact of process on system must be measurable.

- The surveillance team actions are independent of certification.
- Analysis of the surveillance data is done by a different group.
- Quality assurance of data/report prior to analysis
- Higher level system analysis takes broader view of system
- Independent audit of surveillance process
- CSET(?)
- Preliminary analysis process validates and verifies original systems analysis and surveillance plan
- Each sub-process has a self-assessment function built-in.

18

Slide 19



Validate & verify assertions - How are the themes implemented?

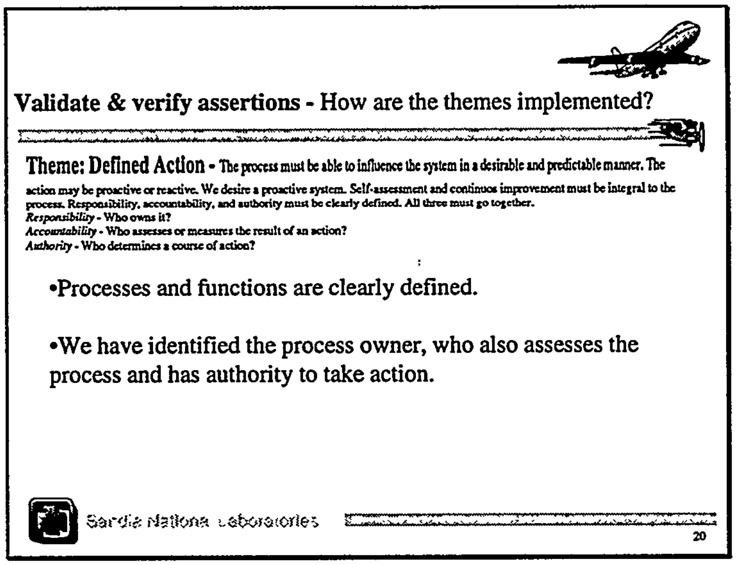
Theme: Communication - Information is vital for decision making. Channels for information dissemination and feedback are required, including a means for comparing actual performance with desired performance and ensuring that required action is taken.

- •Critical decisions and findings are communicated via feedback loops
- •Certificate management and surveillance information sharing is inherent in the process
- •Corporate knowledge is retained and communicated using the training programs.
- •Critical information is directed to the action processes with minimal filtering

Sandia National Laboratories

19

Slide 20



Validate & verify assertions - How are the themes implemented?

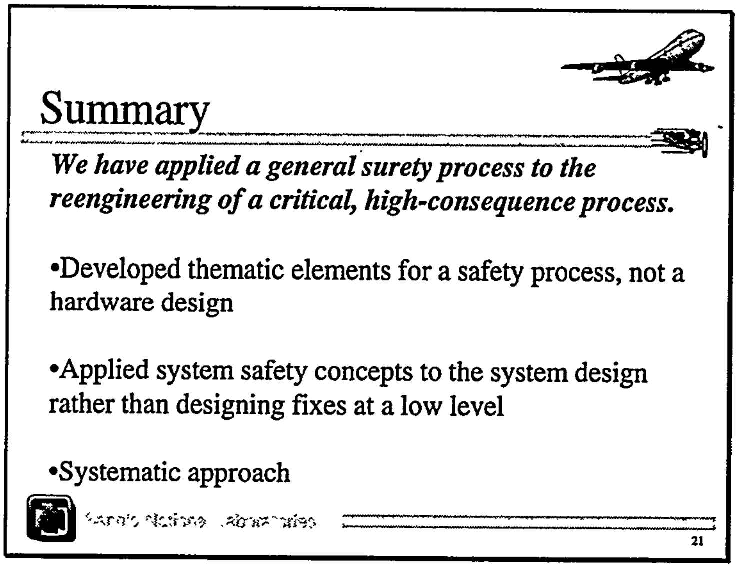
Theme: Defined Action - The process must be able to influence the system in a desirable and predictable manner. The action may be proactive or reactive. We desire a proactive system. Self-assessment and continuos improvement must be integral to the process. Responsibility, accountability, and authority must be clearly defined. All three must go together.
Responsibility - Who owns it?
Accountability - Who assesses or measures the result of an action?
Authority - Who determines a course of action?

- •Processes and functions are clearly defined.
- •We have identified the process owner, who also assesses the process and has authority to take action.

Sandia National Laboratories

20

Slide 21



Summary

We have applied a general surety process to the reengineering of a critical, high-consequence process.

•Developed thematic elements for a safety process, not a hardware design

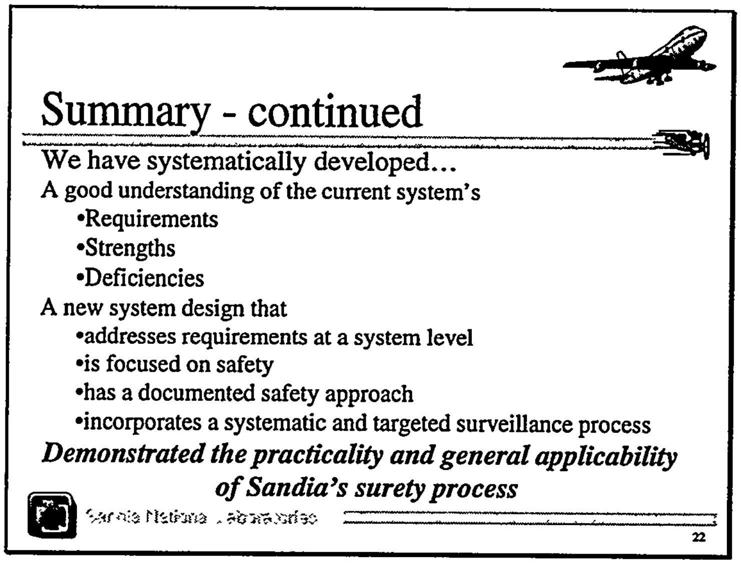
•Applied system safety concepts to the system design rather than designing fixes at a low level

•Systematic approach

Sandia National Laboratories

21

Slide 22



Summary - continued

We have systematically developed...

A good understanding of the current system's
- •Requirements
- •Strengths
- •Deficiencies

A new system design that
- •addresses requirements at a system level
- •is focused on safety
- •has a documented safety approach
- •incorporates a systematic and targeted surveillance process

Demonstrated the practicality and general applicability of Sandia's surety process

Sandia National Laboratories

22

Intentionally left blank

Public Perception in High Consequence Operations

Carol Silva
University of New Mexico
Albuquerque, New Mexico

Intentionally left blank

Incorporating Subjective Expertise in Risk Analysis

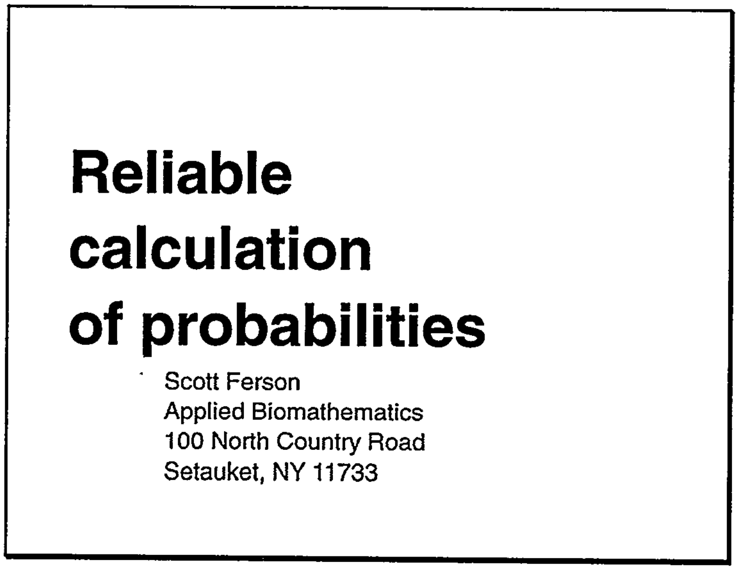
Tim Ross
University of New Mexico
Albuquerque, New Mexico

Intentionally left blank

Reliable Calculation of Probabilities

Scott Ferson
Applied Biomathematics
Setauket, New York

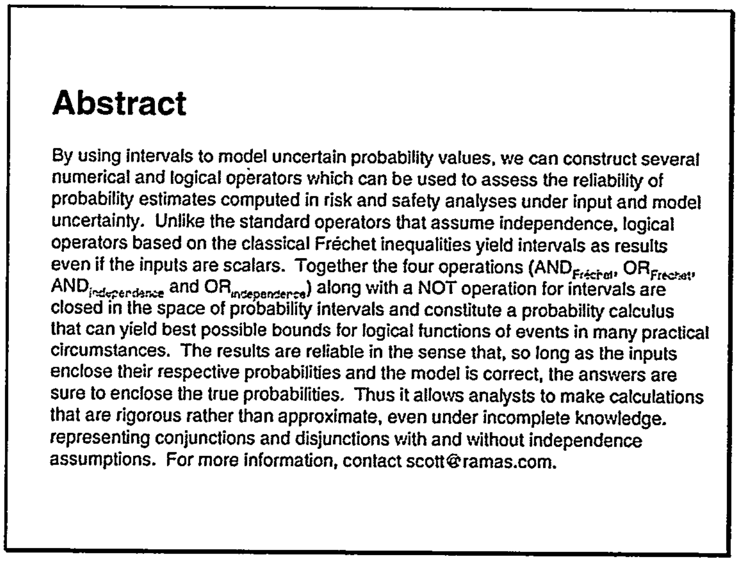
Slide 1



Reliable calculation of probabilities

Scott Ferson
Applied Biomathematics
100 North Country Road
Setauket, NY 11733

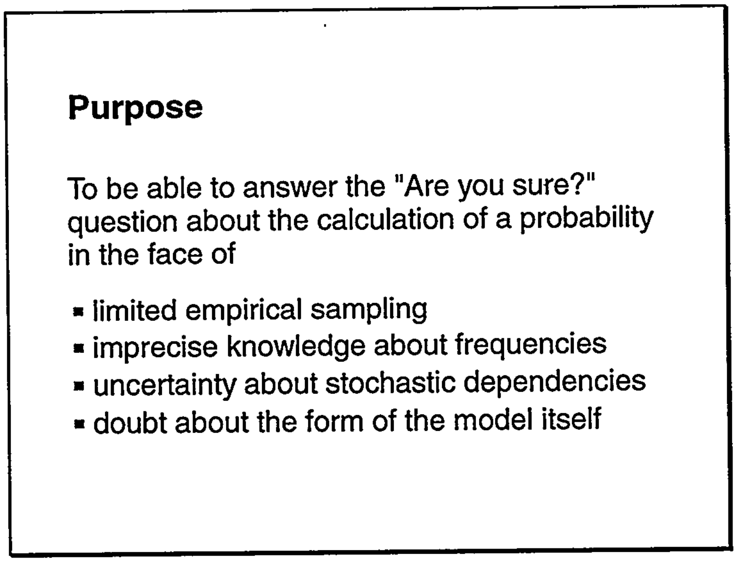
Slide 2



Abstract

By using intervals to model uncertain probability values, we can construct several numerical and logical operators which can be used to assess the reliability of probability estimates computed in risk and safety analyses under input and model uncertainty. Unlike the standard operators that assume independence, logical operators based on the classical Fréchet inequalities yield intervals as results even if the inputs are scalars. Together the four operations ($\text{AND}_{\text{Fréchet}}$, $\text{OR}_{\text{Frechet}}$, $\text{AND}_{\text{independence}}$ and $\text{OR}_{\text{independence}}$) along with a NOT operation for intervals are closed in the space of probability intervals and constitute a probability calculus that can yield best possible bounds for logical functions of events in many practical circumstances. The results are reliable in the sense that, so long as the inputs enclose their respective probabilities and the model is correct, the answers are sure to enclose the true probabilities. Thus it allows analysts to make calculations that are rigorous rather than approximate, even under incomplete knowledge. representing conjunctions and disjunctions with and without independence assumptions. For more information, contact scott@ramas.com.

Slide 3

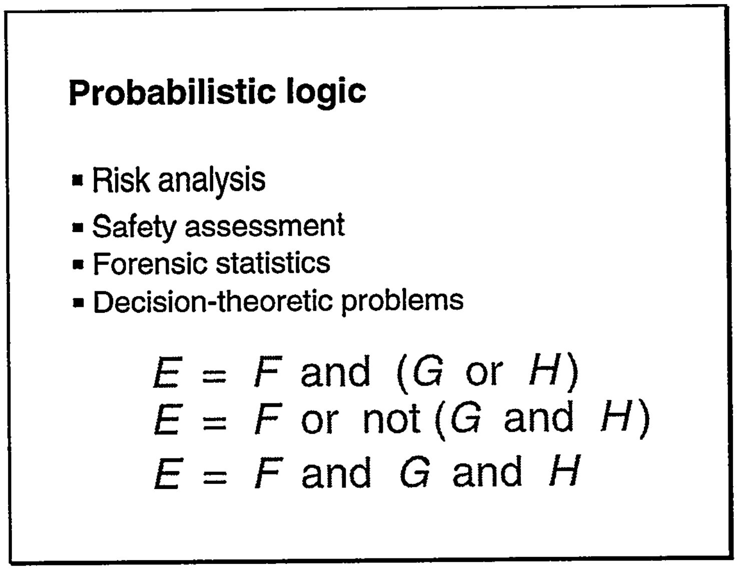


Purpose

To be able to answer the "Are you sure?" question about the calculation of a probability in the face of

- limited empirical sampling
- imprecise knowledge about frequencies
- uncertainty about stochastic dependencies
- doubt about the form of the model itself

Slide 4

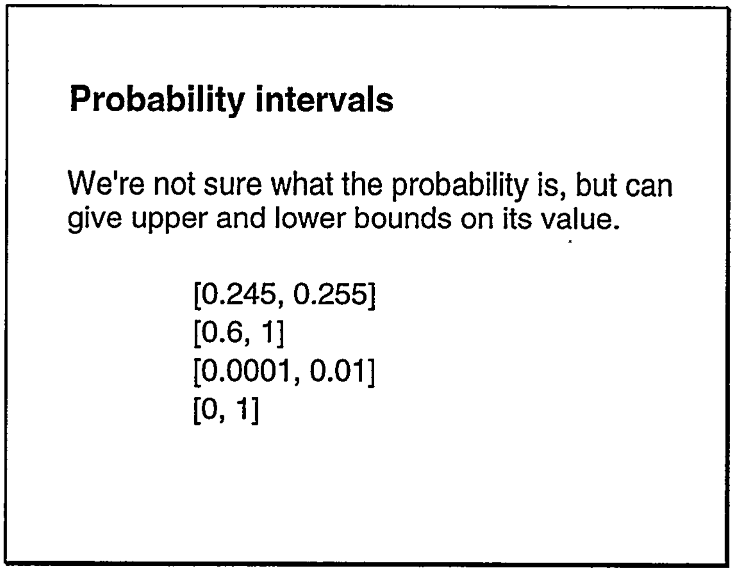


Probabilistic logic

- Risk analysis
- Safety assessment
- Forensic statistics
- Decision-theoretic problems

$$E = F \text{ and } (G \text{ or } H)$$
$$E = F \text{ or not } (G \text{ and } H)$$
$$E = F \text{ and } G \text{ and } H$$

Slide 5

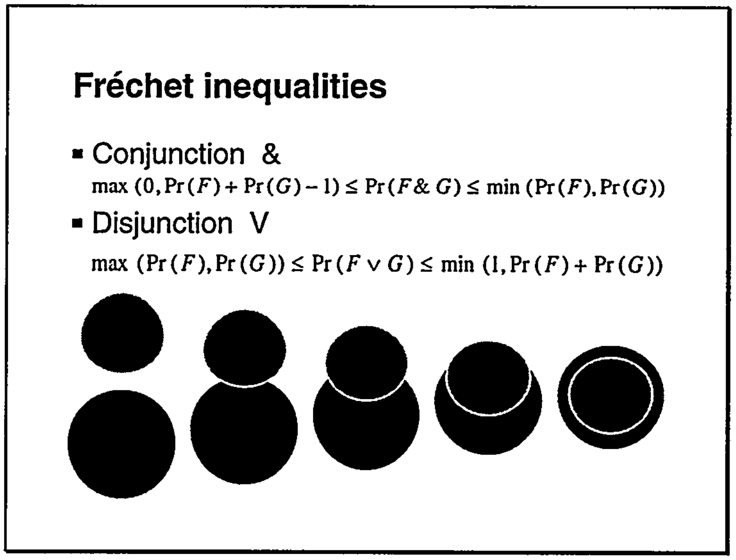


Probability intervals

We're not sure what the probability is, but can give upper and lower bounds on its value.

[0.245, 0.255]
[0.6, 1]
[0.0001, 0.01]
[0, 1]

Slide 6



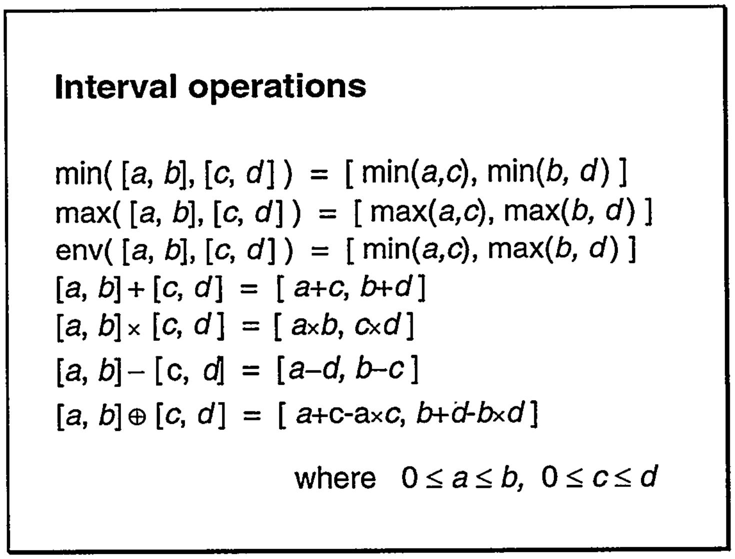
Fréchet inequalities

- Conjunction &

  $\max(0, \Pr(F) + \Pr(G) - 1) \le \Pr(F \& G) \le \min(\Pr(F), \Pr(G))$
- Disjunction V

  $\max(\Pr(F), \Pr(G)) \le \Pr(F \vee G) \le \min(1, \Pr(F) + \Pr(G))$

Slide 7



Interval operations

$\min([a, b], [c, d]) = [\min(a,c), \min(b, d)]$

$\max([a, b], [c, d]) = [\max(a,c), \max(b, d)]$

$\text{env}([a, b], [c, d]) = [\min(a,c), \max(b, d)]$

$[a, b] + [c, d] = [a+c, b+d]$

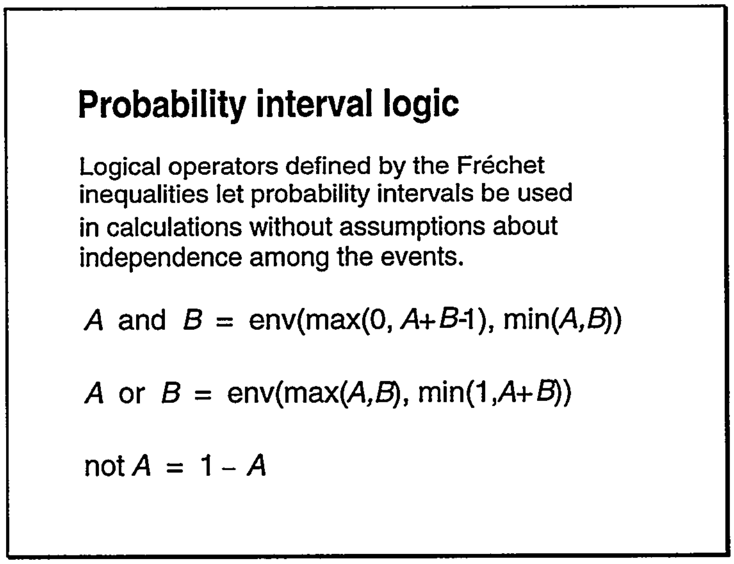
$[a, b] \times [c, d] = [a \times b, c \times d]$

$[a, b] - [\text{c}, d] = [a-d, b-c]$

$[a, b] \oplus [c, d] = [a+\text{c}-\text{a}\times c, b+d-b\times d]$

where $0 \le a \le b, \ 0 \le c \le d$

Slide 8



Probability interval logic

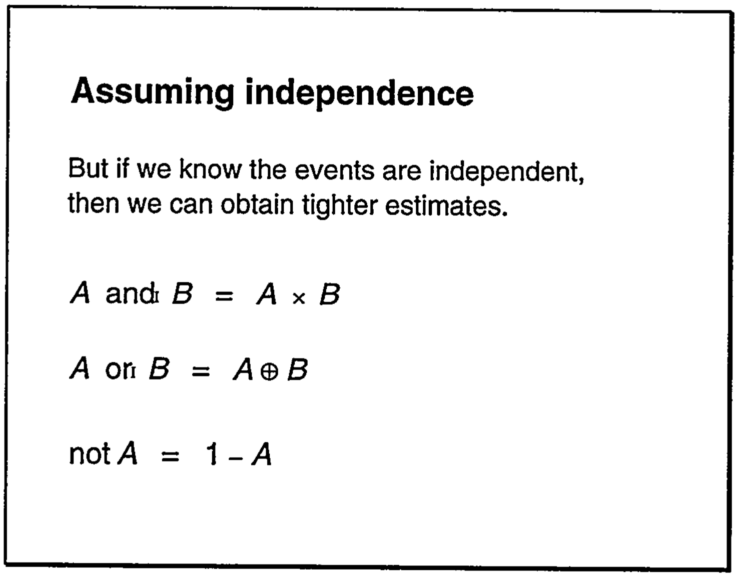
Logical operators defined by the Fréchet inequalities let probability intervals be used in calculations without assumptions about independence among the events.

A and B = env(max(0, $A+B-1$), min(A,B))

A or B = env(max(A,B), min(1,$A+B$))

not A = $1 - A$

Slide 9



Assuming independence

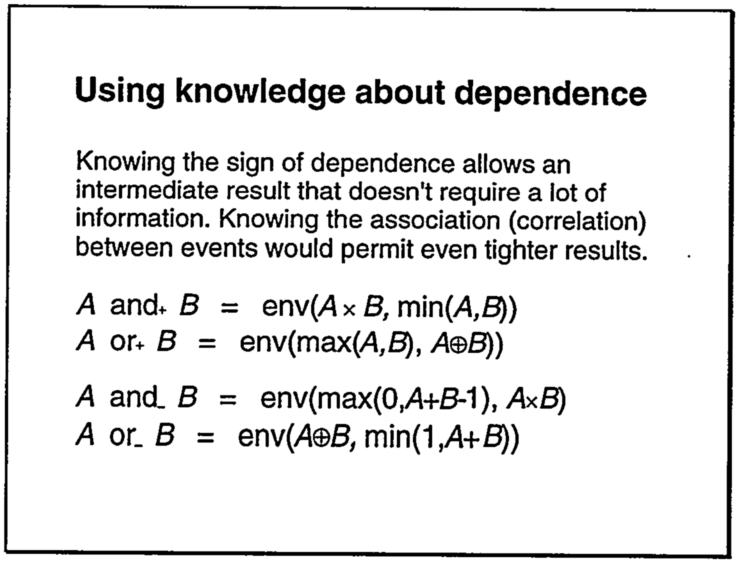
But if we know the events are independent, then we can obtain tighter estimates.

A and$_{\mathrm{I}}$ B = $A \times B$

A or$_{\mathrm{I}}$ B = $A \oplus B$

not A = $1 - A$

Slide 10



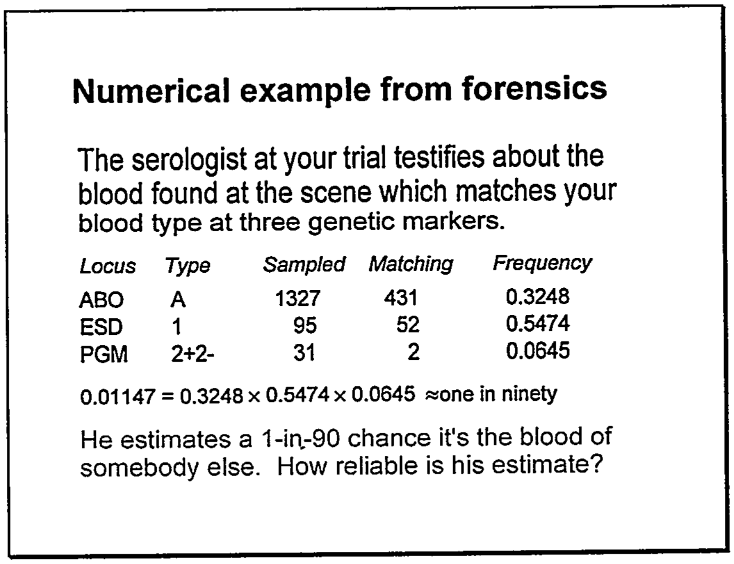
Using knowledge about dependence

Knowing the sign of dependence allows an intermediate result that doesn't require a lot of information. Knowing the association (correlation) between events would permit even tighter results.

A and$_{+}$ B = env($A \times B$, min(A,B))
A or$_{+}$ B = env(max(A,B), $A \oplus B$))

A and$_{-}$ B = env(max(0,A+B-1), $A \times B$)
A or$_{-}$ B = env($A \oplus B$, min(1,A+B))

Slide 11



Numerical example from forensics

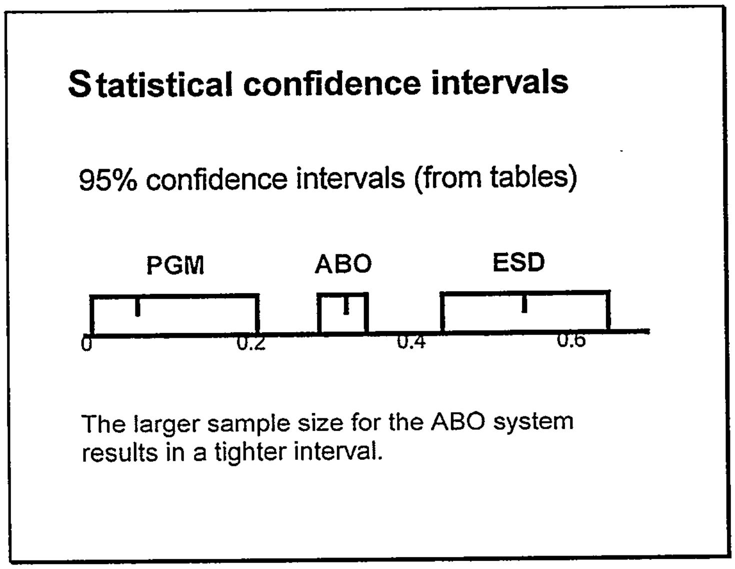
The serologist at your trial testifies about the blood found at the scene which matches your blood type at three genetic markers.

Locus	*Type*	*Sampled*	*Matching*	*Frequency*
ABO	A	1327	431	0.3248
ESD	1	95	52	0.5474
PGM	2+2-	31	2	0.0645

0.01147 = 0.3248 × 0.5474 × 0.0645 ≈one in ninety

He estimates a 1-in-90 chance it's the blood of somebody else. How reliable is his estimate?

Slide 12

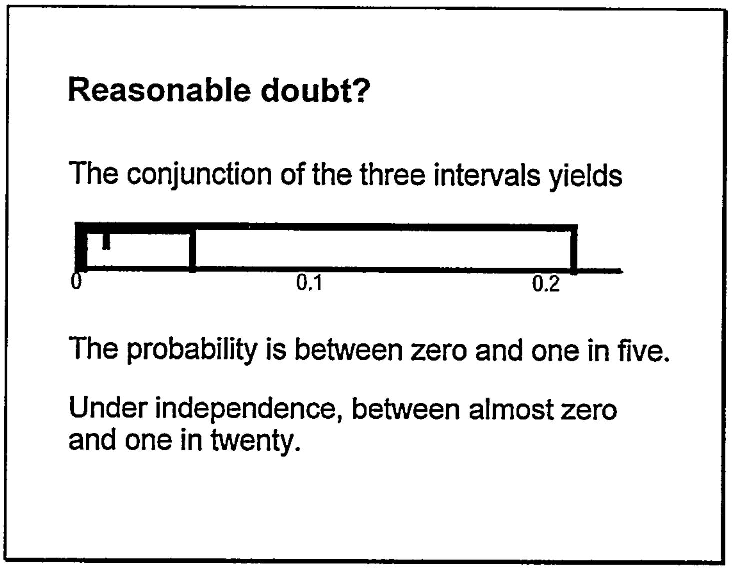


Statistical confidence intervals

95% confidence intervals (from tables)

The larger sample size for the ABO system results in a tighter interval.

Slide 13



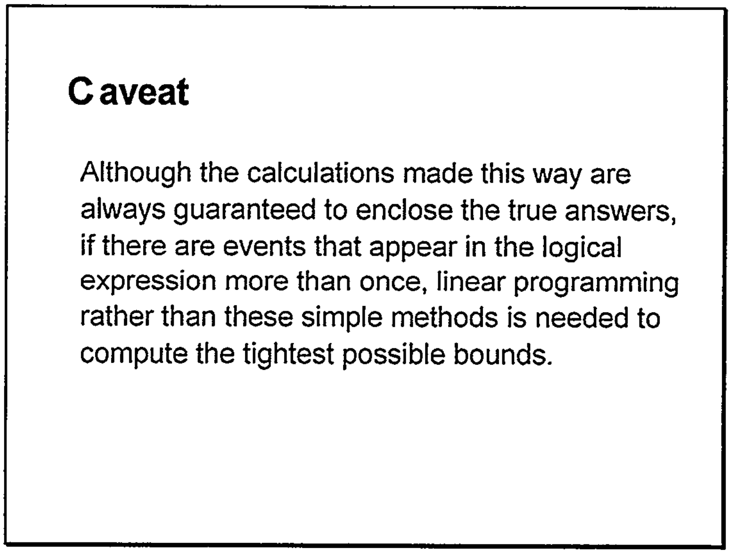
Reasonable doubt?

The conjunction of the three intervals yields

The probability is between zero and one in five.

Under independence, between almost zero and one in twenty.

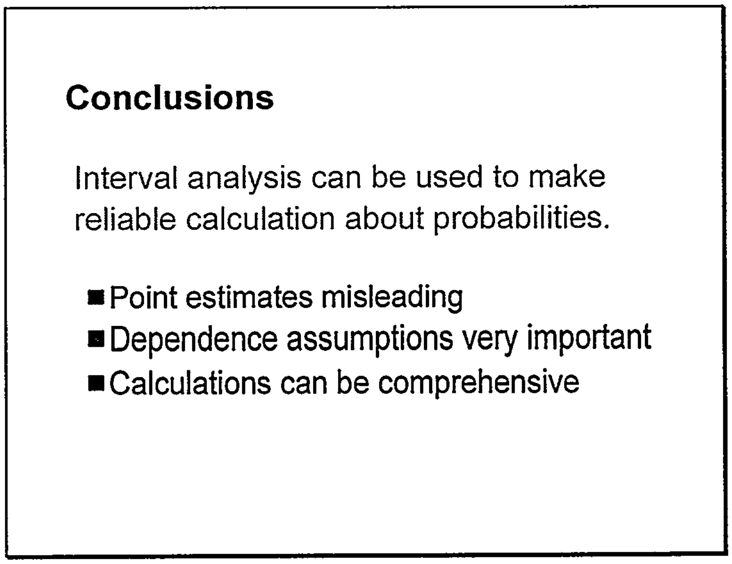
Slide 14



C aveat

Although the calculations made this way are always guaranteed to enclose the true answers, if there are events that appear in the logical expression more than once, linear programming rather than these simple methods is needed to compute the tightest possible bounds.

Slide 15

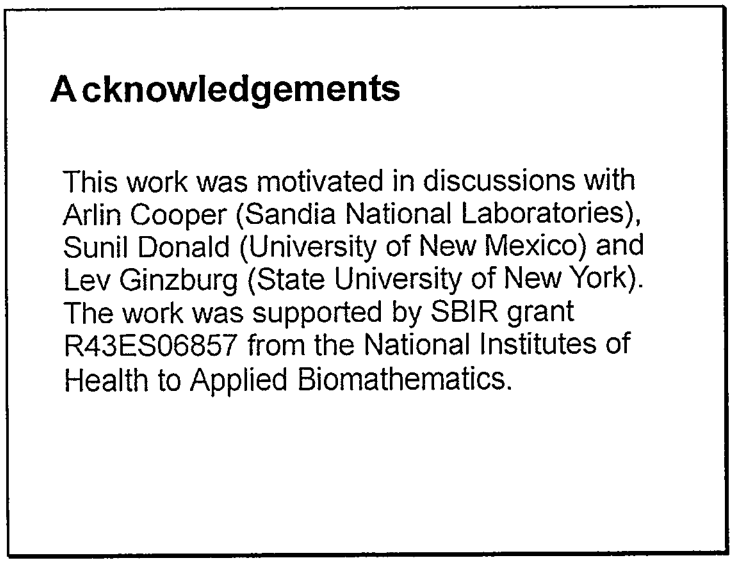


Conclusions

Interval analysis can be used to make reliable calculation about probabilities.

- Point estimates misleading
- Dependence assumptions very important
- Calculations can be comprehensive

Slide 16



Acknowledgements

This work was motivated in discussions with Arlin Cooper (Sandia National Laboratories), Sunil Donald (University of New Mexico) and Lev Ginzburg (State University of New York). The work was supported by SBIR grant R43ES06857 from the National Institutes of Health to Applied Biomathematics.

The Pentagon-S Process: A Systematic Approach for Achieving High Confidence in High Consequence Products

Perry E. D'Antonio
John M. Covan
Mark E. Ekman
Sandia National Laboratories*
Albuquerque, New Mexico

Abstract

Sandia National Laboratories has developed a systematic approach for achieving high confidence in major products requiring high reliability for use in high-consequence applications. A high-consequence application is one in which product failure could result in significant loss of life, damage to major systems or to the environment, financial loss, or political repercussions. The application of this process has proven to be of significant benefit in the early identification, verification, and correction of potential product design and manufacturing process failure modes. Early identification and correction of these failure modes and the corresponding controls placed on safety-critical features ensures product adherence to safety-critical design requirements and enhances product quality, reliability, and the cost effectiveness of delivered products. Safety-critical features include design features such as materials and dimensions, as well as manufacturing features such as assembly processes, inspections, and testing.

Keywords

High consequence, safety, surety, Pentagon-S, manufacturing controls, production controls, change control, product documentation, system safety, best practices, /S/

Pentagon-S Overview

The Pentagon-S process is a multi-organizational team approach that includes the designer, customer, supplier and safety engineer working in concert to define safety-critical features and determine how those features will perform in accident and operational environments the product may encounter. The purposes of the process are to

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

identify safety-critical design features of a product, use a graded approach to control these features during production, implement a system of change control, and provide an auditable, pedigreed trail of documentation from requirements to final product. Systems-analysis tools (e.g., fault tree, FMEA) are used to determine safety critical features and their failure modes. Pentagon-S helps the customer weigh safety requirements against other system requirements and understand the consequences of not implementing certain manufacturing controls. The process, with its supporting information archival and retrieval system, received two *Best Practices* awards from the Navy Best Manufacturing Practices Office.

Introduction

Pentagon-S, or /S/, implementation is a systematic process that analyzes product design features in the context of their environments and operations to identify safety-critical features. Safety-critical features include materials, dimensions, processes, testing, and so on. On production control drawings, /S/ markings identify safety-critical features that if changed or deviated from could degrade the safety function of piece parts or subsequent assemblies. Changes to /S/ features require review and management approval by both the design and safety organizations.

Safety critical features must be identified and controlled in high-consequence applications. Pentagon S ensures that safety-critical features will not be changed without recognizing the effect such changes could have on the safety of the component or system as a whole.

Properly identifying, documenting, and controlling safety-critical features ensures that components and systems are built as designed and respond in a predictably safe manner. Documentation provides an auditable, traceable path between safety requirements and the product and provides a record for future designers and producers.

Significant improvements in production yield have also been demonstrated with /S/ because of the enhanced manufacturing screens and defect controls the process provides.

Background

The Pentagon-S process was created during the development of the modern US nuclear weapon program. Pentagon-S was created to augment traditional quality controls that were in place at the manufacturing site. At that time, no controls specific to safety-critical products or processes were in place and it was judged to be an inappropriate "weak link" in the product life-cycle of a high-consequence system. As we shall show, /S/ increased both the authority level and broadened the review body for change control, as well as strengthened Sandia National Laboratories' system safety methodology for assuring nuclear weapon detonation safety.

The Need for Control

Sandia's system safety engineering methodology–briefly described below– promotes high confidence in the product's safety performance only if an equally robust process manufactures it. Production must be controlled appropriately to ensure safety-critical features conform to their design requirements and are properly integrated into the system. Only then will the system meet its design requirements for high levels of safety in both operational and accident conditions.

The Scope of Control and Documentation

In general, the scope of control and documentation cuts across the entire safety process–from requirements development to design to manufacturing to operations to system shutdown and disposition. The most intense effort, however, occurs during the design phase after a *safety theme* has been developed. The safety theme describes the philosophy and implementation plan the designer will use to engineer a safe product and meet safety requirements. The safety theme describes the ideal safety performance of the system when exposed to normal operational and accident conditions. However, in practice, there is a tendency for safety performance to decrease with the realities of engineering tradeoffs and manufacturing difficulties. As Figure 1 shows, the role of Pentagon-S is to maintain safety performance at a high and acceptable level. It maintains performance by *identifying safety-critical features of components that are most critical to safety and then controlling their manufacture and documentation.*

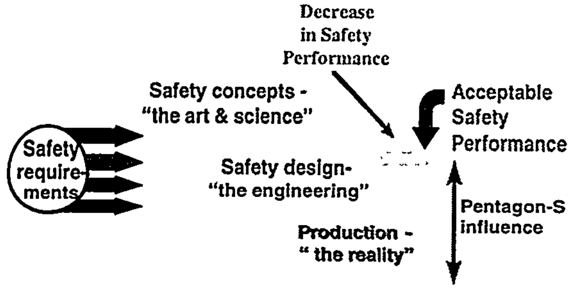

Decrease in Safety Performance
Safety concepts - "the art & science"
Acceptable Safety Performance
Safety requirements
Safety design- "the engineering"
Pentagon-S influence
Production - " the reality"

Figure 1. Pentagon-S maintains the designed-in safety performance.

How /S/ Fits into Sandia's System Safety Engineering Methodology

Modern nuclear weapon detonation safety is the result of decades of analysis, testing, and experience that has led to the development of a design methodology for keeping the weapon *predictably* safe under a variety of stresses, both operational (expected) and accident-based (unexpected). The methodology relies on mutually supportive safety design principles that are integrated through the proper implementation of fundamental physical principles known as *first-principles.* This integration is provided by a *safety* *theme* and its a-priori development avoids "Rube Goldberg" inventions that hinder the achievement of acceptable system safety.

The safety theme is implemented by partitioning safety requirements among multiple safety subsystems whose elements are essential to maintaining the safe state of the entire system. These elements are referred to as "safety critical" because their failure, either singly (first order failure) or in combination (lower order failure), will result in system failure and the realization of (negative) high consequences. Safety critical elements utilize engineered features that are identifiable, analyzable, and controllable. The goal is to minimize the number of system components that are safety-critical in accident environments. Because the safety assurance then hinges on a relatively small subset of overall system design, limited design and verification resources can be better focused to improve confidence that predictable safety will result.

The /S/ Process

The essential elements of the Pentagon-S process are: identify and rank safety critical elements, controls, analize control measures, document, and implement change control.

Identify and Rank Safety Critical Elements

Fault trees are created having basic nodes (Basic Events) identifying possible failures of safety critical elements. Each failure in the fault tree can be identified either as "first order" or "lower order." A first order failure can singly cause a component, subsystem, or system not to perform its intended function, thus reducing or eliminating safety protection from that element. A lower order failure must occur in combination with one or more separate failures to cause a component, subsystem or system not to perform its intended function. This difference is significant because separate controls are implemented depending on the order of a fault.

Selection of Controls

Because first order safety critical elements are more significant, more stringent controls are employed, typically involving 100% verification; lower order faults require less stringent controls.

Analysis of Control Measures

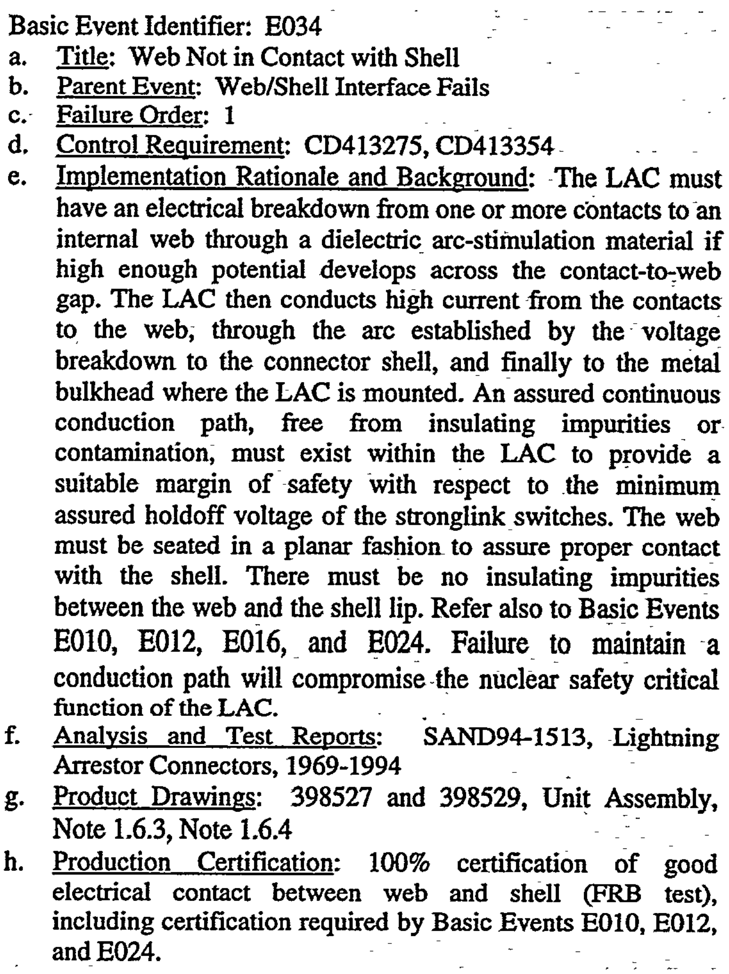
Control measures must be analyzed to ensure changes are not made without first knowing the effect those changes have on the safety functions. This evaluation must determine if any new hazards are introduced or if existing controls will be bypassed if the change is implemented. Management approval by the systems organization, the affected *component organization(s), and the safety organization is required before the change is implemented.*

Documentation

Safety critical features are documented using a formally defined template to capture the significant information about a safety critical feature. A safety critical feature can be traced by using the unique basic event identifier from the fault tree and recording this same identifier on all product-related documentation. Top level system or subsystem safety requirements are referenced in the safety documentation to tie safety requirements to the final product.

Figure 2, an example of this documentation, illustrates essential features of the Pentagon-S process. In order of their appearance in the figure, the entries are:

a. *Basic Event Identifier-* References the unique fault tree event affecting the specific safety critical feature.



Basic Event Identifier: E034

a. Title: Web Not in Contact with Shell

b. Parent Event: Web/Shell Interface Fails

c. Failure Order: 1

d. Control Requirement: CD413275, CD413354

e. Implementation Rationale and Background: The LAC must have an electrical breakdown from one or more contacts to an internal web through a dielectric arc-stimulation material if high enough potential develops across the contact-to-web gap. The LAC then conducts high current from the contacts to the web, through the arc established by the voltage breakdown to the connector shell, and finally to the metal bulkhead where the LAC is mounted. An assured continuous conduction path, free from insulating impurities or contamination, must exist within the LAC to provide a suitable margin of safety with respect to the minimum assured holdoff voltage of the stronglink switches. The web must be seated in a planar fashion to assure proper contact with the shell. There must be no insulating impurities between the web and the shell lip. Refer also to Basic Events E010, E012, E016, and E024. Failure to maintain a conduction path will compromise the nuclear safety critical function of the LAC.

f. Analysis and Test Reports: SAND94-1513, Lightning Arrestor Connectors, 1969-1994

g. Product Drawings: 398527 and 398529, Unit Assembly, Note 1.6.3, Note 1.6.4

h. Production Certification: 100% certification of good electrical contact between web and shell (FRB test), including certification required by Basic Events E010, E012, and E024.

Figure 2. Safety critical feature example documentation.

b. *Title-* Specific Basic Event title found on the fault tree.

c. *Parent Event-* Records with entry (a) the higher level event from which the safety critical basic event is derived (helps to locate the Basic Event in the fault tree).

d. *Failure Order-* As derived from fault tree analysis.

e. *Control Requirement-* Records specific safety requirement documents that are the source for control of this feature.

f. *Implementation Rationale And Background-* Provides a history and knowledge of why a feature is safety critical (especially useful when considering a change to the feature).

g. *Analysis And Test Reports-* Supporting documentation demonstrating safety performance or contains pertinent safety-related information.

h. *Product Drawings-* Location of where the Basic Event identifier appears on production drawings with /S/ notation.

i. *Product Certification-* Lists what verifications are done to ensure the product meets design requirements.

Change Control

Another formal documentation template was developed to document design changes to safety-critical features or to establish the disposition of product containing non-conforming safety critical features. This template includes the following information:

- *Background* - Describes issue or problem with /S/ item.
- *Change Request* - Describes the requested change to the /S/ feature.
- *Impact of Change* - Describes both the impact of not changing and implementing the change.
- *Management Approval* - Component, system, and safety managers sign.

Summary

Sandia National Laboratories has integrated a robust manufacturing process, known as Pentagon-S, into its system surety engineering methodology to deliver an end-to-end safety process for high-consequence systems. The overall process is depicted in Figure 3. This process will ensure safety-critical features are identified and appropriately controlled to ensure their safety performance throughout the system life cycle in both normal and accident conditions.

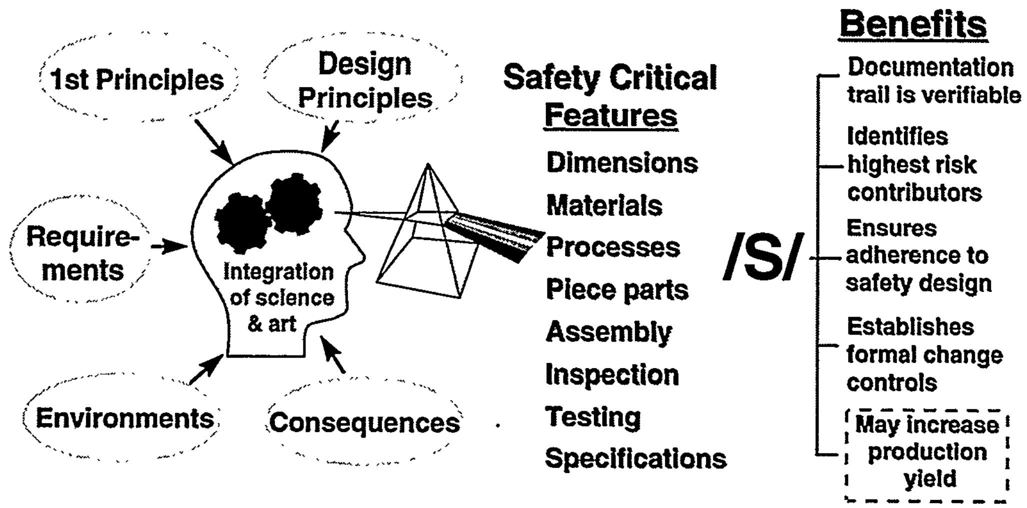

1st Principles
Design Principles
Requirements
Integration of science & art
Environments
Consequences
Safety Critical Features
Dimensions
Materials
Processes
Piece parts
Assembly
Inspection
Testing
Specifications
/S/
Benefits
Documentation trail is verifiable
Identifies highest risk contributors
Ensures adherence to safety design
Establishes formal change controls
May increase production yield

Figure 3. Pentagon-S as a part of the system safety process.

Biography

Mr. Perry E. D'Antonio is currently on a special one-year assignment at the Department of Energy's (DOE) Office of Weapons Surety. Prior to this assignment, he managed the System Surety Engineering department at Sandia National Laboratories (SNL). The department develops system safety engineering solutions for nuclear weapons and other industrial high-consequence operations. He holds a Masters Degree in Electrical Engineering from Stanford University. In seventeen years at SNL he has held staff and management positions in weapon systems engineering design and safety assessment, and managed a research program to improve safety technology. He is the SNL representative to the Lockheed-Martin Engineering Process Improvement Center's System Safety Subcouncil. He is a weapons safety expert in the DOE Accident Response Group. Mr. D'Antonio is currently serving as President of the System Safety Society.

Dr. John M. Covan is a Senior Member of the Technical Staff at Sandia National Laboratories. He holds a Ph.D. in Nuclear Physics from the University of Arizona and an ME in Industrial Engineering from Texas A&M University. He has held a number of positions cutting across surety engineering at Sandia Laboratories. In the use-control arena, he has evaluated related weapon subsystems and has developed new concepts involving use control. In the detonation safety arena he has modeled new safety concepts, done experiments on electromagnetic sensitivities to premature detonation, and proposed procedures for investing detonation safety directly into new systems. He has also been involved in efforts to transport detonation safety-based concepts beyond this arena to more general commercial applications. He is a member of the System Safety Society and is currently serving on its Standards Committee.

Dr. Mark E. Ekman is a Senior Member of the Technical Staff at Sandia National Laboratories. He holds a Ph.D. in Chemical Engineering from Iowa State University. He has led the incorporation of the Pentagon-S process for most of the nuclear weapon safety components in production at multiple DOE production agencies since 1992. He led a DOE multi-agency team to ensure consistency in process implementation throughout the Nuclear Weapons Complex (NWC) and is a co-author of the NWC Technical Business Practices defining the Pentagon-S process. Dr. Ekman is a member of the American Institute of Chemical Engineers and the American Chemical Society.

SAFETY ANALYSIS METHODOLOGY

Wednesday, July 30, 1997
1:30 p.m. – 5:00 p.m.

Intentionally left blank

Evaluation Tools Used by The Boeing Company for High Consequence Operational Safety

James J. Hairston
Boeing Defense and Space Group System Safety
Seattle, Washington

Abstract

The Boeing Company Safety Analyst uses three programs as tools for the analysis of High Consequence Operations Safety. These tools are Simulation and Analytic Fault Tree Evaluator (SAFTE), Fault Tree Analyzer Builder (FTAB), and the Fault Tree Analysis data file BUILDing program (FTABUILD). These tools are used to interactively build Fault Tree drawings that may represent several sequential system operating states. Data sets for numerical evaluation are then formulated from the data files for the drawings. Numerical evaluation provides values of probability, and assesses the relative importance of failure paths, and the importance and sensitivity of basic system part failures. The quantification process is for systems where the occurrence of the event modeled via the fault tree is considered as catastrophic.

Introduction

The Boeing Company Safety Analysis team evaluates High Consequence Operational Safety scenarios using the Boeing Simulation and Analytic Fault Tree Evaluator (SAFTE). This tool was developed during the Nuclear Certification of the B1-B Bomber, and was used for Nuclear Certification of the B-2 Bomber. Currently it is being used for Safety Analysis and Nuclear Certification of the Minuteman Missile System with its latest replacement guidance system.

The initial concepts were conceived during the development of the Nuclear Safety Analysis Computer Program (NSCAP). This program was developed for the former Air Force Weapons Laboratory, located at Kirtland Air Force Base, New Mexico, in the early eighties. The shortcomings of the NSCAP program became evident during its test and evaluation phase of development. Improvements were suggested, but budgetary considerations precluded any further development of the program. At that time neither NSCAP nor any similar Fault Tree Analysis program could analyze a system whose operating state changed during an operational mission. Normally evaluations were accomplished for the operational state that the analyst assumed posed the greatest risk to an assumed friendly nation's populations or resources. In some cases, the evaluation was for the operational state that posed the greatest apparent probability of occurrence of the undesirable event. These operating states were usually assumed without any real proof that they were the most safety critical high-risk operating states. There may have been other operating states of the system that posed a higher risk that were not evaluated because the analyst assumed that the exposure time was too short or the safeguards in use were adequate to consider the risk as sufficiently remote.

No known Fault Tree Analysis tool at the time SAFTE was in conceptual development computed the probability of the undesirable event where its occurrence is considered as catastrophic. All analysis tools computed the expected number of failures and/or unavailability. Most high-consequence undesirable events are indeed catastrophic, and should be evaluated as such. The inadvertent release of a weapon, the inadvertent launch of a missile, the collapse of a dam, the detonation of an explosive, and so on. cannot be repaired or renewed. Once such events occur there is no way to renew the failed system to its operating state prior to the undesired event. You can not reach up into the air, repair an inadvertently released missile, and place it back on the launching pad. Once it is launched, the undesirable event has occurred; there is no repair recourse available.

The SAFTE Program

The SAFTE program was developed as a logical extension of the older Boeing Aerospace Company SIMulation (BACSIM) program developed in the early sixties for Safety Analysis and Nuclear Certification of the Minuteman System. This new innovative program operates on an IBM PC or IBM compatible PC as a DOS program.

The SAFTE program is capable of evaluating a system that transitions through from one to 18 sequential operating states or phases of operation. These operating states may be evaluated as having occurred once or a number of times. For example, a system may transition from the first operating state through the third state; then cycle through the fourth operating state 17 times prior to transitioning to the fifth operating state. Operating states, or phases of operation as we refer to them, may actually be nested up to three levels deep.

Quantification is accomplished by the SAFTE program via an algorithm developed by Dr. Thomas J. Tosch. Dr. Tosch presented this algorithm to the American Statistical Association in 1989. His paper is included in the proceedings of this conference in the statistical computation section.

The simulation process used in the SAFTE program was based upon the BACSIM program and works accomplished by Drs. Phyllis M. Nagel and Roberto E. Altschul on power rules for phased fault tree analysis simulation systems. The SAFTE simulation process uses a similar power factor to increase the simulation efficiency. There are actually three power factor rules of operation employed in the SAFTE program. Power Rule "A" and "B" are used with quantification via the statistical process. Rule "A" emphasizes the derivation and ordering of failure paths. Rule "B" emphasizes the overall mission probability computations. However, each rule provides the same end results. Rule "C" increases the efficiency of failure path generation and does not provide correct statistical quantification results. The statistical quantification processes are still under development at this time. The program is normally run under Rule "C" to find failure paths that are then quantified via a Direct Failure Path Quantification module that was developed by Dr. Tosch. In addition to the simulation process, SAFTE has a direct evaluation tool to derive all first and second order failure paths. This module was included to ensure that all single points of failure were found regardless of the fact that there is a chance that a remote event or events may be overlooked. Thus, the direct evaluation module was developed.

The direct quantification process incorporates the catastrophic system algorithm developed by Dr. Tosch. In addition the percent contribution to the undesired event or the probability of occurrence of a specific failure path, is computed for each failure path. The failure paths are listed by basic event mnemonics and ranked by their probability of occurrence as illustrated in Figure 1. This listing is an aid to the analyst in identifying the failure paths most likely to have caused the undesired event. Additionally, a list of probabilities by phase and the total mission probability is provided as illustrated at the bottom of Figure 1.

System individual part failures are normally referenced by a mnemonic as mentioned above. Parts that contribute to the occurrence of the failure paths are evaluated for their percent contribution and ranked in a similar format as failure paths. This listing of parts is an aid to the analyst in identifying safety critical parts.

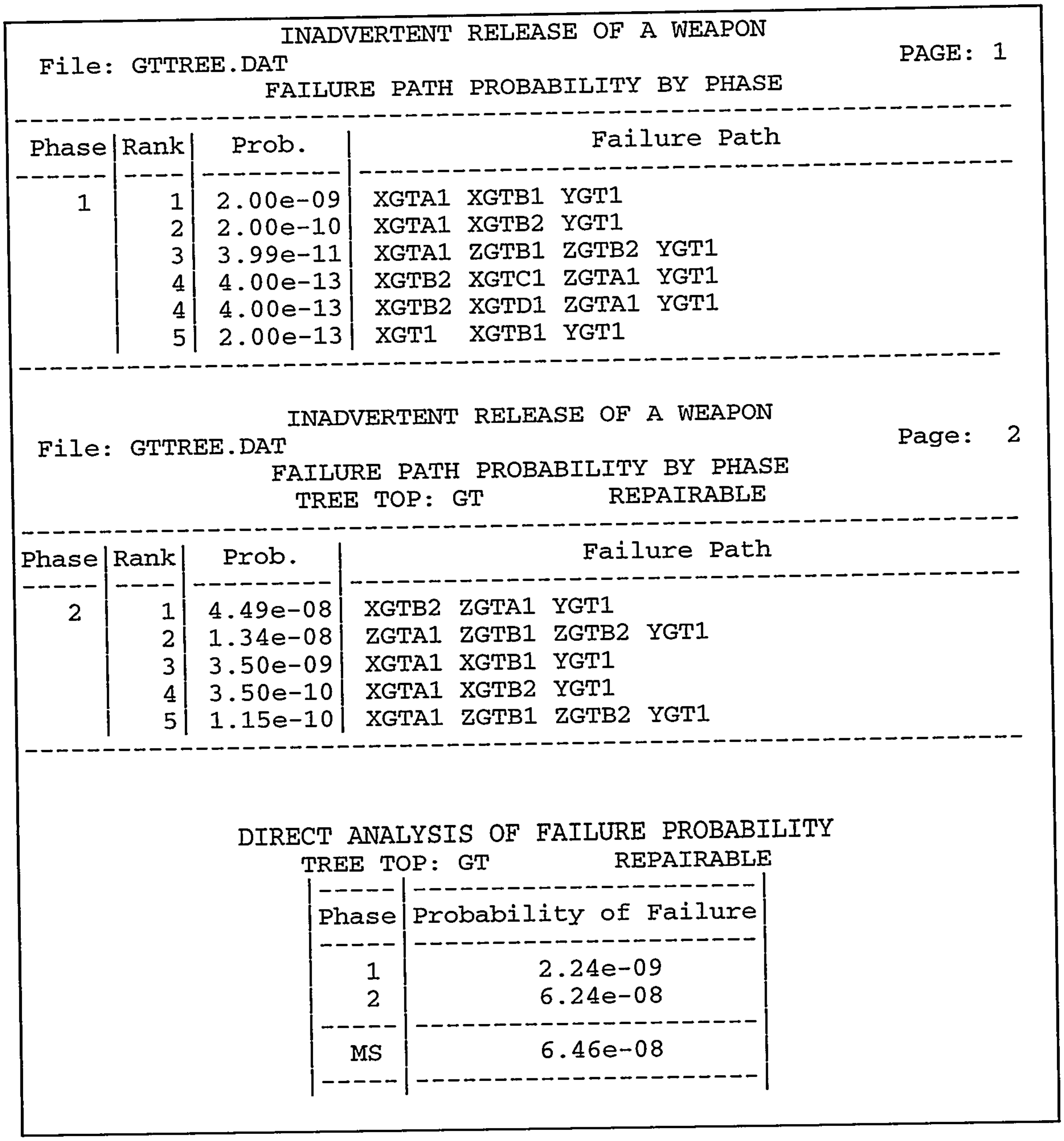
Individual parts are numerically evaluated for the sensitivity of the undesired event probability to a change in the expected failure rates of the parts. The parts are ranked by the absolute change in the probability of the undesired event given a change in the expected failure rate of a specific part. This ranking is presented in a similar format as failure paths shown. If the analyst desires, the actual partial derivative value may be displayed also. This value is the relative change in undesired event probability given a change in the failure rate of a specific part. Note that parts are not ranked by this value. These importance value rankings are provided by phase of operation and for the overall mission.

The input data set for the SAFTE program consists of the elements listed below

(1) A definition of the fault tree logic comprised of:

  (a) Logical AND gates
  (b) Logical OR gates
  (c) INHIBIT gates
  (d) Basic part failure modes (Circle)
  (e) Secondary part failures (Diamond)
  (f) Environmental conditions (Oval)
  (g) System state events (House)

(2) Phase duration times.
(3) The expected failure rate for basic events (part failures).



```
                    INADVERTENT RELEASE OF A WEAPON
 File: GTTREE.DAT                                          PAGE: 1
                   FAILURE PATH PROBABILITY BY PHASE
-----------------------------------------------------------------
 Phase|Rank|  Prob.    |               Failure Path
------|----|-----------|-----------------------------------------
   1  |   1| 2.00e-09| XGTA1 XGTB1 YGT1
      |   2| 2.00e-10| XGTA1 XGTB2 YGT1
      |   3| 3.99e-11| XGTA1 ZGTB1 ZGTB2 YGT1
      |   4| 4.00e-13| XGTB2 XGTC1 ZGTA1 YGT1
      |   4| 4.00e-13| XGTB2 XGTD1 ZGTA1 YGT1
      |   5| 2.00e-13| XGT1  XGTB1 YGT1
-----------------------------------------------------------------

                    INADVERTENT RELEASE OF A WEAPON
 File: GTTREE.DAT                                          Page:  2
                   FAILURE PATH PROBABILITY BY PHASE
                    TREE TOP: GT         REPAIRABLE
-----------------------------------------------------------------
Phase|Rank|  Prob.    |               Failure Path
-----|----|-----------|------------------------------------------
  2  |   1| 4.49e-08| XGTB2 ZGTA1 YGT1
     |   2| 1.34e-08| ZGTA1 ZGTB1 ZGTB2 YGT1
     |   3| 3.50e-09| XGTA1 XGTB1 YGT1
     |   4| 3.50e-10| XGTA1 XGTB2 YGT1
     |   5| 1.15e-10| XGTA1 ZGTB1 ZGTB2 YGT1
-----------------------------------------------------------------


               DIRECT ANALYSIS OF FAILURE PROBABILITY
                   TREE TOP: GT         REPAIRABLE
                  |-----|----------------------|
                  |Phase|Probability of Failure|
                  |-----|----------------------|
                  |  1  |       2.24e-09       |
                  |  2  |       6.24e-08       |
                  |-----|----------------------|
                  | MS  |       6.46e-08       |
                  |-----|----------------------|
```

Figure 1. Typical SAFTE Failure Path Output.

(4) The hazard duration times for basic events (parts).
(5) Multipliers used to adjust failure rates to an appropriate value per phase (K-Factor).
(6) Phase boundary conditions concerning repair:

(a) Repair continues across the boundary
(b) New repair mechanism occurs
(c) Repair at the boundary

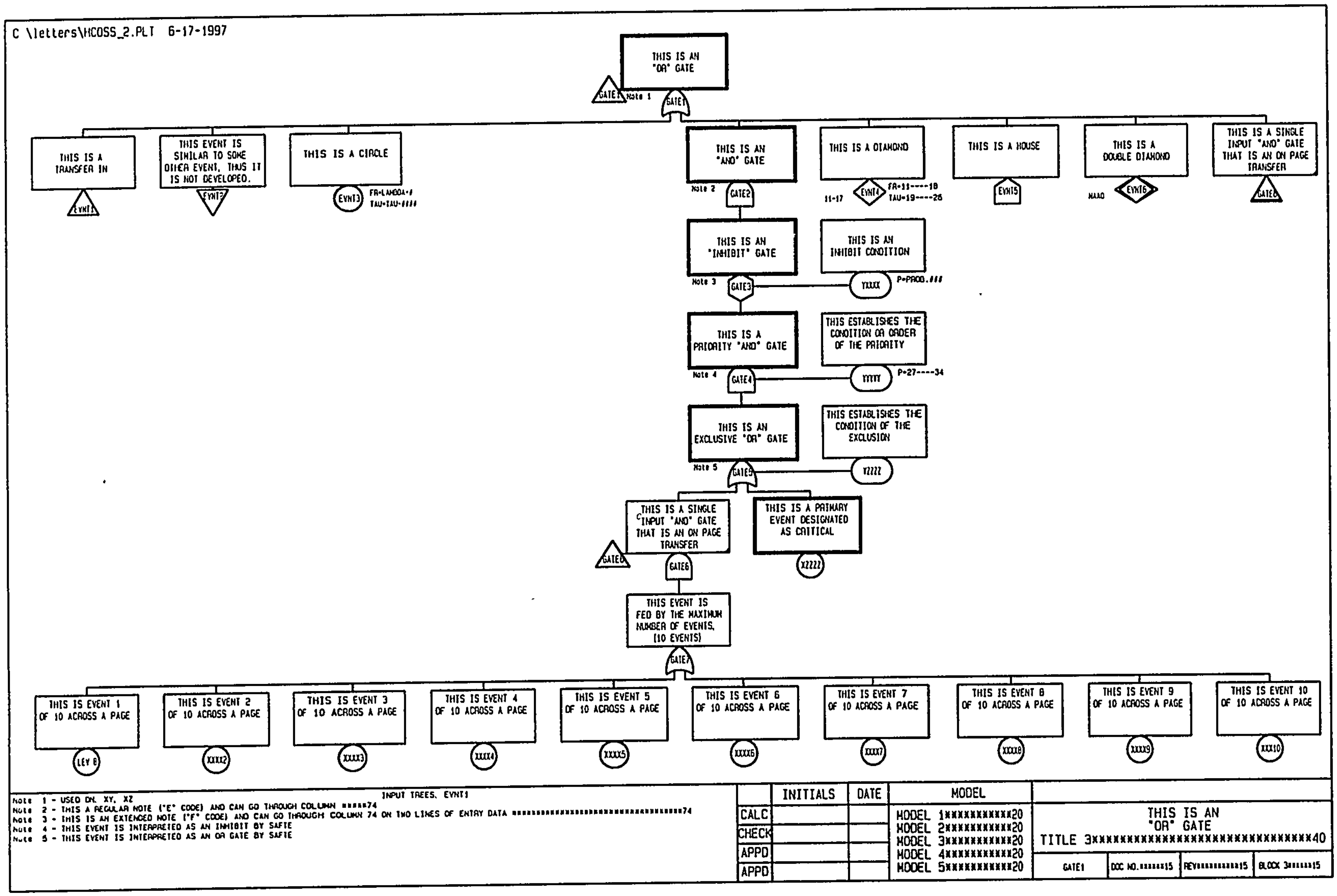
The SAFTE program provides for a number of checks of the input data to insure completeness and coherence of the input data set. Several output data sets can be used by the analyst as an aid to formulating the input data. One program capability that is of assistance in evaluating the validity of the results from the SAFTE program is the pathing tool. The program will draw the fault tree as a connectivity model indicating gate type and event mnemonics that are used to identify gates, basic events, conditions, and system state events. This drawing tool can start at the top undesired event or any intermediate event the analyst desires. The drawing may be limited by fault tree level, or accomplished to a specific basic event or set of basic events forming a failure path. This can show the analyst all ways that parts that form a specific failure path can reach the top event of the fault tree. This feature is a powerful aide in evaluating the validity of the failure path resulting from the evaluation of a fault tree.

The FTAB Program

The Fault Tree Analyzer Builder (FTAB) program developed by C.A. Ericson of the Boeing Company is an interactive graphics program to construct and edit individual fault trees. The FTAB program was initially developed as a DOS program with a; a Windows version now in development. The program uses classical fault tree symbols to develop fault tree pages up to eight levels high and 10 events wide. The fault tree events have text descriptions consisting of up to four lines of 20 characters. The drawing produced may be printed on 8 ½" by 11" or 11" by 17" pages, as illustrated in Figure 2.

The FTABUILD Program

The FTABUILD program is used to build a properly formatted basic input data set for the SAFTE program. An example input data set for the SAFTE program is illustrated in Figure 3.


C \letters\HCOSS_2.PLT 6-17-1997
THIS IS AN "OR" GATE
GATE1
Note 1
THIS IS A TRANSFER IN
EVNT1
THIS EVENT IS SIMILAR TO SOME OTHER EVENT, THUS IT IS NOT DEVELOPED.
EVNT2
THIS IS A CIRCLE
EVNT3
FR=LAMBDA=#
TAU=TAU=####
THIS IS AN "AND" GATE
Note 2
GATE2
THIS IS A DIAMOND
EVNT4
11-17
FR=11----18
TAU=19----26
THIS IS A HOUSE
EVNT5
THIS IS A DOUBLE DIAMOND
EVNT6
MAAO
THIS IS A SINGLE INPUT "AND" GATE THAT IS AN ON PAGE TRANSFER
GATE6
THIS IS AN "INHIBIT" GATE
Note 3
GATE3
THIS IS AN INHIBIT CONDITION
YXXX
P=PROD.###
THIS IS A PRIORITY "AND" GATE
Note 4
GATE4
THIS ESTABLISHES THE CONDITION OR ORDER OF THE PRIORITY
YYYY
P=27----34
THIS IS AN EXCLUSIVE "OR" GATE
Note 5
GATE5
THIS ESTABLISHES THE CONDITION OF THE EXCLUSION
YZZZZ
THIS IS A SINGLE INPUT "AND" GATE THAT IS AN ON PAGE TRANSFER
GATE6
THIS IS A PRIMARY EVENT DESIGNATED AS CRITICAL
XZZZZ
THIS EVENT IS FED BY THE MAXIMUM NUMBER OF EVENTS, (10 EVENTS)
GATE7
THIS IS EVENT 1 OF 10 ACROSS A PAGE
LEY 8
THIS IS EVENT 2 OF 10 ACROSS A PAGE
XXXX2
THIS IS EVENT 3 OF 10 ACROSS A PAGE
XXXX3
THIS IS EVENT 4 OF 10 ACROSS A PAGE
XXXX4
THIS IS EVENT 5 OF 10 ACROSS A PAGE
XXXX5
THIS IS EVENT 6 OF 10 ACROSS A PAGE
XXXX6
THIS IS EVENT 7 OF 10 ACROSS A PAGE
XXXX7
THIS IS EVENT 8 OF 10 ACROSS A PAGE
XXXX8
THIS IS EVENT 9 OF 10 ACROSS A PAGE
XXXX9
THIS IS EVENT 10 OF 10 ACROSS A PAGE
XXX10
INPUT TREES, EVNT1

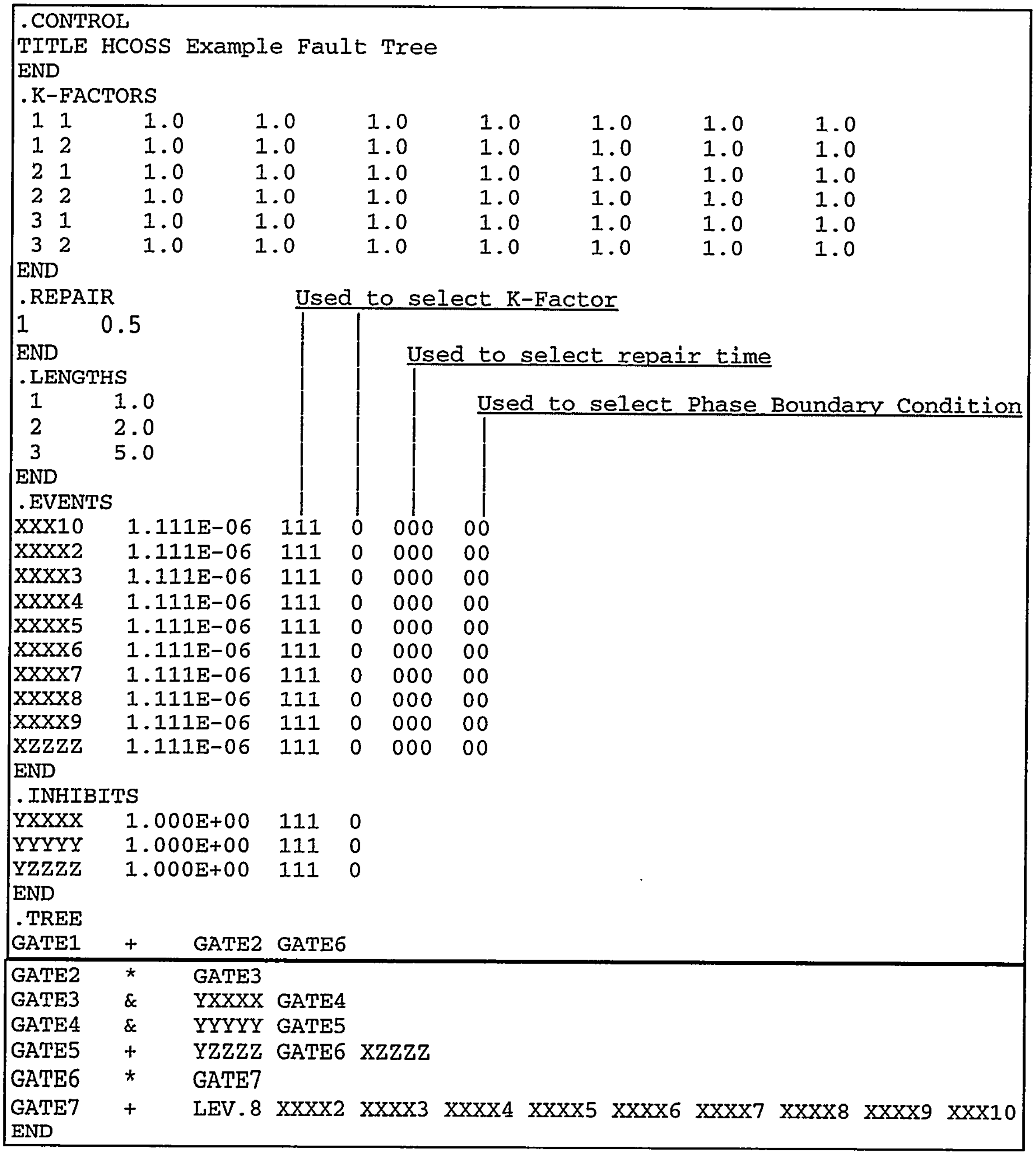
Note 1 - USED ON, XY, XZ
Note 2 - THIS A REGULAR NOTE ("E" CODE) AND CAN GO THROUGH COLUMN *****74
Note 3 - THIS IS AN EXTENDED NOTE ("F" CODE) AND CAN GO THROUGH COLUMN 74 ON TWO LINES OF ENTRY DATA ************************************74
Note 4 - THIS EVENT IS INTERPRETED AS AN INHIBIT BY SAFTE
Note 5 - THIS EVENT IS INTERPRETED AS AN OR GATE BY SAFTE

	INITIALS	DATE	MODEL
CALC			MODEL 1***********20
CHECK			MODEL 2***********20
APPD			MODEL 3***********20
APPD			MODEL 4***********20
			MODEL 5***********20

THIS IS AN
"OR" GATE
TITLE 3***********************************40

GATE1	DOC NO.******15	REV***********15	BLOCK 3******15

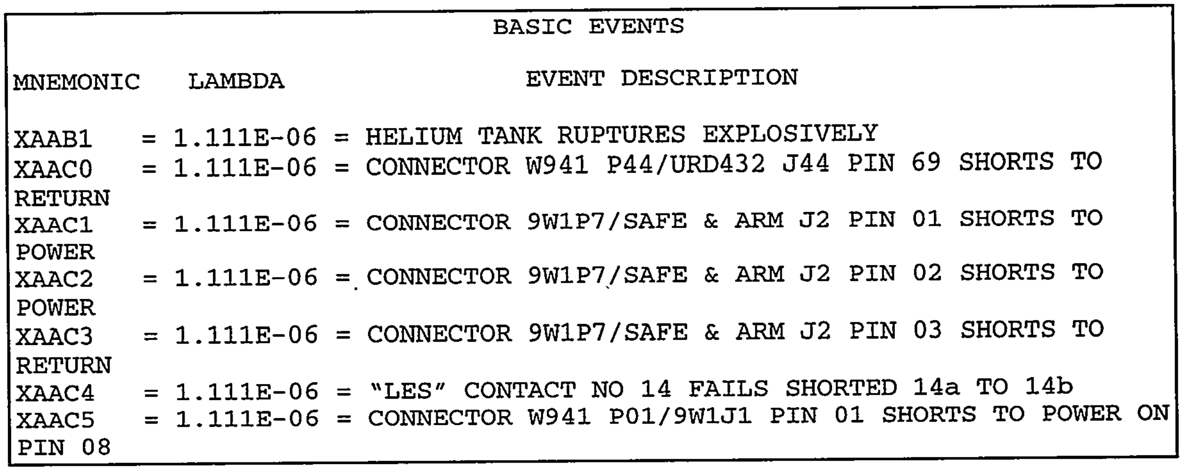
Figure 2. Example fault tree plot.



```
.CONTROL
TITLE HCOSS Example Fault Tree
END
.K-FACTORS
 1 1      1.0      1.0      1.0      1.0      1.0      1.0      1.0
 1 2      1.0      1.0      1.0      1.0      1.0      1.0      1.0
 2 1      1.0      1.0      1.0      1.0      1.0      1.0      1.0
 2 2      1.0      1.0      1.0      1.0      1.0      1.0      1.0
 3 1      1.0      1.0      1.0      1.0      1.0      1.0      1.0
 3 2      1.0      1.0      1.0      1.0      1.0      1.0      1.0
END
.REPAIR                 Used to select K-Factor
1    0.5
END                              Used to select repair time
.LENGTHS
 1     1.0                             Used to select Phase Boundary Condition
 2     2.0
 3     5.0
END
.EVENTS
XXX10   1.111E-06  111  0  000  00
XXXX2   1.111E-06  111  0  000  00
XXXX3   1.111E-06  111  0  000  00
XXXX4   1.111E-06  111  0  000  00
XXXX5   1.111E-06  111  0  000  00
XXXX6   1.111E-06  111  0  000  00
XXXX7   1.111E-06  111  0  000  00
XXXX8   1.111E-06  111  0  000  00
XXXX9   1.111E-06  111  0  000  00
XZZZZ   1.111E-06  111  0  000  00
END
.INHIBITS
YXXXX   1.000E+00  111  0
YYYYY   1.000E+00  111  0
YZZZZ   1.000E+00  111  0
END
.TREE
GATE1   +    GATE2 GATE6
GATE2   *    GATE3
GATE3   &    YXXXX GATE4
GATE4   &    YYYYY GATE5
GATE5   +    YZZZZ GATE6 XZZZZ
GATE6   *    GATE7
GATE7   +    LEV.8 XXXX2 XXXX3 XXXX4 XXXX5 XXXX6 XXXX7 XXXX8 XXXX9 XXX10
END
```

Figure 3. SAFTE Data Set example.

This program used the drawing files created by the FTAB program and combines them to BUILD a single fault tree input model. This program also provides an output listing of labels for gates, basic events, conditions, and system state events sorted by mnemonic. This output is illustrated in Figure 4, and is usually referred to as a report file. This data set is valuable for cross checking the text used in the tree and for inclusion in analysis documentation.



```
                                BASIC EVENTS

MNEMONIC    LAMBDA                  EVENT DESCRIPTION

XAAB1    = 1.111E-06 = HELIUM TANK RUPTURES EXPLOSIVELY
XAAC0    = 1.111E-06 = CONNECTOR W941 P44/URD432 J44 PIN 69 SHORTS TO
RETURN
XAAC1    = 1.111E-06 = CONNECTOR 9W1P7/SAFE & ARM J2 PIN 01 SHORTS TO
POWER
XAAC2    = 1.111E-06 = CONNECTOR 9W1P7/SAFE & ARM J2 PIN 02 SHORTS TO
POWER
XAAC3    = 1.111E-06 = CONNECTOR 9W1P7/SAFE & ARM J2 PIN 03 SHORTS TO
RETURN
XAAC4    = 1.111E-06 = "LES" CONTACT NO 14 FAILS SHORTED 14a TO 14b
XAAC5    = 1.111E-06 = CONNECTOR W941 P01/9W1J1 PIN 01 SHORTS TO POWER ON
PIN 08
```

Figure 4. Example of FTABUILD Report.

SAFTE, FTAB, and FTABUILD are all considered as analysis tools and are continuously being expanded in capability, comprehensiveness, and user friendliness as time and budget allows. They are evolving and will probably continue to do so as long as they are of use to our analysts.

Biography

James J. Hairston.
Boeing Defense & Space Group System Safety
PO Box 3999, Seattle, WA 98124-2499
Phone (253) 773 9421
Email: james.j.hairston@boeing.com

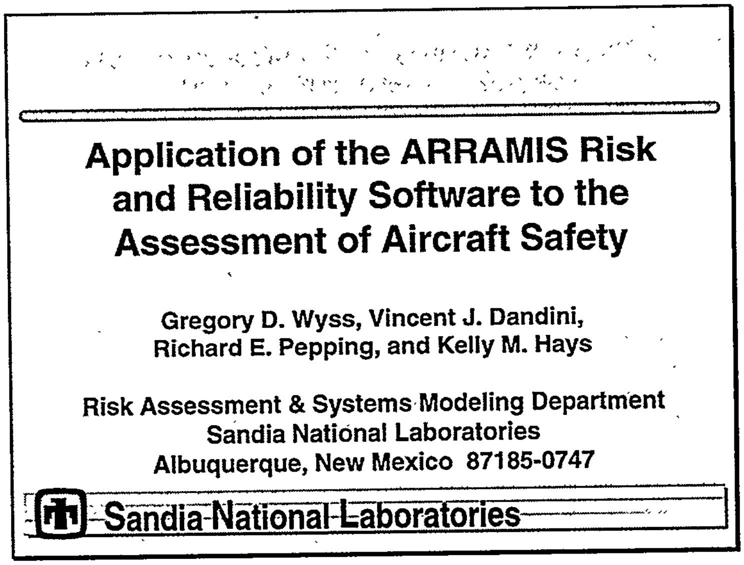
Mr. Hairston is a Principle Safety Engineer for Boeing Defense & Space Group. He has Bachelor of Science degrees from Jacksonville University in Mathematics & Physics; a Masters in System Safety Engineering from the University of Southern California (USC), and is listed in Marquees Who's Who. He served in the Air Force as an Electronics Technician, was commissioned, and became a Navigator Bombardier. He flew over 200 combat missions in Vietnam, and retired from the Air Force in 1978. As a Principle System Safety Engineer with the Boeing Company, Mr. Hairston has accomplished safety analyses on numerous major programs.

Application of the ARRAMIS Risk and Reliability Software to the Assessment of Aircraft Safety

Gregory D. Wyss
Vincent J. Dandini
Richard E. Pepping
Kelly M. Hays
Sandia National Laboratories*
Albuquerque, New Mexico

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

Slide 1



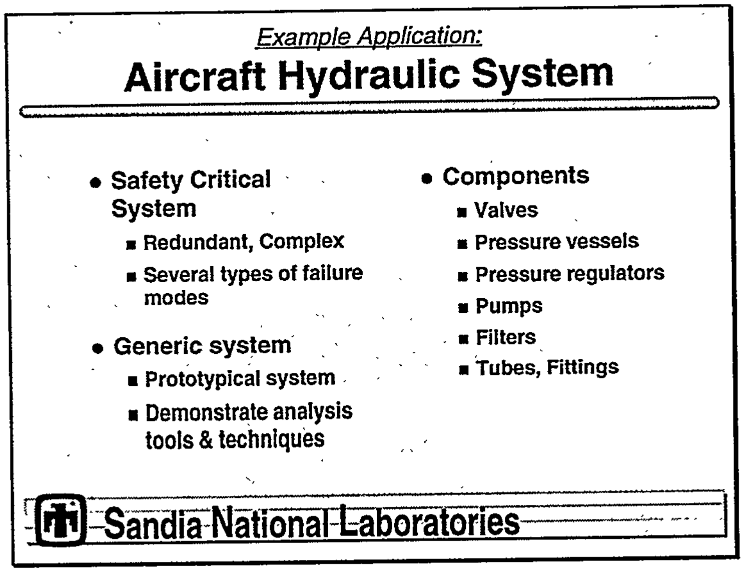
Application of the ARRAMIS Risk and Reliability Software to the Assessment of Aircraft Safety

Gregory D. Wyss, Vincent J. Dandini,
Richard E. Pepping, and Kelly M. Hays

Risk Assessment & Systems Modeling Department
Sandia National Laboratories
Albuquerque, New Mexico 87185-0747

Sandia National Laboratories

Slide 2



Example Application:

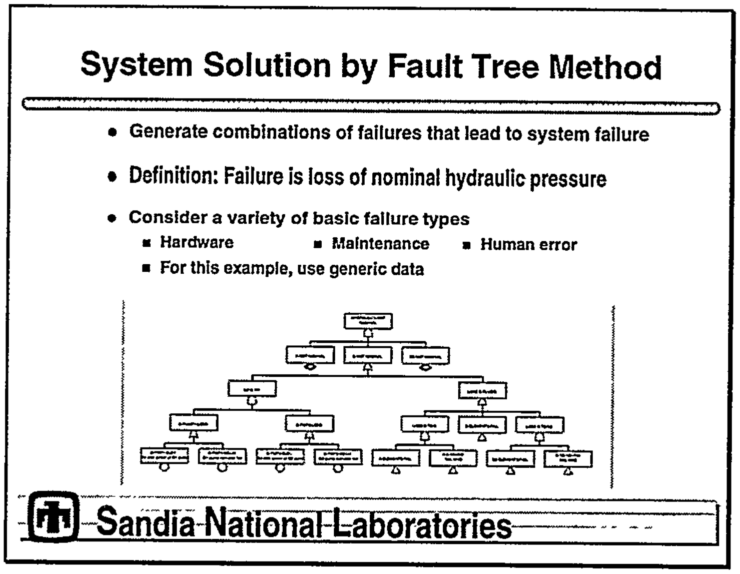
Aircraft Hydraulic System

- Safety Critical System
  - Redundant, Complex
  - Several types of failure modes
- Generic system
  - Prototypical system
  - Demonstrate analysis tools & techniques

- Components
  - Valves
  - Pressure vessels
  - Pressure regulators
  - Pumps
  - Filters
  - Tubes, Fittings

Sandia National Laboratories

Slide 3

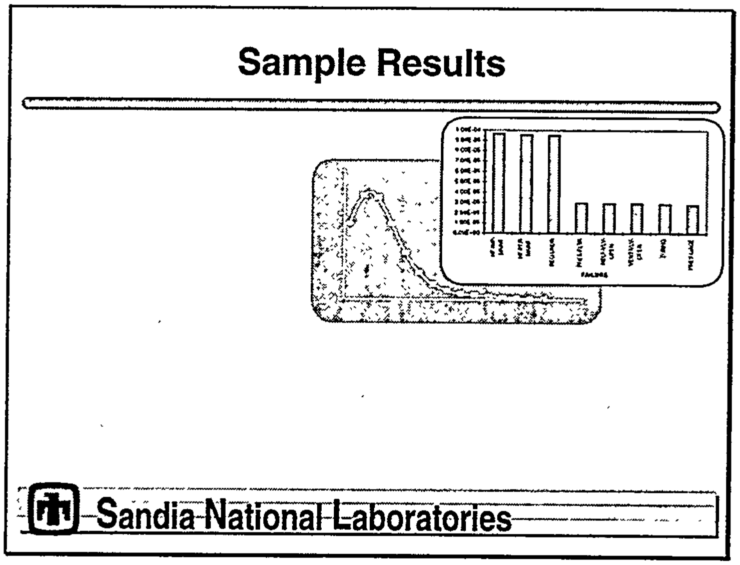


System Solution by Fault Tree Method

- Generate combinations of failures that lead to system failure
- Definition: Failure is loss of nominal hydraulic pressure
- Consider a variety of basic failure types
  - Hardware
  - Maintenance
  - Human error
  - For this example, use generic data

Sandia National Laboratories

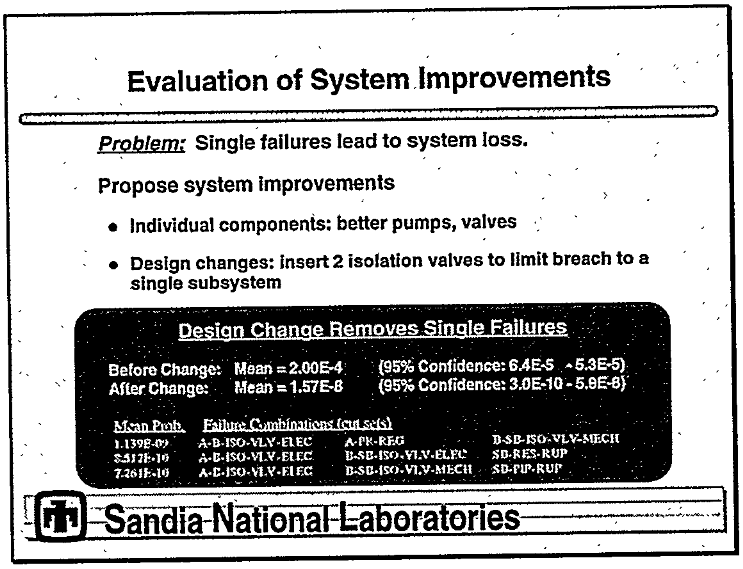
Slide 4



Sample Results

Sandia National Laboratories

Slide 5



Evaluation of System Improvements

Problem: Single failures lead to system loss.

Propose system improvements

- Individual components: better pumps, valves
- Design changes: insert 2 isolation valves to limit breach to a single subsystem

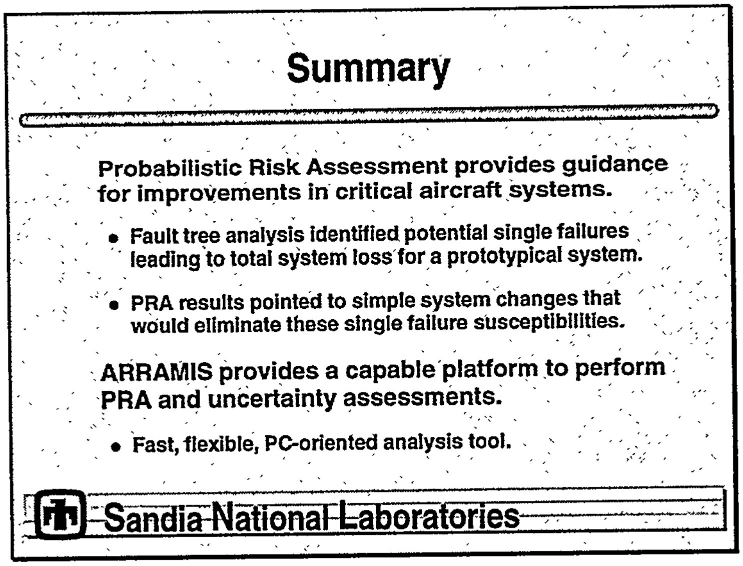
Design Change Removes Single Failures

Before Change: Mean = 2.00E-4 (95% Confidence: 6.4E-5 - 5.3E-5)
After Change: Mean = 1.57E-8 (95% Confidence: 3.0E-10 - 5.9E-8)

Mean Prob.	Failure Combinations (cut sets)		
1.139E-09	A-B-ISO-VLV-ELEC	A-PK-REG	B-SB-ISO-VLV-MECH
8.517E-10	A-B-ISO-VLV-ELEC	B-SB-ISO-VLV-ELEC	SD-RES-RUP
7.261E-10	A-B-ISO-VLV-ELEC	B-SB-ISO-VLV-MECH	SD-PIP-RUP

Sandia National Laboratories

Slide 6



Summary

Probabilistic Risk Assessment provides guidance for improvements in critical aircraft systems.

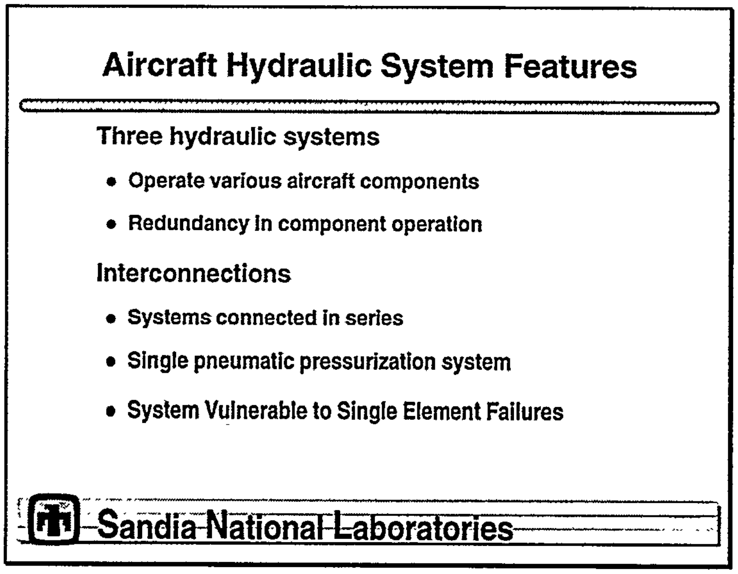
- Fault tree analysis identified potential single failures leading to total system loss for a prototypical system.
- PRA results pointed to simple system changes that would eliminate these single failure susceptibilities.

ARRAMIS provides a capable platform to perform PRA and uncertainty assessments.

- Fast, flexible, PC-oriented analysis tool.

Sandia National Laboratories

Slide 7



Aircraft Hydraulic System Features

Three hydraulic systems

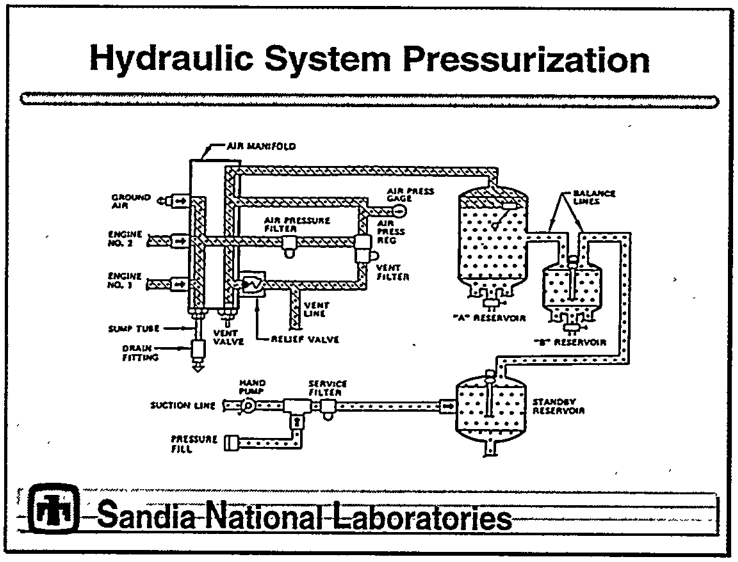
- Operate various aircraft components
- Redundancy in component operation

Interconnections

- Systems connected in series
- Single pneumatic pressurization system
- System Vulnerable to Single Element Failures

Sandia National Laboratories

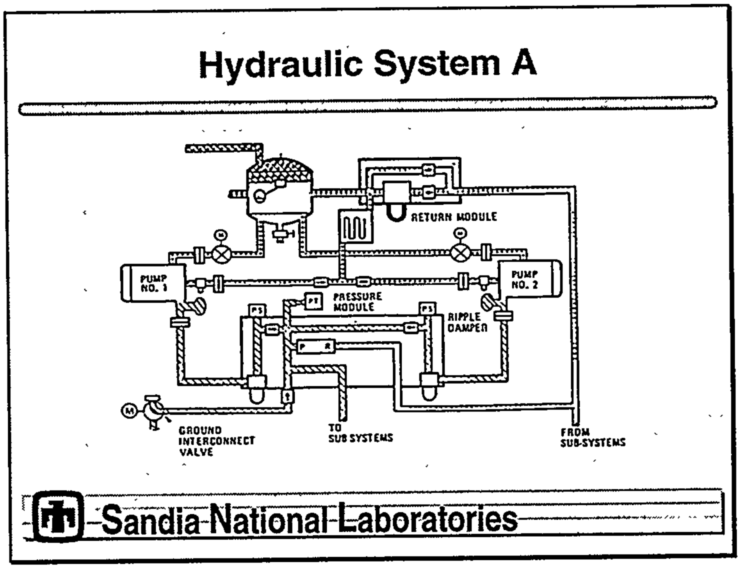
Slide 8



Hydraulic System Pressurization

Sandia National Laboratories

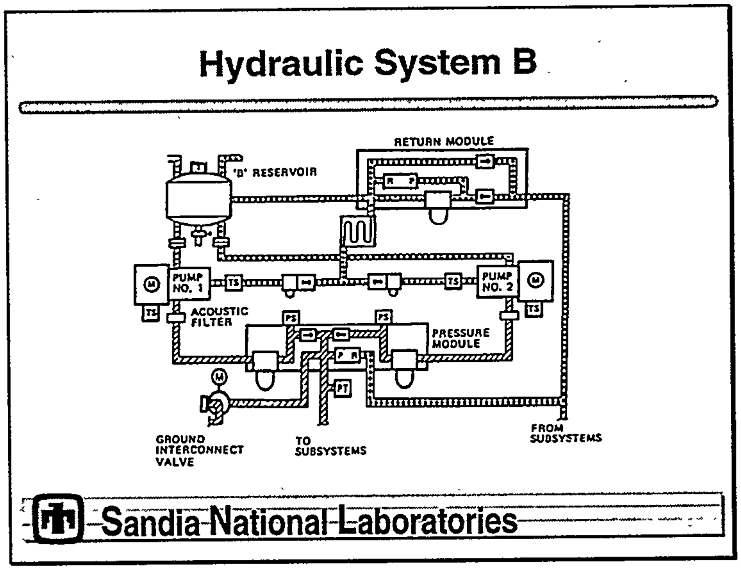
Slide 9



Hydraulic System A

Sandia National Laboratories

Slide 10

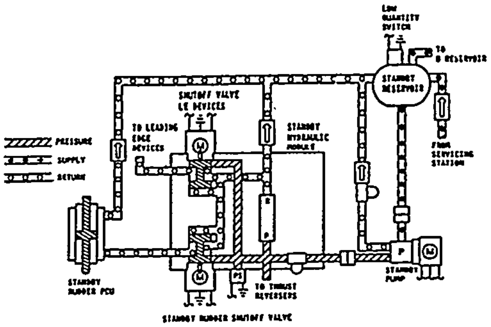


Hydraulic System B

Sandia National Laboratories

Slide 11

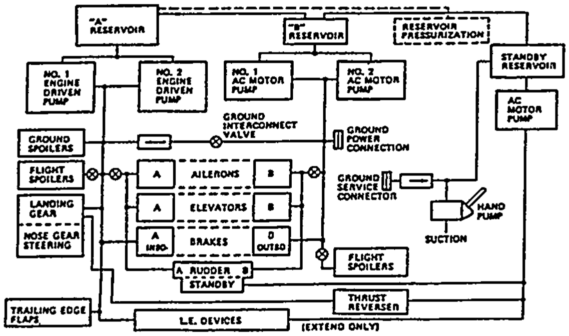
Standby System



Sandia National Laboratories

Slide 12

Hydraulic System Interconnections



Sandia National Laboratories

Intentionally left blank

Safety Analysis of Redundant Systems Using Fuzzy Probability Theory

James Dunyak
Ihab W. Saad
Donald Wunsch
Texas Tech University
Lubbock, Texas

Abstract

This paper develops a new theory of independent fuzzy probabilities, that addresses limitations of fuzzy fault trees both and Zadeh's fuzzy extension of probability. In contrast to the fuzzy fault tree approach, the new theory is complete since it assigns a fuzzy probability to every event. In the case of a probability theory built from independent events, Zadeh's extension is not consistent with fuzzy fault trees. Our new extension is also consistent. The new theory is demonstrated with an example.

Introduction

Many safety assessment models require, as input, the probabilities of a number of independent events. Often these probabilities can be estimated from data or theory, but sometimes choosing probabilities for input is difficult. This work is part of an ongoing study in high-consequence surety analysis. Many of the factors of interest come from traditionally non-mathematical areas of research, such as estimating the probability of a terrorist attack, compliance with safety practices, or a flawed design of a safety system. Other factors are too expensive or dangerous to measure experimentally. Instead, expert opinion is used to provide these probabilities, but these estimates are rarely precise. Fuzzy sets and possibility theory provide a tool for describing and analyzing these uncertain quantities.

Fuzzy fault trees provide a powerful and computationally efficient technique for developing fuzzy probabilities based on independent inputs. The probability of any event that can be described in terms of a sequence of independent unions, intersections, and complements may be calculated by a fuzzy fault tree. Unfortunately, fuzzy fault trees do not provide a complete theory: Events of substantial practical interest for calculating safety margins cannot be described only by independent operations. Thus the standard fuzzy extension (based on fuzzy fault trees) is not complete, since not all events are assigned a fuzzy probability. Zadeh and others have proposed other complete extensions. Unfortunately, the calculations of these models are not consistent with the underlying fuzzy probabilities of the independent inputs.

In this paper, we discuss a new extension of crisp probability theory. Our model is based on n independent inputs, each with a fuzzy probability. The elements of our sample space describe exactly which of the n input events did and did not occur. Our extension is complete, since a fuzzy probability is assigned to every subset of the sample space. Our extension is also consistent with all calculations that can be arranged as a fault tree [1].

Our approach allows the reliability analyst to develop complete and consistent fuzzy reliability models from existing crisp models. This allows a comprehensive analysis of the system. Computational algorithms are provided both to extend existing models and develop new models. The technique is demonstrated with an example.

An uncertain parameter $F \in \Re$ may be assigned a fuzzy membership function $\underline{F}(y)$ mapping $\Re$ into [0,1], which is the membership function of a fuzzy set $\underline{F}$. Then the possibility that $\underline{F}$ is in a set S is designated by $\Pi_F(S)$, and

$$\Pi_F(S)=\sup_{y \in S} \underline{F}(y).$$

This is the sense in which we describe uncertainty in the probability of an event A. Note the inherent conservative nature of possibility theory: the possibility of a set is high if a single point in the set has high possibility. This may be viewed as a worst-case calculation and is appropriate for the study of rare but high- consequence events. An uncertainty model based on probability theory, on the other hand, better models the average risk over repeated trials.

In this paper, $\underline{P}_A$ is a fuzzy set describing uncertainty in the crisp number P(A). Fuzzy fault trees provide a method for developing fuzzy probabilities based on independent fuzzy inputs $\underline{P}_A$ [2]. The probability of any event that can be described in terms of a sequence of independent unions, intersections, and complements may be calculated by a fuzzy fault tree. Unfortunately, we show below that some events of substantial practical interest cannot be described only by independent operations; fuzzy fault trees do not provide a complete theory. Thus the standard fuzzy extension (based on fuzzy fault trees) is not complete, since not all events are assigned a fuzzy probability. Zadeh proposed another extension that is complete [3], but his extension is shown (in our context) to be inconsistent with the calculations from fuzzy fault trees.

Here we develop a new extension of crisp probability theory, based on n independent inputs, each with a fuzzy probability. The elements of our sample space describe exactly which of the n input events did and did not occur. This extension will be shown to be both complete and consistent. These results are discussed in more detail in [1].

Independent Calculations and Fuzzy Fault Trees

Throughout this paper, we use the bar notation $\underline{P}_A$ to indicate a fuzzy set representing probability of A, the notation $\underline{P}_A(y)$ to indicate the corresponding membership function, and $\underline{P}_A{}^{\alpha}=\{y:\underline{P}_A(y)\geq\alpha\}$ to indicate the corresponding α-cuts. A convex fuzzy set $\underline{P}_A$ has special structure; each α-cut is a closed and convex subset of $\mathfrak{R}$. We see for a convex fuzzy probability that each α-cut can be written as a closed interval with $\underline{P}_A{}^{\alpha} = [P_{A1}{}^{\alpha}, P_{A2}{}^{\alpha}]$. This assumption of convexity is equivalent to assuming that the membership function has a single mode. Earlier work with independent fuzzy probabilities relied on this (often quite reasonable) assumption of convexity, but our work will be more general. Following the lead of most fuzzy models, all fuzzy sets here are required to have nonempty α=1 cut. This property is called normality.

Consider independent events $A_1, A_2, \ldots, A_n$ with estimated fuzzy probabilities $\underline{P}_{A1}$ $\underline{P}_{A2}, \ldots, \underline{P}_{An}$, which will be used in a reliability model. Our goal is to build a fuzzy probability theory to describe the probabilities of various unions, intersections, and complements of these sets. To this end, we follow the standard approach of Tanaka et. al. [2] and first build fuzzy intersections of independent events.

If events A_i are independent, then for crisp probabilities we have

$$P(A_i \cup A_j)=P(A_i)+P(A_j)-P(A_i)P(A_j)$$

and

$$P(A_i \cap A_j)=P(A_i)P(A_j).$$

Using the usual extension principle, we define the fuzzy independent union and intersection as

$$\underline{P}_{Ai\cup Aj}(y)= \quad \sup_{y=pi+pj-pi\,pj} \quad \min[\,\underline{P}_{Ai}(p_i),\underline{P}_{Aj}(p_j)] \qquad \text{(Eq. 1)}$$

and

$$\underline{P}_{Ai\cap Aj}(y)= \quad \sup_{y=pi\,pj} \quad \min[\,\underline{P}_{Ai}(p_i),\underline{P}_{Aj}(p_j)]. \qquad \text{(Eq. 2)}$$

Complements of fuzzy probabilities are similarly defined by

$$\underline{P}_{Ai}(y)= \quad \sup_{y=1-pi} \quad \underline{P}_{Ai}(p_i) \; = \; \underline{P}_{Ai}(1-y). \qquad \text{(Eq. 3)}$$

We then have the following familiar properties:

$$\underline{P}_{Ai\cup Aj} = \underline{P}_{Aj\cup Ai} \qquad\qquad \underline{P}_{Ai\cap Aj} = \underline{P}_{Aj\cap Ai}$$

$$\underline{P}_{(Ai\cup Aj)\cup Ak} = \underline{P}_{Ai\cup(Aj\cup Ak)} \qquad \underline{P}_{(Ai\cap Aj)\cap Ak} = \underline{P}_{Ai\cap(Aj\cap Ak)}$$

$$\underline{P}_{(Ai\cup Aj)'} = \underline{P}_{Aj'\cap Ai'} \qquad\qquad \underline{P}_{(Ai\cap Aj)'} = \underline{P}_{Aj'\cup Ai'}\,. \qquad \text{(Eq. 4)}$$

This third formula is DeMorgan's law and extends in the obvious way to

$$\underline{P}_{(A1\cup A2\cup\ldots\cup Ak)'} = \underline{P}_{A1'\cap A2'\cap\ldots\cap Ak'} \qquad\qquad \underline{P}_{(A1\cap A2\cap\ldots\cap Ak)'} = \underline{P}_{A1'\cup A2'\cup\ldots\cup Ak'} \quad \text{(Eq. 5)}$$

If the fuzzy probabilities are convex, we have the relationships between endpoints of the α-cut intervals

$$[P_{Ai\cup Aj\ 1}{}^{\alpha}, P_{Ai\cup Aj\ 2}{}^{\alpha}] =$$

$$[P_{Ai\ 1}{}^{\alpha} + P_{Aj\ 1}{}^{\alpha} - P_{Ai\ 1}{}^{\alpha} P_{Aj\ 1}{}^{\alpha},\quad P_{Ai\ 2}{}^{\alpha} + P_{Aj\ 2}{}^{\alpha} - P_{Ai\ 2}{}^{\alpha} P_{Aj\ 2}{}^{\alpha}] \qquad \text{(Eq. 6)}$$

and

$$[P_{Ai\cap Aj\ 1}{}^{\alpha}, P_{Ai\cap Aj\ 2}{}^{\alpha}] = [P_{Ai\ 1}{}^{\alpha} P_{Aj\ 1}{}^{\alpha}, P_{Ai\ 2}{}^{\alpha} P_{Aj\ 2}{}^{\alpha}]. \qquad \text{(Eq. 7)}$$

Unfortunately, the distributive laws fail. Straightforward application of the above formulas shows

$$\underline{P}_{Ai\cup(Aj\cap Ak)} \neq \underline{P}_{(Ai\cup Aj)\cap(Ai\cup Ak)} \qquad \underline{P}_{Ai\cap(Aj\cup Ak)} \neq \underline{P}_{(Ai\cap Aj)\cup(Ai\cap Ak)}\ . \qquad \text{(Eq. 8)}$$

This formula fails because of the violation of independence.

As we see in Equation 8, care must be used in organizing calculations to maintain independence. This is usually done by describing calculations as a tree structure. This viewpoint was naturally assumed in several papers on fuzzy fault trees [2,4,5,6,7,8]. To illustrate this concept, consider the example tree diagram in Figure 1. This diagram contains three varieties of nodes: unions, intersections, and complements. At the nodes, fuzzy input probabilities are combined according to the formulas in equations (1-3). As long as the tree only feeds upward and each node has only one output, independence is maintained. Because of DeMorgan's laws in Equation 5, we can develop fault trees using only unions and intersections (but no complements) or only intersections and complements (but no unions). Thus several somewhat different approaches to fault trees are in fact equivalent when the standard extensions in Equations 1 through 3 are used.

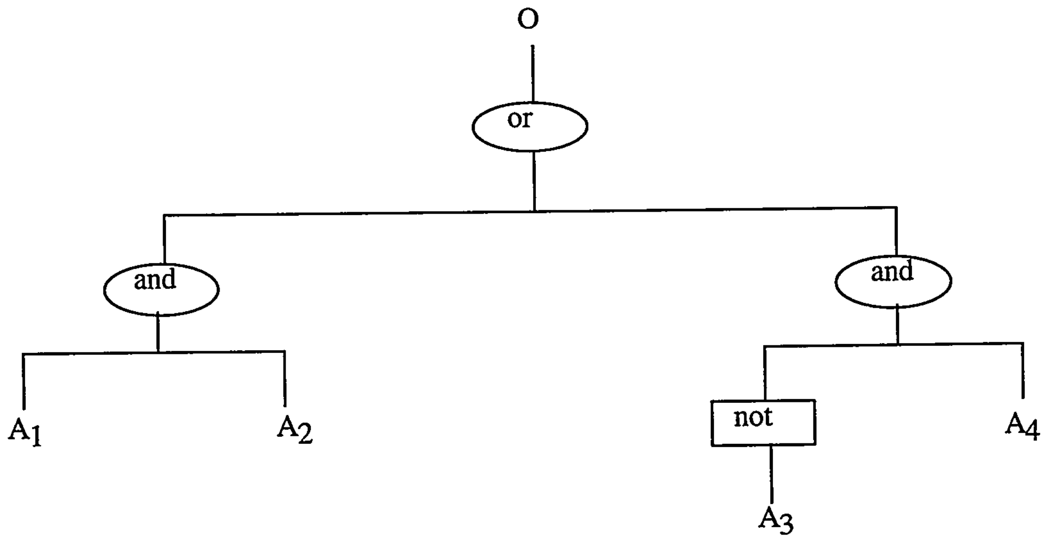


Figure 1. A fuzzy fault tree which maintains independence.

Unfortunately, many problems do not easily fit into a straightforward tree structure, with each node having only one output. In our investigations, certain factors (such as terrorism risk) influence many different events, so that construction of independent trees is problematic. As we will see in the next section, other problems also occur.

Completeness

The representation of some sets can be rearranged to allow use of Equations 1 through 3. For example, in Equation 8, since $A_i \cup A_j$ is not (necessarily) independent of $A_i \cup A_k$, we could simply define

$$\underline{P}_{(Ai\cup Aj)\cap(Ai\cup Ak)} = \underline{P}_{Ai\cup(Aj\cap Ak)} \, . \qquad \text{(Eq. 9)}$$

Now A_j and A_k are independent so we can correctly calculate $\underline{P}_{Aj\cap Ak}$ using equation 2. Since A_i is independent of $A_j \cap A_k$, we can apply Equation 1 to calculate $\underline{P}_{Ai\cup(Aj\cap Ak)}$. Unfortunately, unraveling such relationships can be very difficult in complex models. Of greater concern is the fact that not all possible fuzzy probabilities can be calculated by rearranging them into a calculation that maintains independence.

For example, a listing of all possible independent calculations easily shows that $(A_i' \cap A_j) \cup (A_i \cap A_j')$ may not be rearranged to allow calculation by independence formulas. Consider two independent system components numbered i and j. If event A_i indicates that i is operational and A_j indicates that j is operational, then $\underline{P}_{(Ai'\cap Aj)\cup(Ai\cap Aj')}$ is the fuzzy probability that exactly one of the two components is operational. The inability of Equations 1 through 3 to calculate such probabilities is a serious limitation in reliability applications.

This limitation is illustrated by the example we use in this paper. Consider the three-stage manufacturing process shown in Figure 2. This diagram shows the flow of an industrial process through three stages. Stage 1 may be performed by two redundant units, each with a throughput capacity of 0.5 items per second. If both units 1 and 2 are operational, stage 1 has a throughput capacity of 1 item per second. If only one of the two units is operational, the stage 1 throughput is 0.5 items per second. If neither unit 1 nor unit 2 is operational, the throughput capacity of stage 1 is 0. This viewpoint may be used to build the throughput capacity of the entire process, with the capacity of stage 1 limiting the possible flow through stage 2, and so on. Let A_i be the event that unit i is operational. Assume the process has repairable (or replaceable) independent units, and that the process has been in operation long enough to approximately reach stationarity. Then $p_i = P(A_i)$ is the stationary readiness coefficient of unit i [9]. Letting T be the process throughput capacity, we can calculate the steady state distribution of T as

$$P(T=1) = P(A_1 \cap A_2 \cap A_3 \cap A_4 \cap A_5 \cap A_6)$$

$$P(T=0.8) = P(A_1 \cap A_2 \cap ((A_3 \cap A_4 \cap A_5') \cup (A_3 \cap A_4' \cap A_5) \cup (A_3' \cap A_4 \cap A_5) \cap A_6), \qquad \text{(Eq. 10)}$$

and so on. Possible values of T are {0, 0.4, 0.5, 0.8, 1.0}. Calculation of the distribution of T follows easily when the stationary readiness coefficients are crisp; our goal is to study this process with fuzzy readiness coefficients. To calculate the fuzzy probability $\underline{P}_{T=0.5}$, we must calculate the fuzzy probability that exactly one of units 1 and 2 is functional. Unfortunately, as discussed in the proceeding paragraph, this fuzzy probability cannot be modeled using Equations 1 through 3. Several other "gaps" occur in the fuzzy reliability model of the system.

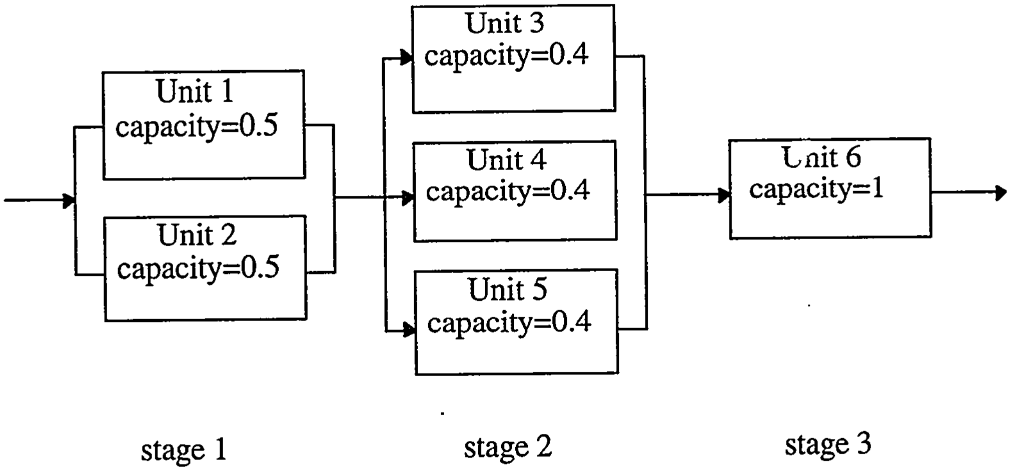


Figure 2. A three-stage industrial process.

Clearly, many important fuzzy probabilities cannot be reached by the standard independence formulas in equations 1-3. To understand what sets are missing, we should more carefully specify the probability space of interest in our reliability problem.

Definition: The sample space S_n based on n independent events A_1, A_2, ..., A_n the set of 2^n distinct elements

$$S_n=\{s_1,s_2, ..., s_{2^n}\}$$

of the form

$$s=\cap_{i=1,n}B_i \quad \text{with} \quad B_i=A_i \quad \text{or} \quad B_i=A_i'.$$

For the remainder of this paper, the notation A_i will be used to indicate the independent events from which S_n is defined.

Note that S_n has a finite number of elements, so our sample space is discrete. A fuzzy probability theory, in keeping with both our needs and the structure of crisp probability theory for discrete sample spaces, should assign a probability for every subset of S_n.

Definition: A fuzzy probability theory is called complete if it assigns a fuzzy probability to every subset of S_n.

Consider a set subset B of S_n, which can be constructed through independent operations. For an event B, which can be organized as an independent calculation, we define $\underline{B}$ as the fuzzy probability theory resulting from repeated application of Equations 1 through 3.

Zadeh's Linguistic Probabilities and Consistency

Now we must build the definition of fuzzy probability for subsets of S_n from the given fuzzy probabilities $\underline{P}_{A1}$ $\underline{P}_{A2}$, ..., $\underline{P}_{An}$. Following Zadeh [3], we can define an extension. Consider a proper subset B of a sample space $S_n=\{s_1,s_2,\ldots,s_{2^n}\}$, with $B=\{t_1, t_2, \ldots, t_k\}$ where t_i are the elements in S_n which are in B. We define, using a superscript Z to indicate Zadeh's extension,

$$\underline{P}_B{}^Z(y)=\sup_{y=x1+x2+\ldots+xk;\ \ x1+x2+\ldots+xk\leq 1} \min[\underline{P}_{\{t1\}}(x_1),\underline{P}_{\{t2\}}(x_2),\ldots,\underline{P}_{\{tk\}}(x_k)]\ . \qquad \text{(Eq. 11)}$$

The inequality in the sup is a result of the interactivity of crisp probabilities, since

$$\Sigma_{i=1,2^n}\ P(\{s_i\})\ =1.$$

Each $\underline{P}_{si}(.)$ is calculated from $\underline{P}_{A1}$ $\underline{P}_{A2}$, ..., $\underline{P}_{An}$ using independence and Equations 1 through 3. This formulation does provide a fuzzy probability for every subset of S_n. Unfortunately, Equations 11 and 12 are not consistent with the calculations in Equations 1 through 3 [1].

A Complete and Consistent Formulation of Independent Fuzzy Probabilities

As an alternative to Zadeh's approach, we cônsider a different extension. Consider a reliability model built in terms of the independent fuzzy probabilities $\underline{P}_{Ai}$, i=1,2, ..., n, for sample space S_n. Using, for crisp probabilities, the definition $p_i=P(A_i)$, we see, for subset B of S_n, that

$$P(B)=\ P(\ \cup_{si\in B}\ \{s_i\}\ )=\ \Sigma_{si\in B}\, P(\ \{s_i\}\ )=\ f_B(p_1,p_2,\ldots,p_n\ ) \qquad \text{(Eq. 12)}$$

for a function $f_B(.)$. Thus the crisp probability of every B can be written uniquely as a function $f_B(.)$ in terms of p_1, p_2, ..., p_n. For the empty set ϕ we have $f_\phi(p_1,p_2,\ldots,p_n)=0$ and for the sample space we have $f_{Sn}(p_1,p_2,\ldots,p_n)=1$. We use these functions to build our extension of Equations 1 through 3. We can now define our extension for B.

Definition: For subset B of S_n, the extension of independent fuzzy probabilities is

$$\underline{P}_B{}^E(y)=\sup_{y=\,fB(p1,p2,\ldots,pn\,)} \min(\underline{P}_{A1}(p_1),\underline{P}_{A2}(p_2),\ldots,\underline{P}_{An}(p_n)]$$

with $P(B)=f_B(p_1,p_2,\ldots,p_n)$ when $P(A_i)= p_i$. If, for a fixed y, the set $\{(p_1,p_2,\ldots,p_n):y=f_B(p_1,p_2,\ldots,p_n)\}$ is empty, we take $\underline{P}_B{}^E(y)=0$. The function $f_B(.)$ is defined in Equation 12.

The extension $\underline{P}_B{}^E$, when derived from independent fuzzy probabilities $\underline{P}_{Ai}$, is both consistent and complete. See [1] for a complete proof.

An Example

To demonstrate the technique, we consider the three-stage process discussed above and illustrated in Figure 2. To demonstrate the calculations, the event T=0.8 will be discussed. To simplify the illustration, all six independent units are assumed to have the fuzzy readiness coefficient shown in Figure 3. Note that

$$P(T=0.8)= f_{T=0.8}\,(p_1,\ldots,p_6)=p_1p_2(p_3p_4(1\text{-}p_5)+p_3(1\text{-}p_4)p_5+(1\text{-}p_3)p_4p_5)p_6$$

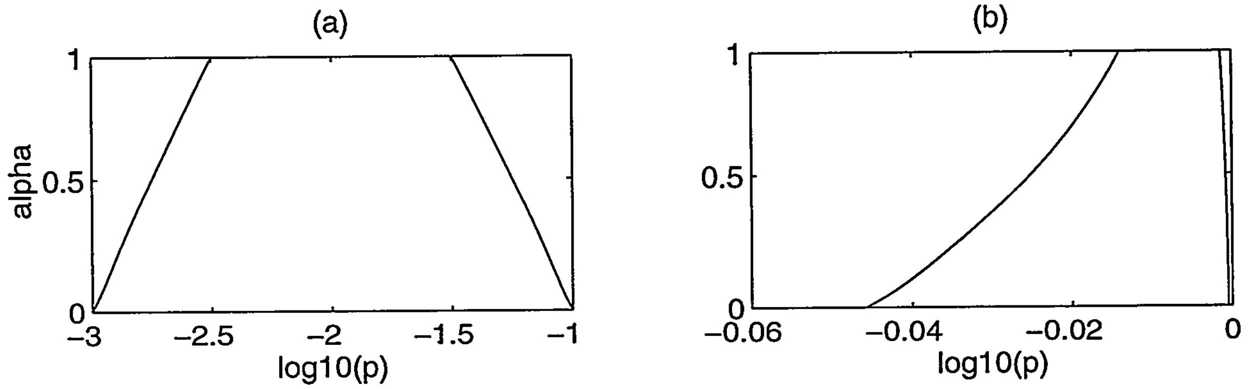
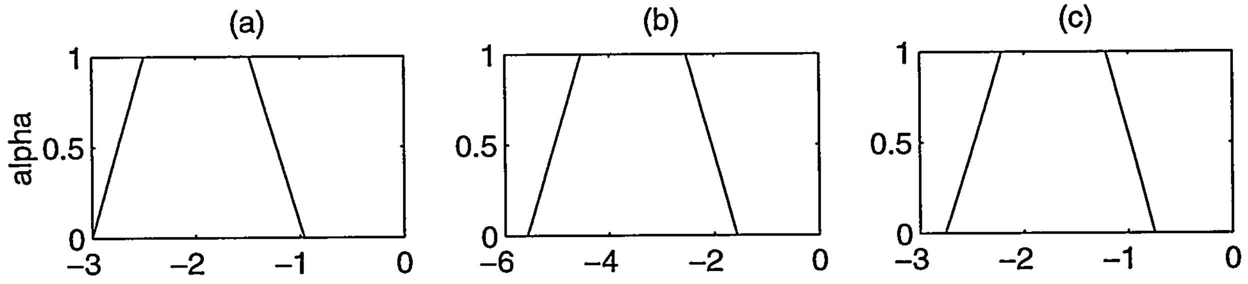


Figure 3. The fuzzy idleness coefficient (a) and readiness coefficient (b) for a single unit.

Figure 4 shows the resulting fuzzy probabilities for T=0, T=0.4, T=0.5, T=0.8, and T=1.0. These fuzzy probabilities describe the long-term performance of the industrial process.



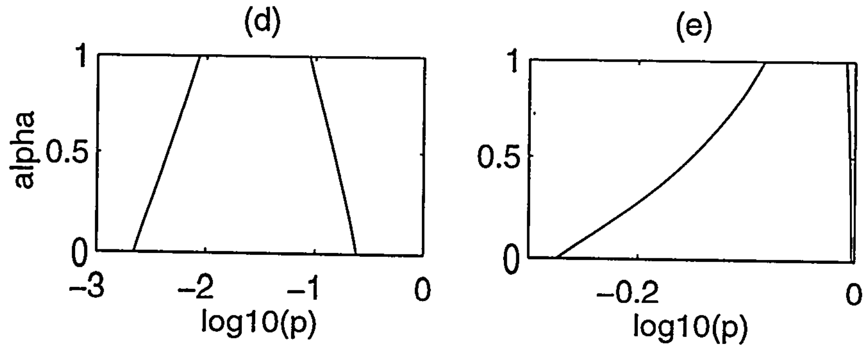


Figure 4. The resulting fuzzy probabilities for the process throughput T=0 (a), T=0.4 (b), T=0.5 (c), T=0.8 (d), and T=1 (e).

References

[1] Dunyak, J., Saad, I., and Wunsch, D., "A Theory of Independent Fuzzy Probabilities for Reliability," preprint.

[2] Tanaka, H, Fan, C., Lai, F., and Toguchi, K., 1983, "Fault Tree Analysis by Fuzzy Probability," *IEEE Transactions on Reliability*, Vol. R-32, No. 5, p. 453-457.

[3] Zadeh, L.A., 1975, "The Concept of a Linguistic Variable and its Application to Approximate Reasoning III," *Information Sciences*, 8, p. 199-249.

[4] Kenarangui, R., 1991, "Event-Tree Analysis by Fuzzy Probability," *IEEE Transactions on Reliability*, Vol. 40, No. 1, p. 120-124.

[5] Singer, D., 1990, "A Fuzzy Set Approach to Fault Tree and Reliability Analysis," *Fuzzy Sets and Systems*, Vol. 34, p. 145-155.

[6] Weber, D., 1994, "Fuzzy Fault Tree Analysis," *Proceedings for the Third IEEE International Conference on Fuzzy Systems*, Orlando, Florida, p. 1899-1904.

[7] Cooper, J.A., 1994, *Fuzzy-Algebra Uncertainty Analysis of Abnormal-Environment Safety Assessment*, Sandia Technical Report SAND93-2665 UC-706.

[8] Page, L.B., and Perry, J.E., 1994, "Standard Deviation as an Alternative to Fuzziness in Fault Tree Models," *IEEE Transactions on Reliability*, Vol. 43, No. 3, p. 402-407.

[9] Ushakov, I.A., 1994, *Handbook of Reliability Engineering*, John Wiley and Sons.

Biography

James Dunyak
Department of Mathematics
Texas Tech University
Lubbock, TX 79409

James Dunyak received a BS and MS in Engineering Mechanics from Virginia Tech in 1982 and 1987 respectively. From 1984 through 1992, he worked in systems engineering variously for Locus Inc, the Naval Research Laboratory, and Mitre Corporation. After completing his PhD in Applied Mathematics from the University of Maryland in 1994, he took a position in the Department of Mathematics at Texas Tech University. His research interests include random processes and their application to a wide variety of engineering and physics problems, fuzzy set theory as an alternate model of uncertainty, and neural networks.

Ihab W. Saad
Department of Electrical Engineering
Texas Tech University
Lubbock, TX 79409

Ihab W. Saad was [redacted] He received his BS in Electrical Engineering from Ain Shams University, Cairo, Egypt, in 1993. He has recently completed an MS in Electrical Engineering from Texas Tech University.

Donald Wunsch
Department of Electrical Engineering
Texas Tech University
Lubbock, TX 79409

Donald Wunsch (Senior Member, 94) received a Ph.D. in Electrical Engineering and a M.S. in Applied Mathematics from the University of Washington in 1991 and 1987, a B.S. in Applied Mathematics from the University of New Mexico in 1984, and completed a Humanities Honors Program at Seattle University in 1981. He is Director of the Applied Computational Intelligence Laboratory at Texas Tech University. Prior to joining Tech in 1993, he was Senior Principal Scientist at Boeing, where he invented the first optical implementation of the ART1 neural and other optical neural networks and applied research contributions. He has also worked for International Laser Systems and Rockwell International. Current research activities include neural optimization, forecasting and control, financial engineering, fuzzy risk assessment for high-consequence surety, wind engineering, characterization of the cotton manufacturing process, intelligent agents, and Go. He is an Academician in the International Academy of Technological Cybernetics, and in the International Informatization. He is a member of the International Neural Network Society and a past member of the IEEE Neural Network Council.

Superfund Site Risk Assessments Using Uncertainty Propagation

Peter T. Katsumata
Booz·Allen & Hamilton, Inc.
Los Angeles, California

Abstract

Health risk assessments at Superfund Sites are based on the United States Environmental Protection Agency's (EPA) *Risk Assessment Guidance for Superfund* (RAGS). The methodology outlined in RAGS uses "default" values in the exposure models that result in conservative point estimates of risk. This procedure introduces major limitations due to the inherent uncertainty and variability in many of the exposure model parameters.

Computer software developments in uncertainty propagation have aided in the assessment of these uncertainties. These software packages allow the user to assign uncertainty distributions to the parameters in the models, thus eliminating the need to choose a single "default" point estimate. These uncertainty distributions can then be propagated through the risk calculations resulting in a distribution of risk. This risk distribution represents the risk and its associated uncertainty.

To illustrate the value of this method, it is applied to a Superfund Site which has been assigned a Record of Decision (ROD) and utilizes the current EPA point estimate (deterministic) approach and the so-called "default" values. These risk values are compared to the results of the uncertainty propagation (probabilistic) approach. The health risk assessments utilizing the deterministic approach were found to predict risks that were much larger than the 90th percentile of the probabilistic approach.

Introduction

The United States Environmental Protection Agency (EPA) currently performs risk assessments in support of the decision-making process regarding remedy selection for sites on the National Priority List, the so-called Superfund Sites. Because of uncertainty in risk assessment models and data, the US EPA uses a conservative approach that can exaggerate typical risk estimates and can lead to the selection of very costly, resource-intensive, and time-consuming remedies. This paper examines the use of more realistic state-of-the-art methods and currently available data to reassess the risks and their uncertainties at a Superfund Site.

In assessing the potential human health risks associated with exposure to environmental contaminants, the US EPA originally recommended considering only a "reasonable maximum exposure" (RME) (US EPA, 1989), defined as the "highest exposure that is reasonably expected to occur." In practice the RME is a conservative estimate, calculated by assuming and combining a series of conservative and worst-case parameters in the US EPA exposure models, as well as selecting conservative values for the environmental contaminant concentrations. In so doing, the applicability of the calculated risk, which is sometimes called a "point estimate," and the confidence one has regarding this point estimate, becomes questionable for decision making. The RME approach, as well as other point estimate approaches, has several major limitations due to the inherent parameter uncertainties in the exposure models, including the environmental contaminant concentrations. The inherent uncertainties in cancer potency factors and reference doses also contribute to uncertainty in risk. In general, these uncertainties can result from natural variability of site-specific and temporal parameters, measurement and extrapolation errors, and/or the inherent lack of knowledge regarding biological, chemical, and physical processes.

The advent of inexpensive computing has facilitated convenient adaptation of uncertainty propagation in risk assessment. Commercially available computer programs such as Crystal Ball® and @Risk® enable the user to represent uncertain variables using probability distributions and to propagate uncertainty throughout the risk assessment models. In addition to characterizing the uncertainty in the risk, the resulting risk distribution can be used to estimate the mean, median, and other percentile risks. Using these values, a more informed decision regarding remedy selection can be made. In this paper, a Monte Carlo based set of simulations is presented for a wood and paper processing plant in California. The results are compared to the US EPA estimates of risk contained in the Record of Decision (ROD) for the site.

Methodology

Introduction

As noted above, state-of-the-art methods and inexpensive computing have allowed the possibility of propagating uncertainty through the risk assessment process. There are two general classifications for uncertainty, model uncertainty and data (or parameter) uncertainty. In this paper, no new exposure or dose/response models were developed. Rather, the paper is focused on new methods for dealing with parameter uncertainty and variability.

For the site considered in this paper, measured contaminant concentrations were available and employed by the US EPA. The use of measured contaminant concentrations is an attempt to capture the existing risk without regard to natural dilution or degradation processes. The analyses presented in this paper use these measured contaminant concentrations in conjunction with US EPA developed exposure and dose/response models. Conservative parameter-value selection for these exposure and dose/response models is the primary contributor to over-conservativeness, and thus inadequacy, in the US EPA approach.

To address the inadequacies of the current US EPA approach to risk assessment, the uncertainties and variabilities in the exposure parameters are first evaluated. Parameter uncertainty accounts for the inherent lack of knowledge as well as measurement and extrapolation errors. Parameter variability accounts for the natural variability of site-specific and temporal parameters as well as human physiological behavior. After determining which parameters require reassessment, the corresponding uncertainties and variabilities are quantified. The most effective quantification method is to assign each parameter a cumulative probability distribution function or a probability density function. These distribution or density functions can take several different forms (e.g., normal, log-normal, uniform, triangular, and so on). The determination of which form of distribution function to assign to each parameter depends on both site-specific data and judgment based on statistical analysis. The distributions used in this project are assembled from site-specific data, existing data in the most current literature, and professional judgment, and are considered to be the most up-to-date description of the parameter.

After characterizing the uncertainty and/or variability associated with each parameter, the uncertainty in the risk can be estimated. For the risk assessments presented in this paper, the commercially available software package called Crystal Ball® (Version 3.0.1, January 1994, Decisioneering Corporation, Denver, CO) is used. Crystal Ball® propagates the uncertainty and variability of the parameters throughout the calculation of the risk. This propagation results in a distribution function for the risk.

Crystal Ball® uses a Monte Carlo (MC) simulation to propagate the distributions. The MC method is commonly used because of its simplicity, general applicability, and asymptotic exactness (Salhotra et al., 1990). The MC simulation calculates the risk several thousand times by drawing parameter values randomly from the distribution functions. Each value of risk has a corresponding probability. Certain values within each distribution function will be drawn more frequently due to their higher likelihood. Others will be drawn less frequently. The end result is a distribution of the risk with corresponding probabilities.

Exposure

In calculating the lifetime average daily dose (LADD) an individual receives from a particular chemical, the basic equations were taken from EPA's Risk Assessment Guidance for Superfund (US EPA, 1989). As an example, the equation for the LADD from soil ingestion is:

$$LADD(mg/kg-day)=\frac{CS\times IR\times CF\times FI\times EF\times ED}{BW\times AT} \qquad \text{(Eq. 1)}$$

where,

CS = Chemical concentration in soil (mg/kg)
IR = Ingestion rate (mg soil/day)
CF = Conversion factor (1×10^{-6} kg/mg)

FI = Fraction ingested from contaminated source (unitless)
EF = Exposure frequency (days/year)
ED = Exposure duration (years)
BW = Body weight (kg)
AT = Averaging time (days)

The parameter values used by the US EPA in the Record of Decision (ROD) will differ from those used in this paper for the MC analysis. The parameter distributions will also differ from workers to residents, as well as from adults to children.

The incremental lifetime risk (ILR) is obtained from the LADD. The LADD is multiplied by an appropriate risk slope factor. For carcinogens the slope factor is the cancer potency factor (CPF). Hence, the incremental lifetime cancer risk (ILCR) is given by:

$$ILCR = LADD \times CPF \qquad \text{(Eq. 2)}$$

Procedure

In reassessing the site, the chemical contaminants of interest were first selected. Only carcinogens were examined in this paper. The exposure pathways and receptor groups evaluated in the original risk assessment were chosen to be reassessed in order to facilitate a fair comparison of risks. The toxicity criteria for each chemical contaminant of concern were then selected, which was the CPF for carcinogens.

The parameters used in calculating the possible exposure to the chemical contaminants of concern were then evaluated. Uncertainty distributions were assigned to the parameters, where possible, using the most up-to-date and applicable data found in the literature. These distributions were then used in conjunction with Crystal Ball® and the exposure equations to run MC simulations. The resulting risk distributions were used to extract risk percentiles, which were then compared to US EPA point estimate risks.

The Baxter/International Paper/Roseburg Site

Background

The Superfund Site evaluated was the J.H. Baxter/International Paper/Roseburg Forest Products (B/IP/R) Superfund Site in Weed, California. The site is comprised of properties currently owned by J.H. Baxter and Company and Roseburg Forest Products. The International Paper Company and predecessor companies previously owned it. These properties have historically been used for lumber product manufacturing and wood treatment operations. Currently, a wood treatment facility owned by J.H. Baxter and Company, and a lumber and veneer mill owned by Roseburg Forest Products occupy the site.

The US EPA's Remedial Investigation (RI) determined that the environmental media affected were air, soils, surface water, and groundwater. The primary contaminants of concern were found to be arsenic, carcinogenic polycyclic aromatic hydrocarbons (PAHs), pentachlorophenol, and polychlorinated dibenzo dioxins and furans (PCDD/PCDF). All of these contaminants were detected at concentrations exceeding State of California, Department of Health Services standards in at least one environmental medium. Contaminants of lesser concern were found to be chromium, copper, zinc, benzene, and noncarcinogenic PAHs. These contaminants were either detected at concentrations below health standards, not as widespread, or considered to be less toxic than the primary contaminants of concern. For current-use conditions, where present activities were assumed to continue, the populations at risk were considered to be workers at the site and residents living in the surrounding area. The routes of exposure considered for workers at the J.H. Baxter facility and the Roseburg Forest Products facility were direct contact with soil and inhalation of fugitive dust. For children living in the surrounding area, direct contact with soil, surface water, and sediments were considered as the exposure routes. For adults living in the area, inhalation of fugitive dust was considered the primary exposure route.

For evaluation of future-use conditions, land-use at the site was assumed by the US EPA to be residential. In this case, the population at risk was considered to be residents living at the site. The routes of exposure considered for residential children at the J.H. Baxter site and at the Roseburg Forest Products site were direct contact with soil, ingestion of groundwater, inhalation of volatiles released from groundwater, and direct contact with sediments. The routes of exposure considered for residential adults at the J.H. Baxter and Roseburg Forest Products sites were direct contact with soil, ingestion of groundwater, and inhalation of volatiles released from groundwater. For each exposure scenario, both an average and maximum plausible exposure were assessed (US EPA, 1990b).

Baseline Risk

Overview

In the US EPA risk assessment, two cases were evaluated: continued industrial use of the property and future-use residential. The exposure routes mentioned in the previous section were assessed. Since future-use conditions were an important consideration in remedy selection, both scenarios are considered in this paper. And although the future-use conditions may be considered unrealistic, it is important that they be assessed since the clean-up criteria were determined mainly from the future-use scenario risks. Hence, baseline risks are determined for current-use and future-use conditions.

The baseline risks reported in the ROD were represented by the use of an average case and a maximum plausible case. The US EPA average case is reproduced in this paper using the arithmetic mean for the contaminant concentration. The maximum plausible case used the maximum concentration as the exposure point concentration in a data set, along with exaggerated exposure assumptions. This case is unlikely to apply to any segment of the exposed population. US EPA currently recommends the use of the 95% upper confidence limit on the arithmetic average concentration that is contacted over the exposure period to represent an upper-bound of exposure that is more likely to occur (ChemRisk, 1990).

The evaluation of risks due to PAH exposure by the US EPA may have been inappropriate in that the concept of toxic equivalency factors (TEF) was not utilized. The use of TEF's is currently specified by the US EPA as an interim policy (US EPA, 1993), as a way of averaging PAHs, yet this was not done in this case. For the US EPA risk assessment, all carcinogenic PAHs were assumed to be toxicologically equivalent to benzo(a)pyrene, which is the most toxic of the PAHs. Hence, the approach taken in this regard, leads to very conservative results.

In order to refine the US EPA's original results and estimate their uncertainty, the baseline risks were reassessed using distribution functions for certain exposure parameters and implementing MC simulations using Crystal Ball®. In the reassessment, both the current-use and future-use scenarios were evaluated. The US EPA average risks were calculated using an arithmetic mean for the environmental contaminant concentration, while keeping all other parameters unchanged. These results will facilitate a fair comparison with the MC results.

To address the exposure point concentrations, the environmental contaminant concentration data sets were reevaluated and their means were represented as normal distributions to reflect sampling uncertainty. However, in reevaluating the data sets, the original values used by the US EPA could not be reproduced in most cases. This is attributed to arithmetic and mathematical errors, failure to incorporate unit conversions appropriately, and transcription errors in the US EPA assessment. Also, it was unclear as to which data sets were used by the US EPA (ChemRisk, 1990). In reevaluating the exposure point concentrations for carcinogenic PAHs, the TEF methodology was applied.

Current-Use Conditions

The results of the baseline risk assessments for the workers and residents living in the area for current-use conditions are shown in Tables 1 through 4. The US EPA results are represented in the first two columns. The first column labeled "EPA (arith. mean)" lists the risk values recalculated using an arithmetic mean for the environmental contaminant concentration. All other parameter values were unchanged. The second column labeled "EPA (maximum)" lists the risk values actually reported in the ROD as the maximum plausible. The MC risk distributions are reported in the last two columns for the mean and 90th percentile.

Tables 1 and 2 show the worker's baseline risk results for each media of concern as well as the total risks for the J.H. Baxter facility and the Roseburg Forest Products facility, respectively. The results indicate that the air exposure route dominates the risk. The soil exposure pathway risk is dominated by arsenic at the J.H. Baxter facility and by cPAH at

Table 1. US EPA and MC Baseline Risks for Workers at the J.H. Baxter Facility by Exposure Route (Current-Use Conditions)

	EPA (arith. mean)	EPA (maximum)	MC Mean	MC 90^{th} %
Soil	1.8×10^{-4}	7.6×10^{-2}	1.7×10^{-5}	3.9×10^{-5}
Air	1.6×10^{-4}	5.8×10^{-2}	2.9×10^{-4}	7.6×10^{-4}
Total	3.4×10^{-4}	1.3×10^{-1}	3.1×10^{-4}	8.1×10^{-4}

Table 2. US EPA and MC Baseline Risks for Workers at the Roseburg Forest Products Facility by Exposure Route (Current-Use Conditions)

	EPA (arith. mean)	EPA (maximum)	MC Mean	MC 90^{th} %
Soil	7.1×10^{-6}	4.8×10^{-3}	5.2×10^{-7}	1.3×10^{-6}
Air	1.6×10^{-4}	5.8×10^{-2}	2.9×10^{-4}	7.6×10^{-4}
Total	1.7×10^{-4}	6.3×10^{-2}	3.1×10^{-4}	8.0×10^{-4}

the Roseburg Forest Products facility. The inhalation exposure risk is dominated by arsenic at the BIPR site (i.e., at both facilities).

Table 3 shows the residential children's baseline risk results for each media of concern and the total risks. Table 4 shows the residential adult's baseline risk results. For children, the risk is dominated by exposure to arsenic via the soil and surface water exposure routes. For adults, the risk is dominated by inhalation of arsenic.

Table 3. US EPA and MC Baseline Risks for Residential Children Living in the Area by Exposure Route (Current-Use Conditions)

	EPA (arith mean)	EPA (maximum)	MC Mean	MC 90^{th} %
Soil:				
Angel Valley Subdivision	1.2×10^{-5}	5.6×10^{-5}†	6.9×10^{-7}	1.5×10^{-6}
Lincoln Park	1.5×10^{-5}	2.8×10^{-4}‡	9.0×10^{-7}	1.9×10^{-6}
Sediment	5.0×10^{-8}	1.7×10^{-6}	4.0×10^{-9}	9.0×10^{-9}
Surface Water	7.0×10^{-7}	7.7×10^{-6}	6.6×10^{-7}	1.2×10^{-6}
Total	2.8×10^{-5}	3.5×10^{-4}	2.3×10^{-6}	4.1×10^{-6}

†This risk reported by US EPA is incorrect. It should be 4.6×10^{-5}.
‡This risk reported by US EPA is incorrect. It should be 2.2×10^{-4}.
These two corrections drive the total down to 2.8×10^{-4}.

Table 4. US EPA and MC Baseline Risks for Residential Adults from Inhalation of Fugitive Dust (Current-Use Conditions)

	EPA (arith. mean)	EPA (maximum)	MC Mean	MC 90th %
Liberty Avenue	2.0×10^{-5}	5.9×10^{-3}	6.2×10^{-6}	1.6×10^{-5}
Union Street	9.6×10^{-5}	2.4×10^{-2}	2.9×10^{-5}	7.2×10^{-5}

Figure 1 shows the 10th, 90th, mean and median values of the MC risk distributions for the total risk to each population. These values are shown to portray the representative spread in the MC risk distributions.

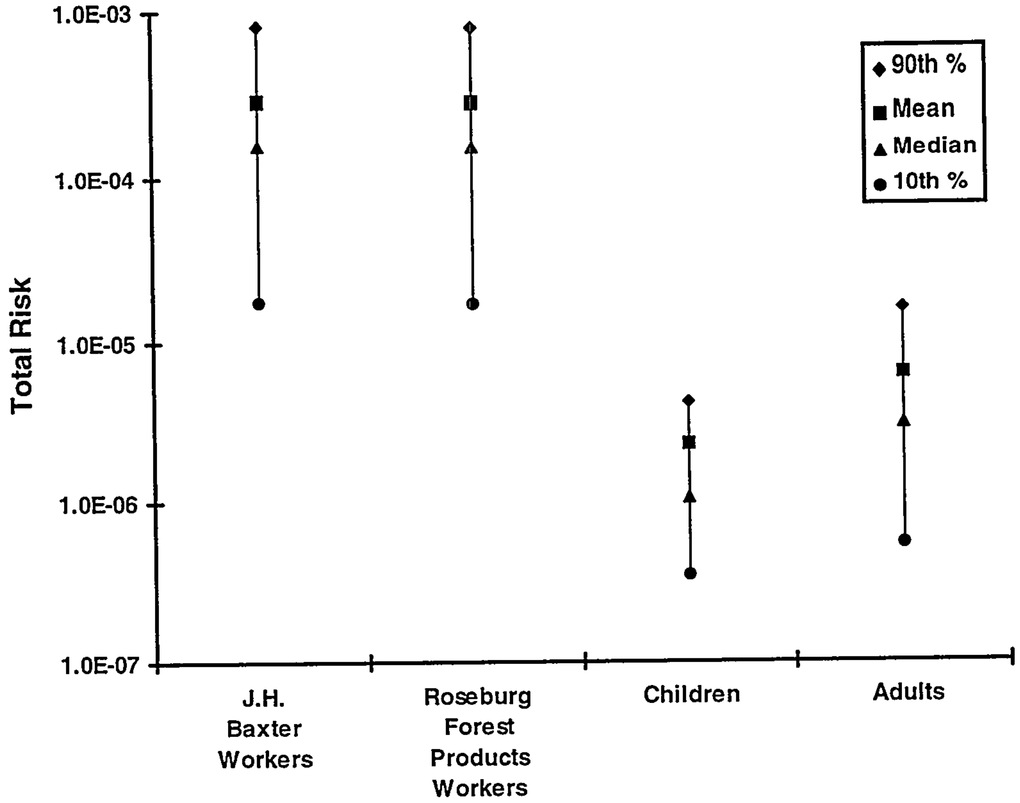


Figure 1. Total risk distributions for all populations at risk (current-use conditions).

Future-Use Conditions

The results of the baseline risk assessments for residents living at the site for future-use conditions are shown in Tables 5 through 8. These tables have a similar format to those of Tables 1 through 4. The columns labeled "Air" in Tables 5 through 8 represent the

Table 5. US EPA and MC Baseline Risks for Residential Children at the J.H. Baxter Facility by Exposure Route (Future-Use Conditions)

	EPA (arith. mean)	EPA (maximum)	MC Mean	MC 90th %
Soil	3.2×10^{-3}	1.2×10^{-1}	1.1×10^{V4}	2.1×10^{-4}
Groundwater	2.0×10^{-2}	$5.0 \times 10^{-1‡}$	3.5×10^{-3}	6.4×10^{-3}
Air	1.0×10^{-2}	$2.9 \times 10^{-1*}$	1.5×10^{-3}	2.8×10^{-3}
Sediments	2.4×10^{-6}	1.1×10^{-4}	1.7×10^{-7}	4.1×10^{-7}
Total	3.3×10^{-2}	9.1×10^{-1}	5.1×10^{-3}	9.4×10^{-3}

‡This risk reported by US EPA is incorrect. It should be 6.8×10^{-1}.
*This risk reported by US EPA is incorrect. It should be 3.5×10^{-1}. These drive the total up to 1.1.

Table 6. US EPA and MC Baseline Risks for Residential Children at the Roseburg Forest Products Facility by Exposure Route (Future-Use Conditions)

	EPA (arith. mean)	EPA (maximum)	MC Mean	MC 90th %
Soil	9.5×10^{-5}	5.9×10^{-3}	2.0×10^{-6}	4.0×10^{-6}
Groundwater	2.0×10^{-2}	$5.0 \times 10^{-1‡}$	3.5×10^{-3}	6.4×10^{-3}
Air	1.0×10^{-2}	$2.9 \times 10^{-1*}$	1.5×10^{-3}	2.8×10^{-3}
Sediments	2.4×10^{-6}	1.1×10^{-4}	1.7×10^{-7}	4.1×10^{-7}
Total	3.0×10^{-2}	8.0×10^{-1}	5.0×10^{-3}	9.3×10^{-3}

‡This risk reported by US EPA is incorrect. It should be 6.8×10^{-1}.
*This risk reported by US EPA is incorrect. It should be 3.5×10^{-1}. These drive the total up to 1.0.

Table 7. US EPA and MC Baseline Risks for Residential Adults at the J.H. Baxter Facility by Exposure Route (Future-Use Conditions)

	EPA (arith. mean)	EPA (maximum)	MC Mean	MC 90th %
Soil	2.3×10^{-4}	5.7×10^{-2}	1.5×10^{-5}	2.9×10^{-5}
Groundwater	2.6×10^{-2}	8.0×10^{-1}‡	1.8×10^{-3}	4.4×10^{-3}
Air	1.3×10^{-2}	5.3×10^{-1}*	7.7×10^{-4}	1.9×10^{-3}
Total	3.9×10^{-2}	1.4	2.6×10^{-3}	6.5×10^{-3}

‡This risk reported by US EPA is incorrect. It should be 1.5.
*This risk reported by US EPA is incorrect. It should be 7.5×10^{-1}. These drive the total up to 2.3.

Table 8. US EPA and MC Baseline Risks for Residential Adults at the Roseburg Forest Products Facility by Exposure Route (Future-Use Conditions)

	EPA (arith. mean)	EPA (maximum)	MC Mean	MC 90th %
Soil	8.9×10^{-6}	3.6×10^{-3}	3.4×10^{-7}	8.2×10^{-7}
Groundwater	2.6×10^{-2}	8.0×10^{-1}‡	1.8×10^{-3}	4.4×10^{-3}
Air	1.3×10^{-2}	5.3×10^{-1}*	7.7×10^{-4}	1.9×10^{-3}
Total	3.9×10^{-2}	1.3	2.6×10^{-3}	6.5×10^{-3}

‡This risk reported by US EPA is incorrect. It should be 1.5.
*This risk reported by US EPA is incorrect. It should be 7.5×10^{-1}. These drive the total up to 2.3.

exposure due to the inhalation of contaminants due to volatilization from groundwater. Tables 5 and 6 show the residential children's baseline risk results for each medium of concern and the total risks for the J.H. Baxter facility and the Roseburg Forest Products facility, respectively. At both facilities, the major exposure routes are groundwater ingestion and air (inhalation), with groundwater ingestion dominating the risk. The groundwater ingestion risk is dominated by exposure to cPAHs. Direct contact with arsenic contaminated soil poses the next highest risk.

Tables 7 and 8 show the residential adult's baseline risk results for each media of concern as well as the total risks for the J.H. Baxter facility and the Roseburg Forest Products facility, respectively. In this case, the major exposure routes are also groundwater and air, with the groundwater pathway dominant. The principle contaminant is cPAH for both exposure routes.

Figure 2 shows the 10th, 90th, mean and median values of the MC risk distributions for the total risk to each population. These values are shown to portray the representative spread in the MC risk distributions. Note that the spread for each site appears identical because the risks are dominated by cPAH contaminated groundwater ingestion and volatile release from groundwater, and the source is identical for each site.

In reassessing the baseline risks for the current- and future-use conditions, two main issues have emerged: 1) use of point estimates versus MC analyses, and 2) characterization of future-use conditions. These issues are discussed in a later section of the paper.

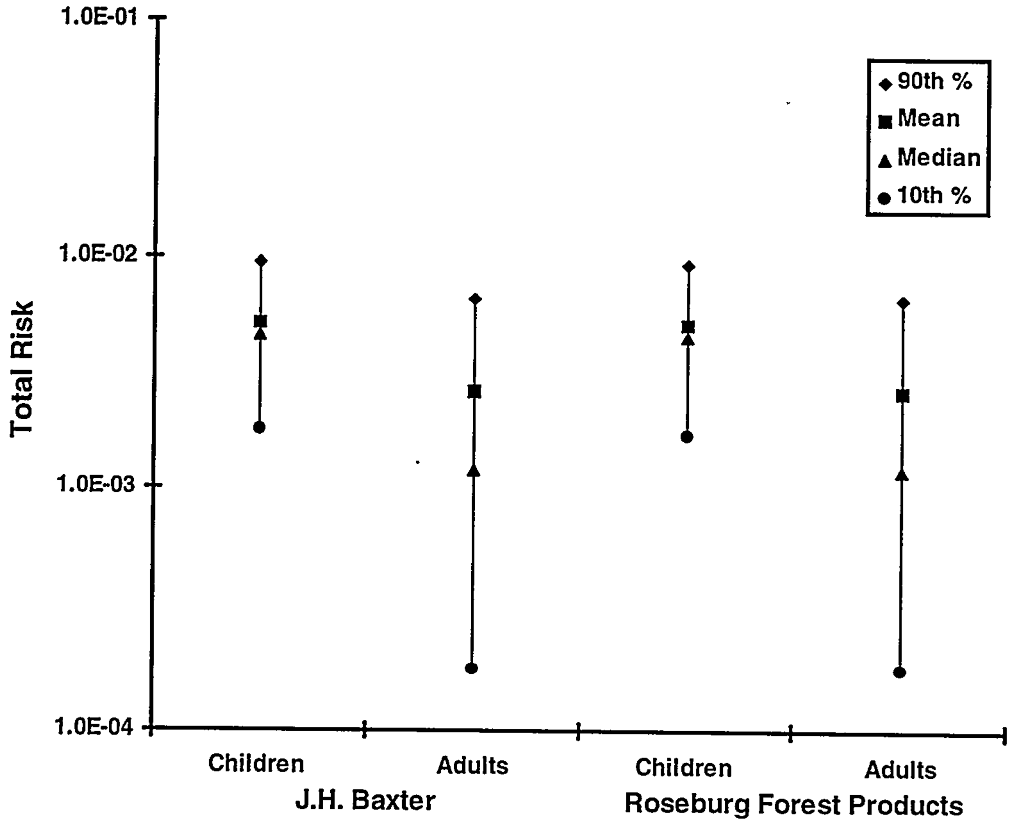


Figure 2. Total risk distributions for all populations (future-use conditions).

Discussion

Point Risks Versus Monte Carlo (MC) Risks

Since the MC risk distributions utilize the arithmetic mean, it is appropriate to compare the MC Mean risks to the US EPA risks calculated using the arithmetic mean. The tables show that the MC Mean risks are lower than the point estimate risks that use the arithmetic mean in all but one case: risks for the air exposure pathway for workers were slightly higher for the MC analysis than the point estimate analysis. Further comparison of the methodologies reveals that two of the distributions used to represent the exposure parameters for the air pathway yield much higher values than their point estimate counterparts because of the large uncertainty. In other words, it was more likely that a value larger than the US EPA point estimate would be sampled in the MC analysis. In general, however, the MC methodology results in lower risk values. In approximately half of the cases, the difference is greater than one order of magnitude. The largest difference exists in Table 6 for the future-use conditions of residential children at the Roseburg Forest Products facility from the soil exposure pathway. The point estimate risk using the arithmetic mean is approximately 50 times greater than the MC Mean risk. In some cases, even the MC 90th percentile is lower than the point estimate risk using the arithmetic mean (e.g., the air and groundwater pathways for residential children under future-use conditions).

For the MC risk distributions, the 90th percentile can be considered a reasonable maximum. Hence these values can be compared to what the US EPA considered the "plausible maximum." The tables show that the MC 90th percentile risks are generally much lower than the US EPA's plausible maximum risks. In approximately half of the cases, the difference is greater than two orders of magnitude. The largest difference exists for the future-use conditions of residential adults at the Roseburg Forest Products facility from the soil exposure pathway. The US EPA plausible maximum value is approximately 4400 times greater than the MC 90th percentile risk.

The total risks, which were not directly assessed by the US EPA, are shown in each of the tables for each population. In all but one case, the MC mean total risks are lower than the point estimate total risks that use an arithmetic mean. Once again, the case in which the MC risk was higher was for the air exposure pathway for workers. However, the MC 90th percentile total risks are seen to be much lower than the US EPA plausible maximum total risks for all cases. These comparisons show the effect on risk estimates of using "best estimate" distribution functions to describe exposure parameters, rather than the US EPA default values.

Future Use

As can be seen in Tables 1 through 8, the risks from the future-use residential conditions (unremediated) are much higher than those from the current-use industrial conditions. The MC results for the continued industrial-use scenario (unremediated) show total risks in the range of 3×10^{-4} to 8×10^{-4} for workers and 2×10^{-6} to 7×10^{-5} for nearby residents. For the residential future use scenario, the risks (unremediated) are in the range 2×10^{-3} to 9×10^{-3}. (In each instance, the upper value is the 90th percentile MC risk). The future-use conditions are very important in this assessment in that they are the driving force behind many of the clean-up criteria. In addition, the clean-up standards for residential areas are much more stringent than those for industrial areas.

Summary and Conclusions

This paper contains the results of a reassessment of the risks for the Baxter/International Paper/Roseburg Site in Weed, California. This reassessment is based upon the use of more realistic state-of-the-art models and currently available data than originally employed in the US EPA Record of Decision (ROD). The exposure parameters are treated as distributions to account for uncertainty and variability in the data. Monte Carlo (MC) methods are used to propagate these distributions to obtain a distribution for the risk.

As a result of the review and reassessment of the risk assessments performed for the B/IP/R Superfund Site, the following can be concluded:

1. There were a small number of significant errors made by the US EPA in calculating the baseline risks. These errors included the assumption that all the carcinogenic polycyclic aromatic hydrocarbons (cPAHs) are toxicologically equivalent to benzo(a)pyrene (BaP), which is the most toxic, rather than using the concept of Toxic Equivalency Factors (TEFs).

2. For the current-use conditions (industrial unremediated) the risk to workers is dominated by arsenic contaminated soil exposure and the risk to the nearby residents is dominated by arsenic as well; however, for adults the dominant exposure pathway is inhalation of contaminated air, and for children it is both contaminated soil and contaminated air.

3. For the future-use, unremediated residential case, the risks were dominated by cPAH ingestion through the groundwater; for both the US EPA risk assessment and the present study.

4. In most cases where comparisons were made, the MC mean risks were approximately 10 to 50 times less than the US EPA point estimate risks based on the arithmetic mean. In the case of groundwater ingestion for the future-use conditions (unremediated) of residential children, even the MC 90th percentile risks were lower than the US EPA point estimate risks using the arithmetic mean.

5. The US EPA repeatedly referred to the "plausible maximum" risks in the ROD in their characterization of the risks for each media and in conjunction with remedy selection. For the MC analysis, the 90th percentile can be considered a reasonable upper bound or maximum. The US EPA "plausible maximum" risks were found to be approximately 10 to 4400 times greater than the MC 90th percentile risks. In approximately half the cases, the difference was greater than 100.

Acknowledgements

This work was performed under the direction of Professor William E. Kastenberg while attending the University of California, Los Angeles. His contributions are greatly appreciated.

We thank David Crawford, Carol Gillis, and Natalie Harrington of ChemRisk, Portland, Maine, and Kevin Holtzclaw of the General Electric Company, Fairfield, Connecticut, for providing us with data and for their assistance in the reassessment. This work received funding from the Business Roundtable.

References

ChemRisk 1990, Technical Review of the USEPA Region IX Endangerment Assessment for the J.H. Baxter/International Paper/Roseburg Forest Products (BIPR) Superfund Site, Weed, California (EPA WA 205-9L74 April 30, 1990).

Salhotra, A.M., Y.J. Meeks, R.Thorpe, T. McKone, and K. Bogen, 1990, "Application of Monte Carlo Simulation to Estimate Probabilities of Exposure and Human Health Risks," A report by Woodward-Clyde, Seattle, Washington.

United States Environmental Protection Agency (US EPA) 1989, *Risk Assessment Guidance for Superfund, Volume 1, Human Health Evaluation Manual Part A*, EPA/540/1-8a/002, Office of Emergency and Remedial Response, Washington, DC.

United States Environmental Protection Agency (US EPA) 1989b, *Exposure Factors Handbook*, EPA/600/8-89/043, Office of Health and Environmental Assessment, Washington, DC.

United States Environmental Protection Agency (US EPA) 1990a, Remedial Investigation Report for the J.H. Baxter/International Paper/Roseburg Forest Products (B/IP/R) Superfund Site, Weed, California, prepared by Camp, Dresser, and McKee, San Francisco, CA for US EPA Region IX.

United States Environmental Protection Agency (US EPA) 1990b, Record of Decision for J.H. Baxter/International Paper/Roseburg Forest Products (B/IP/R) Superfund Site.

United States Environmental Protection Agency (US EPA) 1993, Provisional Guidance for Quantitative Risk Assessment of Polycyclic Aromatic Hydrocarbons.

Biography

Peter T. Katsumata, Ph.D.
Booz·Allen & Hamilton Inc.
523 West Sixth Street, Suite 650
Los Angeles, CA 90014 USA

Dr. Katsumata is a Senior Consultant with Booz·Allen & Hamilton, Inc., Transportation Safety Group. His Ph.D. in mechanical engineering is from the University of California, Los Angeles. He has over five years of engineering research experience in risk analysis and management, cost/risk benefit analysis, and decision analysis. He has several publications in the risk analysis field.

Intentionally left blank

A First-Principle Based Approach to Quantitative Assessment of Nuclear-Detonation Safety

Dr. Paul N. Demmie
Sandia National Laboratories*
Albuquerque, New Mexico

Abstract

Surety of nuclear weapons has high national importance because of the extreme consequences associated with nuclear weapon explosions or plutonium dispersal and the critical need to assure and preserve the high quality and reliability of the nation's nuclear deterrent. Nuclear-detonation safety is one element of the surety of nuclear weapons.

Nuclear weapons are designed to be passively safe systems that must remain in a safe state regardless of external threats and produce a nuclear yield only when intended and authorized by competent authorities. In this paper, I discuss an approach to quantitative assessment of nuclear-detonation safety using a method called the Direct Quantification Method (DQM).

DQM is a synergism of the required design basis of nuclear weapons and fault-tree analysis. Not only does this paper discuss DQM, but it also illustrates its application to a quantitative assessment of Firing System Assembly (FSA) failure and compliance with the Military Characteristics (MCs) for a nuclear weapon. While the description and illustration focus on nuclear-detonation safety, the method is more general and can be applied to systems other than nuclear weapons.

Introduction to Nuclear Weapon Safety

The purpose of this paper is to present an approach for performing quantitative safety assessments, called this the Direct Quantification Method (DQM). DQM was developed to perform quantitative assessments of nuclear-detonation safety and prototyped on an application to the W78 warhead [1]. However, DQM is more generally applicable. I expect that it is particularly useful for assessing passive safety systems or systems where limited data but identifiable first-principle predictability of subsystems or components.

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

Since readers may not be familiar with the philosophy of nuclear weapon safety, I begin with an introduction to nuclear weapon safety. It is national policy that,

Nuclear weapon safety be designed into nuclear weapons on a first-principle basis to provide safety in a predictable manner when subjected to normal and abnormal environments [2].

First principles are the fundamental laws of nature or physics underlying the working of a designed or engineered device or the fundamental characteristics inherent in the physics and/or chemistry of a material that provide a predictable response in a component or assembly when subjected to specified stimuli [3]. Normal environments are environments in which the warhead is designed to retain operational reliability. Such environments include those resulting from weapon shipment, storage, maintenance, handling, and military exercises [3]. Abnormal environments are environments in which the warhead is not designed to retain full operational reliability. Abnormal environments result from both single threats and combinations of threats. They can result from a nuclear warhead accident, incident, or inadvertent action [3].

It is generally accepted that a first-principle design basis was adopted since (1) it is unlikely that enough testing can be performed to assert that a nuclear weapon is safe in all environments and (2) a nuclear weapon must remain in a safe state regardless of its external environment. A nuclear weapon must produce a nuclear yield only when intended and authorized by competent authorities.

The national expectations for nuclear-detonation safety are stated in qualitative nuclear-safety standards and quantitative criteria specified in the MCs for a nuclear weapon. These expectations for a nuclear weapon prior to its intended use are stated in the following table:

The National Expectations for Nuclear-Detonation Safety

- General
  - Nuclear safety has first priority.
  - Components critical to safety will be designed to be predictably safe.
- Warhead
  - Likelihood that one-point detonation at any point of weapon explosive will produce a nuclear yield more than 4 pounds equivalent TNT yield will be less than one in a million.
  - In normal environments, likelihood of premature nuclear detonation will be less than one in a billion per weapon lifetime.
  - In accident environments, likelihood of premature nuclear detonation will be less than one in a million per accident.

- Weapon System
  - In normal environments, likelihood of premature application of enabling stimuli and arming signals will be less than one in a billion per lifetime.
  - In accident environments, likelihood of premature application of enabling stimuli will be less than one in a million per accident.

The remainder of this paper is separated into the following sections:

A Problem
A General Solution
Our Solution
The Direct Quantification Method (DQM)
Value Added by Using the Direct Quantification Method
Concluding Remarks

Several sections include results from reference [1] to illustrate the methodology.

A Problem

The primary goal of nuclear-safety assessment is,

> To identify and understand any design vulnerabilities that could cause existing nuclear safety standards, criteria or design-specific requirements not to be met [2].

Traditional assessment methods used to achieve this goal for nuclear-detonation safety have difficulty determining if quantitative safety goals are met by a weapon system. Although they are very good at identifying soft spots or vulnerabilities in the design or implementation, they are not very good at quantifying and understanding the impact of soft spots or vulnerabilities on system safety performance in normal and abnormal (accident) environments.

A General Solution

A general solution to the main problem in traditional assessment methods would be to develop quantitative assessment methods based on first principles to complement the traditional methods. Such methods would support the primary goal of nuclear safety assessment and complement traditional methods. Since the methods are quantitative, they can be used to determine if quantitative goals or requirements are met. Since they are first-principle based, they can be effective in understanding safety performance and in identifying design vulnerabilities, and understanding how these vulnerabilities result in not meeting safety goals.

Our Solution

The solution introduced in this paper is DQM. DQM is both quantitative and first-principle based. It complements traditional assessment methods by aiding understanding of safety performance; identifying vulnerabilities, potential positive measures, and useful testing; and prioritizing modifications to a weapon. DQM was prototyped on an assessment of nuclear-detonation safety of the W78 warhead [1]. For an accident scenario, the results produced by DQM are undesired-event probabilities in environments occurring during the scenario and the probability that the undesired event occurs during the scenario.

Since I will illustrate DQM with an application to nuclear-detonation safety and the reader may not be familiar with methods used to design safe nuclear weapons, I provide enough information here to understand the application. Figure 1 depicts a generic Firing System Assembly (FSA) for a nuclear weapon in enough detail for this discussion of FSA failure. When nuclear detonation is intended, the FSA receives proper arming and fuzing and initiates the detonators for the nuclear explosive package (NEP) upon receiving a firing signal. The FSA is designed to prevent unintended electrical energy from initiating the detonators. FSA failure occurs when the FSA does not prevent unintended electrical energy from initiating the detonators.

The Unique Signal Switch (UQS) and Environmental Sensing Device (ESD) are called stronglinks in the safety theme that describes the design philosophy used to achieve nuclear-detonation safety. The LAC and stronglinks control electrical energy entering the FSA. An exclusion-region barrier prevents electrical energy from entering the FSA elsewhere. All components critical to nuclear detonation, except the NEP detonators, are inside the exclusion region. The thermal weaklink in the safety theme is the Fireset. For the FSA to fail during an accident, it must continue to survive in an operable state. The safety theme, simply stated, is that in any accident environment, the stronglinks, LAC, and exclusion-region barrier prevent inadvertent electrical energy applied to the weapon from initiating the NEP detonators until the weaklink becomes irreversibly inoperable.

Figure 1 shows electrical energy applied to all circuits entering the FSA through the Lightning Arrestor Connector (LAC). For the FSA to fail, energy applied and transferred across the LAC must be transferred across the Unique Signal Switch (UQS). There are five mechanisms in the system model for transferring electrical energy across the UQS — UQS was installed enabled, UQS has electrical breakdown as a result of environment, UQS is enabled by environment, UQS is electrically bypassed, or Environmental Sensing Signal Generator (ESSG) enables the UQS.

Electrical energy applied to the ESD must be transferred across the ESD for FSA failure to occur. There are four mechanisms in the system model for transferring electrical energy across the ESD — ESD was installed enabled, ESD has electrical breakdown as a result of environment, ESD is enabled by environment, and ESD is electrically bypassed.

An additional design feature shown in Figure 1 is the crowbar circuit. The crowbar circuit grounds the Fireset and prevents its being armed. During normal operation, this ground is removed when the ESD is enabled.

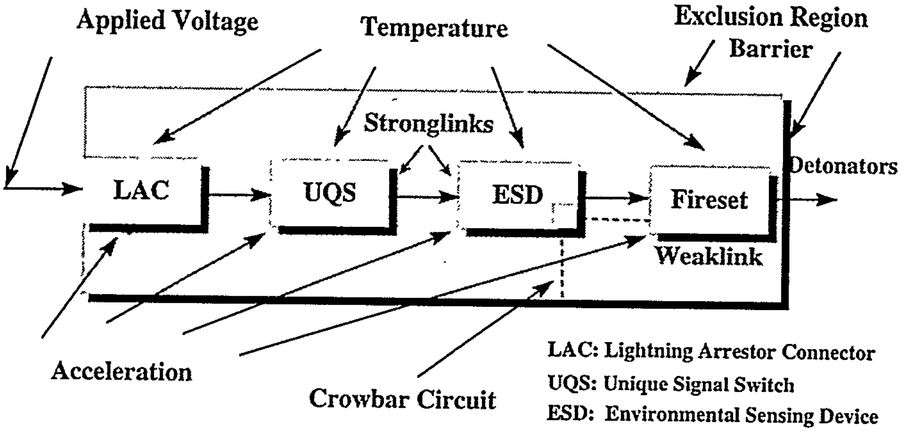


Figure 1. Firing system assembly for a nuclear weapon.[3]

The Direct Quantification Method (DQM)

Table 1 lists the principal steps in using DQM to assess FSA Failure and MC compliance.

Table 1. Principal Steps in Using DQM to Assess FSA Failure and MC Compliance

1. Develop Fault Tree for FSA Failure
2. Solve Fault Tree
3. Develop Basic Event Probability Functions (BEPFs)
4. Perform Analysis for Normal Environments
5. Simulate Accidents Leading to Abnormal Environments
6. Perform Analysis for Abnormal Environments
7. Assess Compliance with Military Characteristics (MCs)

In this section, we discuss the use of DQM to quantify FSA failure, determine MC compliance, and understand the performance of safety-critical subsystems and components in several abnormal environments. In the remainder of this section, we

[3] The FSA in [1] is slightly more complex, but no essential features are lost by the simplifications made here.

discuss and illustrate the seven steps in Table 1 and mathematical formulations used in DQM.

1. *Develop Fault Tree for FSA Failure*

The initial step in fault-tree analysis is to develop a fault tree.[4] Developing a fault tree begins by stating the top event that describes an undesired state of the system. Proper selection of this event is important since the entire fault-tree analysis is tailored to it. For our application, this event must characterize an undesired state of the weapon system that is appropriate for assessing if the FSA performs its intended function to provide for nuclear-detonation safety to the levels specified in its MCs.

Since the intended nuclear-detonation-safety function of the FSA is to withhold unintended electrical energy applied to it from initiating the NEP detonators, a top event that succinctly describes such an undesired state of the weapon whose FSA is depicted in Figure 1 is:

FSA fails to withhold unintended electrical energy sufficient to initiate detonators.

Once a top event is stated, a fault tree for the top event is developed. Developing a fault tree involves writing Boolean equations using events that are necessary and sufficient conditions for the top event to occur. Figure 2 shows the initial development of a fault tree for FSA failure based on the system shown in Figure 1.

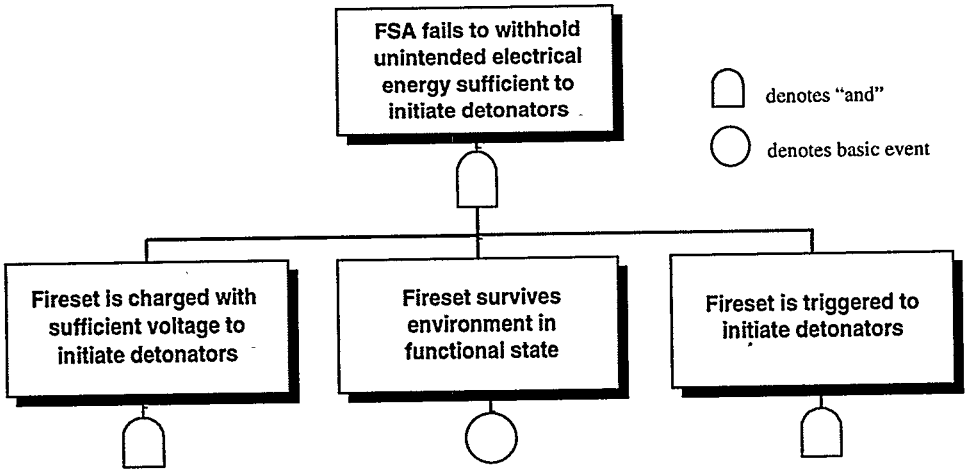

FSA fails to withhold unintended electrical energy sufficient to initiate detonators
denotes "and"
denotes basic event
Fireset is charged with sufficient voltage to initiate detonators
Fireset survives environment in functional state
Fireset is triggered to initiate detonators

Figure 2. Initial development of fault tree for FSA failure.

The development continues by writing equations until only basic or undeveloped events are present that are indicative of the desired resolution of the system. Generally, the resolution is at the safety-critical component level. The fault tree is a graphical model of the combinations of events (faults) that will result in the occurrence of the undesired top event. The events can be associated with component failures, human errors, or other

[4] See [4] for information on fault-tree analysis.

actions or states that lead to the occurrence of the top event. Thus, the fault tree depicts the logical interrelationships of events that lead to the top event.

2. *Solve Fault Tree*

Solved the fault-tree equations. The solution is shown in Equation 1. The solution in this equation expresses the top event as a Boolean sum (logical "or") of cutsets. (Cutsets are inside each pair of parentheses.) Each cutset consists of a Boolean product (logical "and") of basic events and is a sufficient condition for the top event to occur.

The solution to the fault tree shown in Figure 2 in disjunctive normal form is:

FSA-FAILURE
if and only if
{ (FIRESET-SRV-ENV and LAC-XFER-EE and ESD-ENV-ENB
and EE-TO-LAC and ESSG-ENB-UQS)
or
(FIRESET-SRV-ENV and LAC-XFER-EE and ESD-ENV-ENB
and EE-TO-LAC and UQS-INST-ENB)
or
•
•
•
or
(FIRESET-SRV-ENV and LOSS-CROWBAR and UQS-ELEC-BKDN
and LAC-XFER-EE and ESD-INST-ENB and EE-TO-LAC) } (Eq. 1)

Table 2 lists the top event and basic events in the solution to the fault tree along with the symbols representing each event.

3. *Develop Basic Event Probability Functions (BEPFs)*

A fault tree is not a quantitative model, but is a qualitative model of the events that cause the top event to occur. Quantification of the fault tree is often desired to determine the probability of the top event. Given the solution to the fault tree, the probability of the top event can be calculated once the probabilities of the basic events are known.

Therefore, the next step is to develop a set of functions that give the probabilities of the basic events as functions of environmental conditions. These functions are called BEPFs. The environmental conditions considered for the application in reference [1] are applied voltage, temperature, and acceleration. Each safety-critical component is designed to be predictably safe as stated by the national expectations for nuclear-detonation safety. One identifies this design feature from knowledge of the physical principles underlying the operation of safety-critical components and uses it to develop stochastic models for the

Table 2. Basic Events in Solution to the Fault Tree for FSA Failure

Symbol for Event	Description of Event
FSA-FAILURE	FSA fails to withhold unintended electrical energy sufficient to initiate detonators.
EE-TO-LAC	Electrical energy sufficient to initiate detonators is applied to LAC
LAC-XFER-EE	LAC transfers electrical energy
UQS-INST-ENB	Unique signal switch is installed enabled
UQS-ENV-ENB	Unique signal switch is enabled by environment
UQS-ELEC-BKDN	Unique signal switch has electrical breakdown as a result of environment
UQS-BYPASSED	Unique signal switch is electrically bypassed
ESSG-ENB-UQS	ESSG enables unique signal switch
ESD-INST-ENB	ESD is installed enabled
ESD-ENV-ENB	ESD is enabled by environment
ESD-ELEC-BKDN	ESD has electrical breakdown as a result of environment
ESD-BYPASSED	ESD is electrically bypassed
LOSS-CROWBAR	Ground connection provided by crowbar circuit is broken
FIRESET-SRV-ENV	Fireset survives environment in functional state

probabilities of the basic events as functions of applied voltage, temperature, and acceleration. To develop these models, we use test data and other scientific and engineering information.

Once the BEPFs are provided, the probability of the top event is obtained using the solution to the fault tree. We derived the name "Direct Quantification Method" from the direct substitution of BEPF values into the equation for the probability of the top event to obtain the probability of the top event.

The BEPFs and the basis of the stochastic models for the BEPFs in physical (first) principles are the key steps in DQM that distinguish DQM from other quantification methods based on fault-tree analysis. Equation 2 shows the BEPF for the basic event "UQS has electrical breakdown as a result of environment."

$$\mathrm{Pbkdn - temp}\ (V,T) = \left[1 - \mathrm{Pvent}\ (T,A)\right] \left\{ \frac{(\mathrm{Pbkdn}\ (V,20) - \mathrm{Pscrn}\ \mathrm{Pbkdn}\ (\min(V,2600),20))}{1 - \mathrm{Pscrn}\ \mathrm{Pbkdn}\ (\min(V,2600),20)} \right\}$$

$$+\ \mathrm{Pvent}\,(T,A) \left\{ \frac{(\mathrm{Pbkdn}\ (V,T) - \mathrm{Pscrn}\ \mathrm{Pbkdn}\ (\min(V,\mathrm{Vscrn}\ (T)),T))}{1 - \mathrm{Pscrn}\ \mathrm{Pbkdn}\ (\min(V,\mathrm{Vscrn}\,(T)),T)} \right\} \qquad \text{(Eq. 2)}$$

where

$P_{\text{UQS ELEC-BKDN}}$ = probability for basic event "UQS has electrical breakdown as a result of environment,"
V = voltage of electrical energy source applied to UQS in volts,
T = internal temperature of UQS in °C,
A = acceleration of UQS in units of g (acceleration due to gravity),
P_{vent} = probability that UQS vents in thermal or mechanical environments,
P_{bkdn} = probability for electrical breakdown of UQS at constant pressure,
P_{scrn} = screening efficiency of inspection process, 0.95,
V_{scrn} = screening voltage for UQS, and
$\min(A,B)$ = minimum of real numbers A and B.

A BEPF for each basic event in Table 2 was developed.[5]

Mathematical Formulations Used in the Direct Quantification Method

Two mathematical formulations are used with DQM [1]. The first formulation uses the solution to the fault tree and the BEPFs to obtain the top-event probability as a function of environmental conditions. This probability is given as a function of time if these environmental conditions are known as functions of time during an accident scenario. Not only does this formulation provide the top-event probability, but it also provides the capability to help understand the safety performance of a weapon during an accident. Examination of the top-event probability and the BEPFs during an accident scenario can help identify and understand any design vulnerabilities that could cause existing nuclear safety standards, criteria or design-specific requirements not to be met. It is the BEPFs and their development based on first-principle safety design features of a weapon that provides this capability.

The second formulation in DQM is an integral formulation that provides the probability that the top event occurs during an accident scenario. While the first formulation gives the likelihood of the top event for each environmental condition during a scenario, the integral formulation accumulates the likelihood of the top event's occurring during small intervals and yields a probability that the top event occurred during the scenario. Since this probability is not necessarily greater than the maximum top-event probability during the scenario, we use both probabilities to assess MC compliance.

[5] See [1] for details of the development and discussion of Equation 2 and the remaining BEPFs used in the assessment.

To facilitate computation of the probabilities and provide files for use in the normal and abnormal environment analyses (Steps 4 and 6 in Table 1), we wrote a computer program called the DQM Code. Figure 3 shows the computational scheme used by the DQM Code.

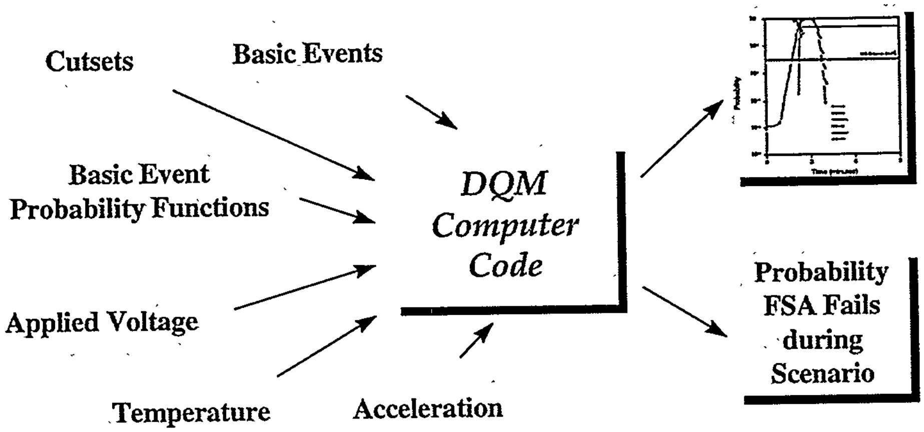


Figure 3. DQM code computational scheme.

4. *Perform Analysis for Normal Environments*

Normal environments are environments in which the weapon is designed to retain operational reliability. The procedure for the normal-environment analysis is outlined in the following table:

Analysis Procedure for Normal Environments

Calculate FSA-failure probabilities as environmental conditions are sampled over normal-environment ranges and values of BEPFs associated with human error are sampled between bounding estimates.

Calculate and examine risk-importance measures -- risk increase and risk reduction.

Perform sensitivity studies on human-error probabilities.

Insight into the performance of the FSA was obtained using risk-importance measure and sensitivity analyses. Sensitivity analyses were performed by considering ranges of probabilities associated with human errors that could lead to not meeting the MC criterion for normal environments.

The risk-importance measures used here are partial derivative, risk reduction, and risk increase. Partial derivative for a basic event gives the rate of change of the top-event probability with respect to the probability of this basic event. The partial derivative can be used to determine how much change in the probability of a basic event is sufficient for the probability of FSA failure to exceed or be less than the MC criteria. Risk reduction for a basic event gives the change of the probability of the top event if the probability of the basic event is reduced to zero. Knowledge of risk reductions can be used to prioritize modifications in weapon components or to suggest positive measures that have the potential to reduce the risk of FSA failure. Risk increase for a basic event gives the change in the probability of the top event if the probability of the basic event is increased to one. One use of this measure is to determine if the probability of any basic event increasing to one will result in the weapon not meeting the 10^{-9} probability per lifetime requirement in normal environments.

5. *Simulate Accidents Leading to Abnormal Environments*

FSA-failure probability and the probability that the FSA fails during an accident can be determined once the environmental conditions at the locations of each component in the FSA are known. These conditions were obtained by computer simulation of accident scenarios leading to abnormal environments. Figure 4 shows the results of one such simulation. This figure shows temperature as a function of time at the locations of the LAC, UQS, ESD, and Fireset for a directed propellant fire with pre-damage to the weapon. The fire temperature is 5000°F and the pre-damage is a 3-inch hole in the aeroshell and exclusion-region barrier near the location of the ESD.

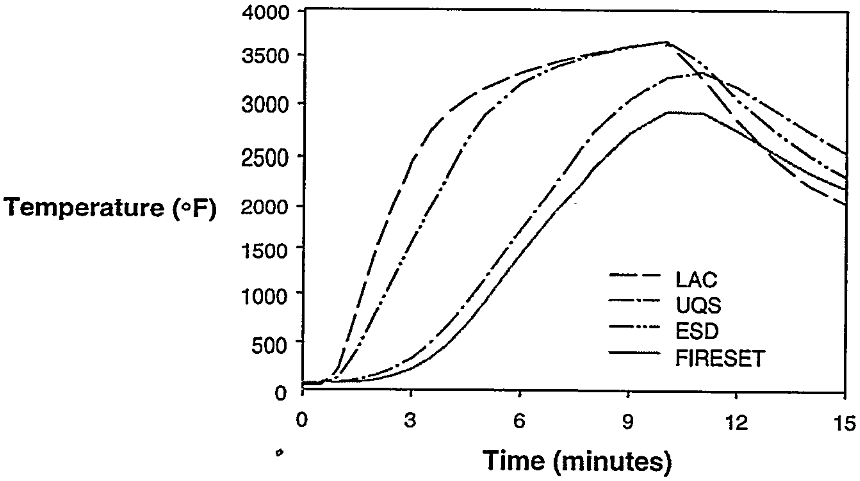


Figure 4. Probability versus time for directed propellant fire (5000°F for 15 minutes) with pre-damage (3-inch diameter hole in aeroshell and FSA cover).

6. *Perform Analysis for Abnormal Environments*

Abnormal environments are environments in which the weapon is not designed to retain full operational reliability. They are environments that occur during accidents. The following table outlines the analysis procedure for abnormal environments:

Analysis Procedure for Abnormal Environments

Calculate failure probabilities using environmental conditions obtained from simulations of accident scenarios.

Calculate uncertainties due to simulation errors and BEPF values.

Calculate and examine risk-importance measures — partial derivative, risk increase, and risk reduction.

Perform sensitivity studies to understand design vulnerabilities or safety performance of the weapon during abnormal environments.

As was the case in the normal-environment analysis, we performed risk-importance and sensitivity analyses to obtain further insight into the performance of the FSA in abnormal environments and its ability to perform its intended function. Risk reduction was used to suggest positive measures that have the potential to reduce the risk of inadvertent nuclear detonation. Risk increase was used to determine if the probability of any basic event increasing to one will result in the weapon not meeting the 10^{-6} probability per accident MC requirement as a result of the FSA failing to perform its intended function. The partial derivative was used to determine how much of a change in a basic-event probability would result in the MC requirement for abnormal environments not being met.

7. *Assess Compliance with Military Characteristics*

Once some analysis has been performed, we assess compliance with MC requirements for normal and abnormal environments by answering the questions in the following table:

Question Used to Assess Compliance with MC Requirements

Normal Environments

Are FSA-failure probabilities over the range of normal environments and probabilities associated with potential human errors less than the MC criterion for normal environments (10^{-9} per lifetime)?

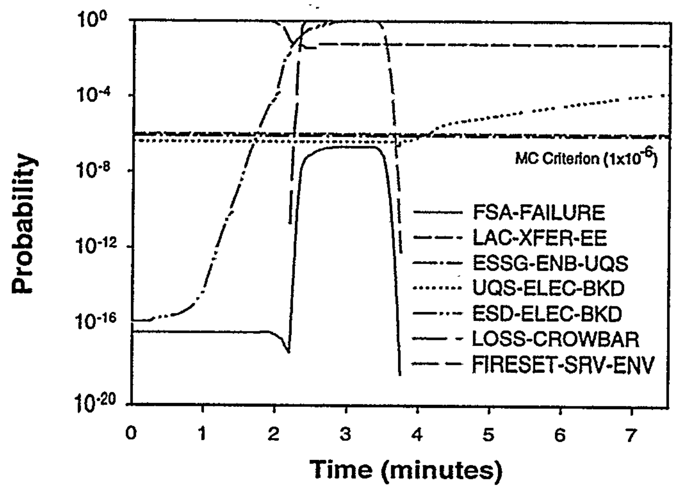
Abnormal Environments

For each accident scenario, are FSA-failure probabilities in all environments occurring during the scenario and their uncertainties due to simulation errors and BEPF sensitivities and the probability that FSA fails during an accident less than MC criterion for abnormal environments (10^{-6} per accident)?

In combined engineering judgment, do the accident scenarios considered cover the spectrum of credible abnormal environments?

In reference [1], the authors considered 17 accident scenarios that in their engineering judgment covered the spectrum of credible abnormal environments. They also considered other scenarios and performed sensitivity studies to better understand the performance of the FSA in providing for nuclear-detonation safety.

In this paper, I consider the thermal-mechanical accident scenario whose temperature histories are shown in Figure 4. Figure 5 shows calculated FSA-failure and selected basic-event probabilities for about the first 7.5 minutes of this scenario and the probability that the FSA fails during this scenario.



Probability that FSA fails during scenario is $2\text{x}10^{-7}$

Figure 5. Calculated probabilities for directed propellant fire (5000°F for 15 minutes) with pre-damage (3-inch diameter hole in aeroshell and FSA cover).

A directed propellant fire with pre-damage to the aeroshell and FSA cover at the location of the ESD is considered to provide the environment in which the FSA is most vulnerable to failure. The main results from the analysis of this scenario are summarized in the following table:

Summary of Accident Scenario: Directed Propellant Fire with Pre-Damage

Prominent Features of Accident Scenario

All failure probabilities are less than the MC criterion for abnormal environments.

It is not until the crowbar circuit is destroyed by melting at its connection to the ESD that electrical breakdown of the ESD contributes to and dominates FSA failure.

The MC criterion for abnormal environments is met because the probability of electrical breakdown across the UQS remains less than 10^{-6} until the fireset becomes irreversibly inoperable and it is less likely that electrical energy is transferred across the LAC since it effectively grounds all applied electrical energy at elevated temperatures.

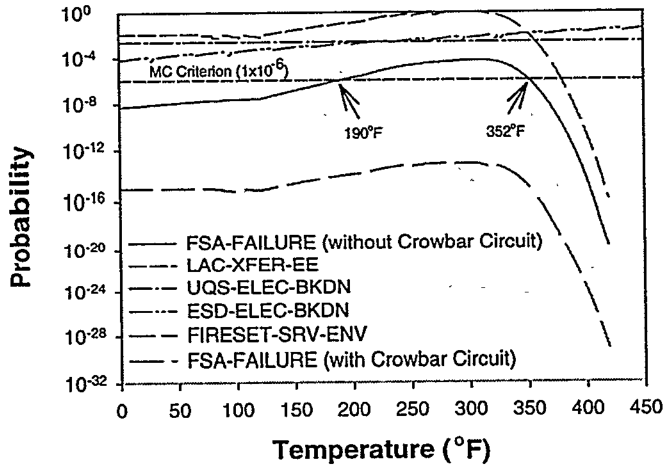
Conclusion

The MC requirement for abnormal environments is met for this accident scenario.

Valued Added by Using the Direct Quantification Method

Additional value beyond assessment of MC compliance is provided by DQM. FSA-failure probability and knowledge of the BEPFs as functions of time permits visualizing and understanding the safety performance of components and subsystems during an accident scenario. Further value is added by providing the capability to identify potential positive measures and useful testing and to prioritize modifications to a weapon system. I provide two examples to illustrate some of this added value.

In the first example, consider a slow cookoff of the weapon with 1800 volts applied to all circuits entering the FSA through the LAC as the temperature is increased from 0°F to 450°F. I performed calculations for FSAs with and without a crowbar circuit. Figure 6 shows probabilities calculated for this scenario.



Probability that FSA fails during scenario is $8x10^{-16}$ for FSA with Crowbar Circuits and $2x10^{-5}$ for FSA without Crowbar Circuits

Figure 6. Calculated probabilities for a slow cookoff with 1800 volts applied to FSAs with and without a crowbar circuit.

This accident scenario is summarized in the following table:

Summary of Slow Cookoff Scenarios with 1800 Volts Applied to LAC

Purpose of calculation

To understand and gain insights into safety performance of the FSA.

Prominent features

The MC requirement for abnormal environments is met for an FSA with a crowbar circuit and is not met if this FSA does not have a crowbar circuit.

Failure probability is greater than MC criterion for temperatures between 190°F and 352°F and probability that FSA fails during scenario is $5x10^{-5}$.

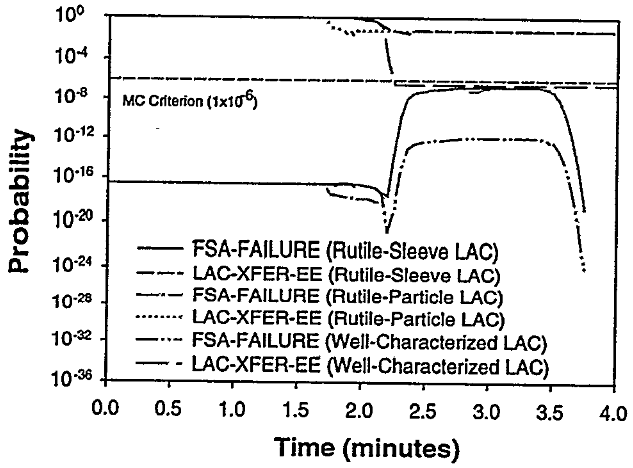
ESD electrical breakdown and LAC energy transfer dominate failure until the Fireset becomes irreversibly inoperable.

Conclusion

The MC requirement for abnormal environments would not be met if a crowbar circuit were not included in the design of this FSA.

The second example shows the result of some sensitivity calculations based on the propellant fire scenario with pre-damage to the weapon. One calculation seeks to determine if replacement of the rutile-sleeve LAC with a rutile-particle LAC would result in smaller failure probabilities. To perform this calculation, I used the electrical-breakdown properties of a rutile-particle LAC instead of the electrical-breakdown properties for the rutile-sleeve LAC in Figure 1. The other calculation seeks to determine if further measurements of the breakdown voltage of the rutile-sleeve LAC might result in smaller failure probabilities. Instead of the rather large, recommended standard deviation for electrical breakdown, I used a value constrained to be no larger than the measurement itself. I call this rutile-sleeve LAC a "well-characterized" LAC.

Figure 7 shows calculated probabilities for the directed propellant fire with pre-damage for FSAs using rutile-sleeve, rutile-particle, and well-characterized LACs.



Probability that FSA fails during scenario is $2x10^{-7}$ for FSA with a Rutile-Sleeve LAC $2x10^{-7}$ for FSA with a Rutile-Particle LAC and $1x10^{-12}$ for FSA with a Well-Characterized LAC

Figure 7. Calculated probabilities for directed propellant fire with pre-damage for FSAs using rutile-sleeve, rutile-particle, and well-characterized LACs.

These sensitivity calculations are summarized in the following table:

Summary of Sensitivity Calculations for FSA Using Various LACs

Purpose of calculation

To suggest potential improvements in safety performance by component modifications and potential improvements in assessed safety levels by additional testing.

Prominent features

The failure probabilities are nearly identical for the FSAs with rutile-sleeve and rutile-particle LACs.

The failure probabilities are over five orders of magnitude smaller for an FSA with a "well-characterized" LAC.

Conclusions

Using rutile-particle LAC rather than a rutile-sleeve LAC is not expected to improve safety.

Additional testing could result in assessing system to be safer.

Concluding Remarks

DQM complements traditional nuclear-weapon assessment methods to achieve the primary goal of nuclear-weapon safety assessment. It is a synergism of the required design basis of nuclear weapons and fault-tree analysis. Since DQM is quantitative, it can be used to determine if quantitative requirements are met. It is first-principle based through its use of the BEPFs. The BEPFs are the key feature of DQM that distinguishes DQM from other quantitative assessment methods based on fault-tree analysis. The stochastic models for the BEPFs are developed by first understanding the physical laws that govern the performance of safety-critical components in normal and abnormal environments and, then, developing the BEPFs using available information including test data and scientific and engineering information. If the safety requirements are not met, then vulnerabilities are easily identified and understood since the basis of BEPF development is an understanding of the physical principles governing the performance of safety-critical components. If the requirements are met, then this basis aids in understanding the contributions of the system components to safety. DQM adds value by providing the capability to understand safety performance, to identify vulnerabilities, potential positive measures, and useful testing, and to prioritize modifications to the weapon system.

References

1. Demmie, P. N., NSafE Probabilistic Risk Assessment Process for the W78 Firing System Assembly, draft report, Sandia National Laboratories, Albuquerque, NM, July 1997.

2. Ives, E. E. and R. L. Schwoebel (Owners), The Process for Achieving Nuclear Weapon Safety at Sandia National Laboratories (The Blue Book), DG 10100, Sandia National Laboratories, Albuquerque, NM, October 1993.

3. Joint UK/US Emergency Response Nuclear Weapons Surety Glossary, The Nuclear Safety Information Center, Sandia National Laboratories, Albuquerque, NM, March 1994.

4. Vesely, W. E., F. F. Goldberg, N. H. Roberts, and D. F. Haasl, Fault Tree Handbook, NUREG-0492, U. S. Nuclear Regulatory Commission, Washington, DC, January 1981.

Biography

Dr. Paul N. Demmie
Sandia National Laboratories
Albuquerque, NM 87185-0491
Phone: 505-844-7400
E-mail: pndemmi@sandia.gov
Fax: 505-844-7494

Dr. Demmie received a BS degree in 1964 and a Ph.D. degree in 1971 in physics from the University of Pittsburgh. He was a faculty member in the Natural Sciences Division of the University of Pittsburgh at Johnstown from 1971 through 1976 where he taught mathematics and physics. He was a Senior Scientist at the Idaho National Engineering Laboratory (INEL) from 1977 until 1983 when he became a Member of the Technical Staff (MTS) at Sandia National Laboratories (SNL). His assignments at INEL and initially at SNL involved nuclear reactor safety. Initially at INEL, he was on the staff of the Thermal Analysis Department and later in the Loss-of-Fluid Test Program where he designed, predicted, and analyzed large break loss-of-coolant accident experiments. He began his tenure at SNL in the Thermal Hydraulics Department where he developed the Heat Structure Package for the MELCOR Program. Later he worked in electromagnetic analysis to support strategic missile defense programs. Since 1992, except for a one-year temporary assignment with the Ballistic Missile Defense Organization in Washington, DC, he has been a Senior MTS in the Surety Assessment Center where he has worked on many aspects of nuclear weapon safety. His interests include developing and applying analytical methods to system-safety assessments.

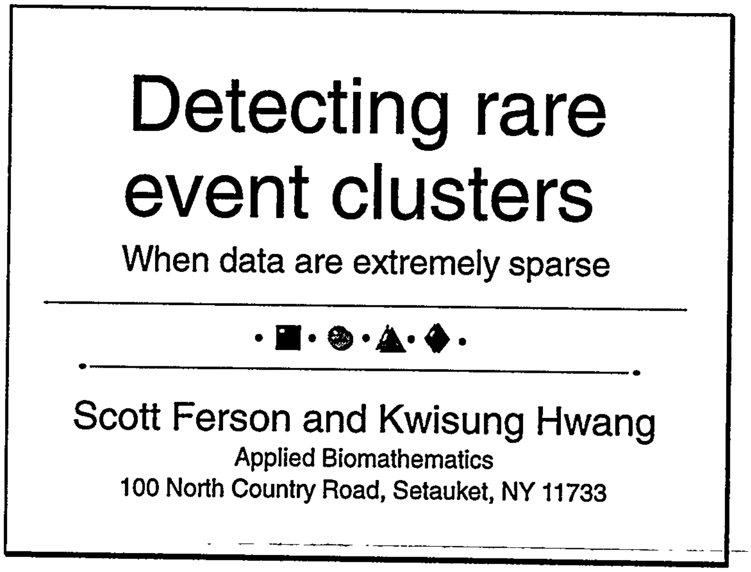
Intentionally left blank

(

Detecting Rare Event Clusters

Scott Ferson
Kwisung Hwang
Applied Biomathematics
Setauket, New York

Slide 1

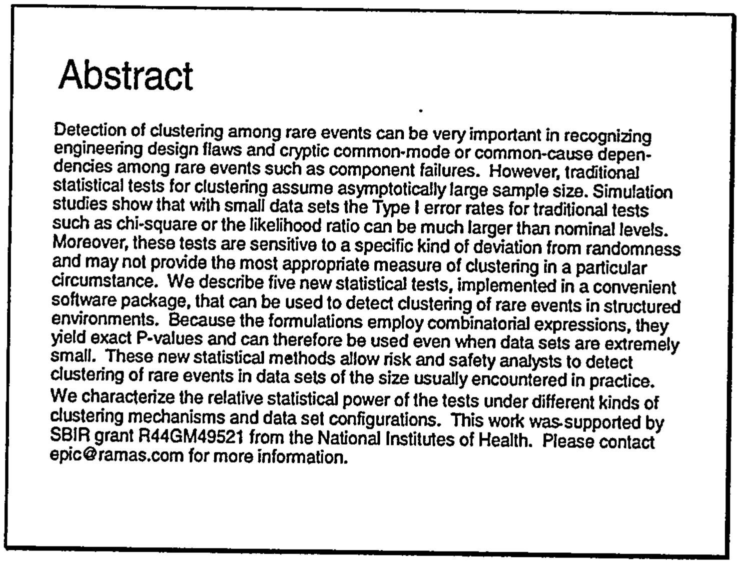


Detecting rare event clusters

When data are extremely sparse

Scott Ferson and Kwisung Hwang
Applied Biomathematics
100 North Country Road, Setauket, NY 11733

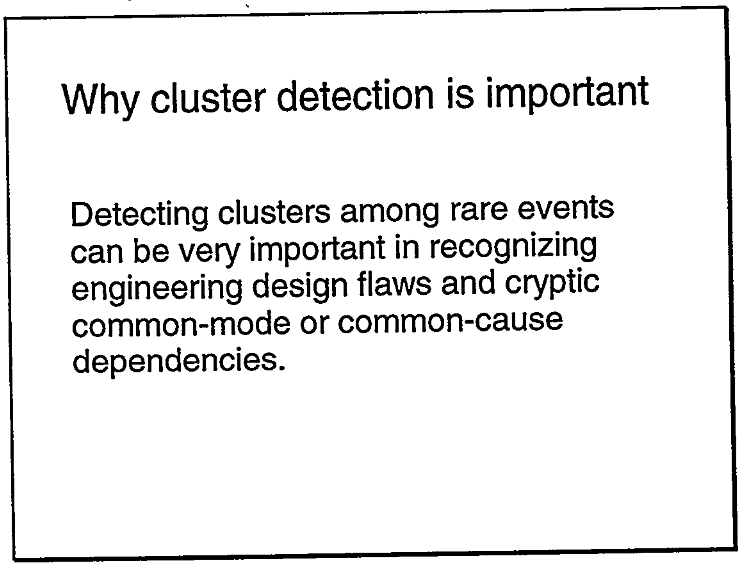
Slide 2



Abstract

Detection of clustering among rare events can be very important in recognizing engineering design flaws and cryptic common-mode or common-cause dependencies among rare events such as component failures. However, traditional statistical tests for clustering assume asymptotically large sample size. Simulation studies show that with small data sets the Type I error rates for traditional tests such as chi-square or the likelihood ratio can be much larger than nominal levels. Moreover, these tests are sensitive to a specific kind of deviation from randomness and may not provide the most appropriate measure of clustering in a particular circumstance. We describe five new statistical tests, implemented in a convenient software package, that can be used to detect clustering of rare events in structured environments. Because the formulations employ combinatorial expressions, they yield exact P-values and can therefore be used even when data sets are extremely small. These new statistical methods allow risk and safety analysts to detect clustering of rare events in data sets of the size usually encountered in practice. We characterize the relative statistical power of the tests under different kinds of clustering mechanisms and data set configurations. This work was supported by SBIR grant R44GM49521 from the National Institutes of Health. Please contact epic@ramas.com for more information.

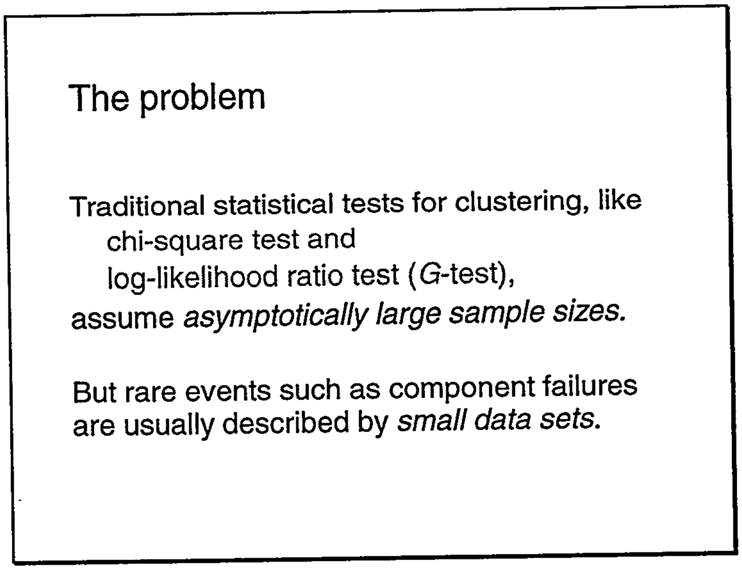
Slide 3



Why cluster detection is important

Detecting clusters among rare events can be very important in recognizing engineering design flaws and cryptic common-mode or common-cause dependencies.

Slide 4

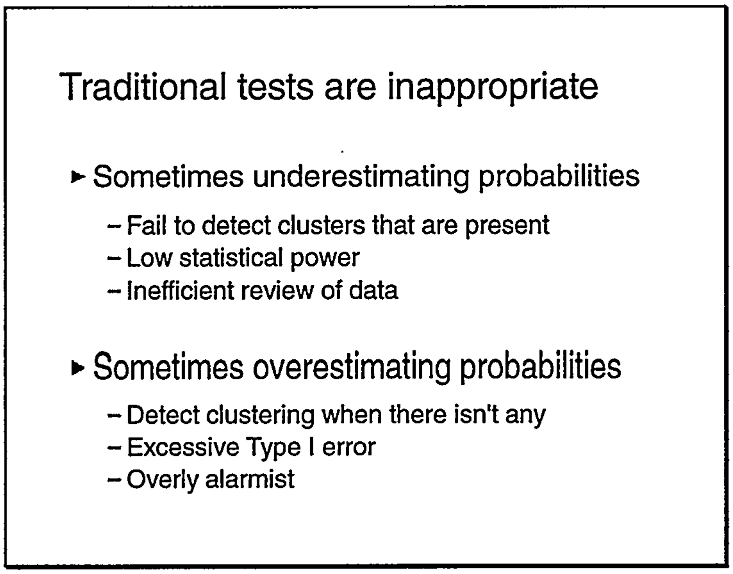


The problem

Traditional statistical tests for clustering, like
chi-square test and
log-likelihood ratio test (*G*-test),
assume *asymptotically large sample sizes.*

But rare events such as component failures are usually described by *small data sets.*

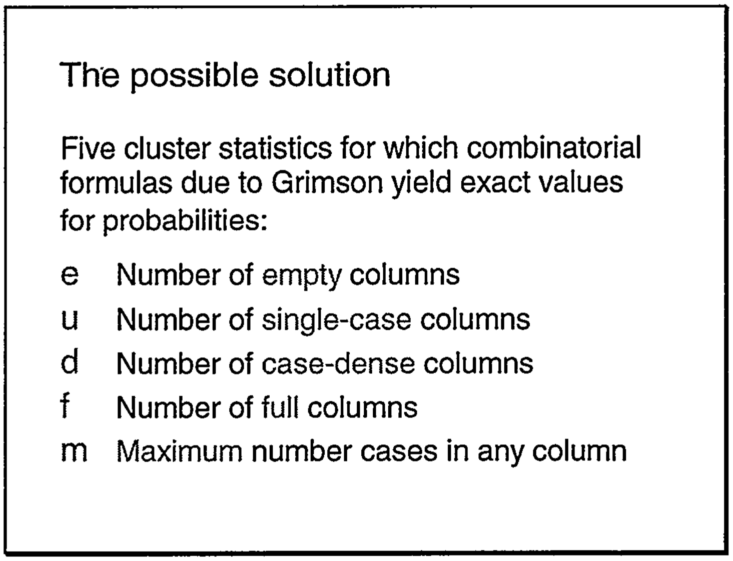
Slide 5



Traditional tests are inappropriate

- Sometimes underestimating probabilities
  - Fail to detect clusters that are present
  - Low statistical power
  - Inefficient review of data
- Sometimes overestimating probabilities
  - Detect clustering when there isn't any
  - Excessive Type I error
  - Overly alarmist

Slide 6



The possible solution

Five cluster statistics for which combinatorial formulas due to Grimson yield exact values for probabilities:

e	Number of empty columns
u	Number of single-case columns
d	Number of case-dense columns
f	Number of full columns
m	Maximum number cases in any column

Slide 7

Is there clustering within columns?

	■					
	■					
	□					
	■	■				
■	■	□		□	□	
□	■	■	□	■	□	■
□	■	□	■	□	□	□
■	■	□	□	□	□	□

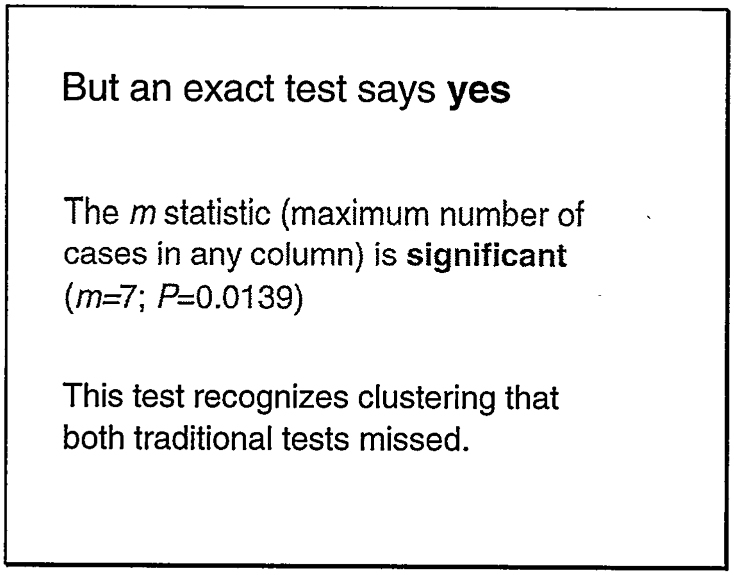
Slide 8

Traditional tests say **no**

Chi-square says **not significant**
(*X*²=9.34; *df*=6; *P*=0.155)

Log-likelihood ratio says **not significant**
(*G*=11.46; *df*=6; *P*=0.0753)

Slide 9

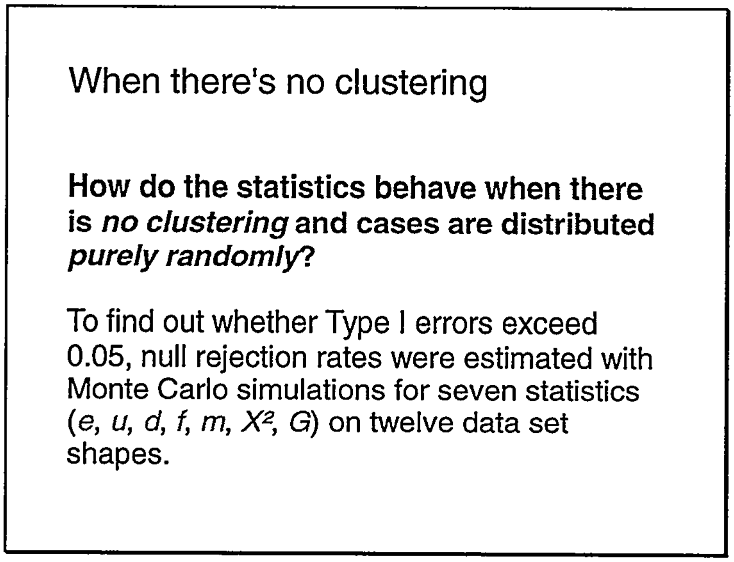


But an exact test says **yes**

The *m* statistic (maximum number of cases in any column) is **significant** (m=7; P=0.0139)

This test recognizes clustering that both traditional tests missed.

Slide 10



When there's no clustering

How do the statistics behave when there is *no clustering* and cases are distributed *purely randomly*?

To find out whether Type I errors exceed 0.05, null rejection rates were estimated with Monte Carlo simulations for seven statistics (e, u, d, f, m, X^2, G) on twelve data set shapes.

Slide 11

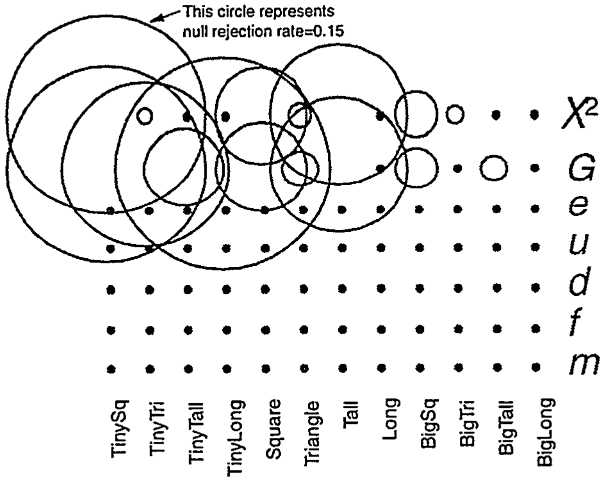
Null rejection rates

An open circle (rather than a ball) indicates a violation of the nominal 5% rejection rate. The bigger the circle, the stronger the violation.

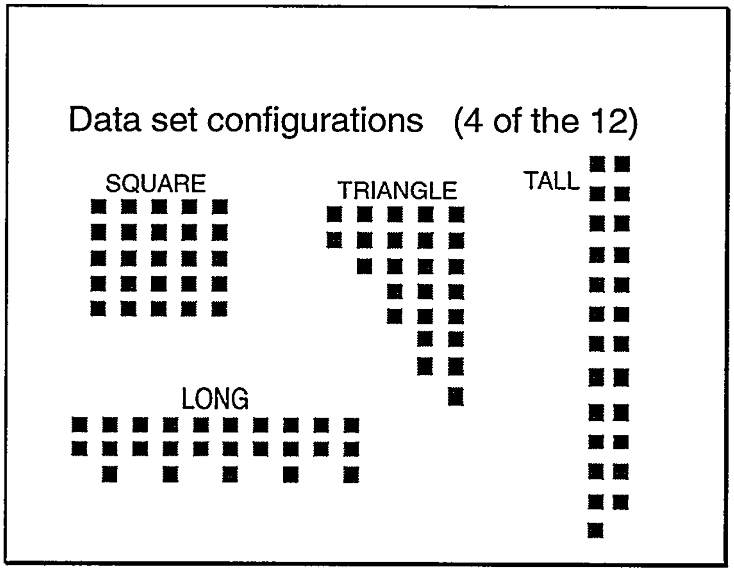
Traditional statistics X^2 and G routinely and strongly violate their nominal rejection rates.

The exact statistics *e, u, d, f, m* never do.

Slide 12



Slide 13



Data set configurations (4 of the 12)

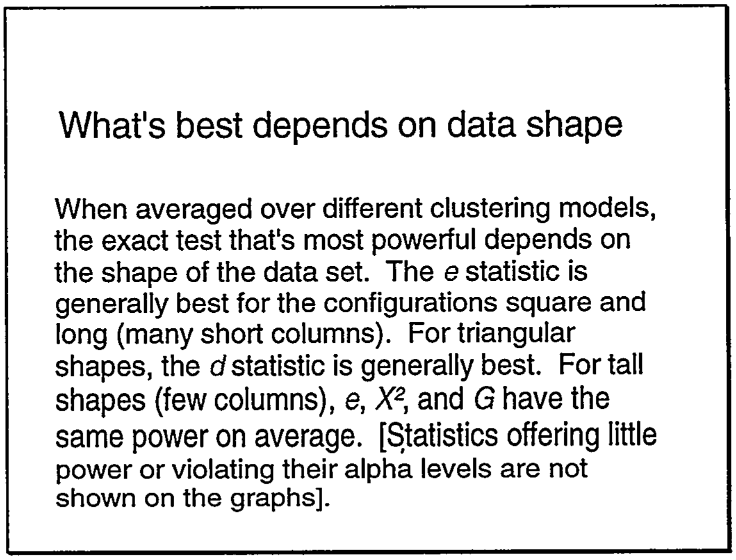
Slide 14

When there is clustering

How easily do the statistics discern the clustering when cases are distributed in some contagious distribution?

Power comparisons among the 7 statistics were made in a Monte Carlo simulation using a factorial design with 12 data set shapes, 3 incidence rates (cases/cell), 5 models for the clustering mechanism, 9 clustering strengths, and 2000 Monte Carlo iterates.

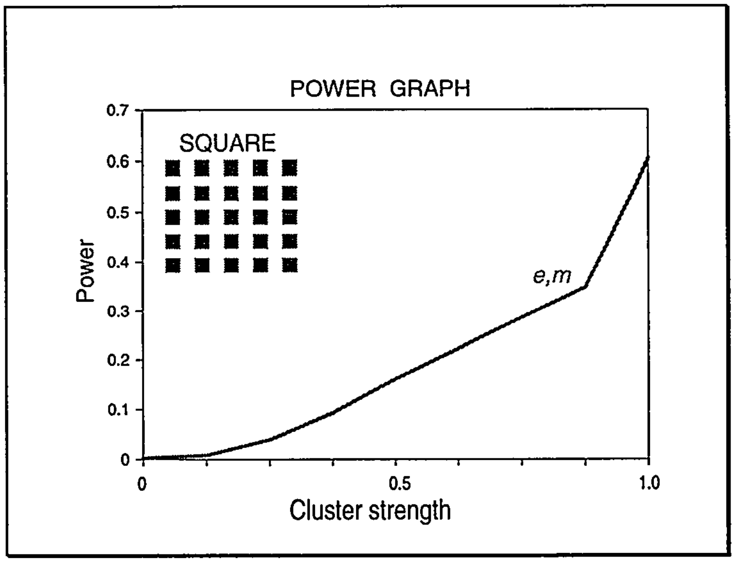
Slide 15



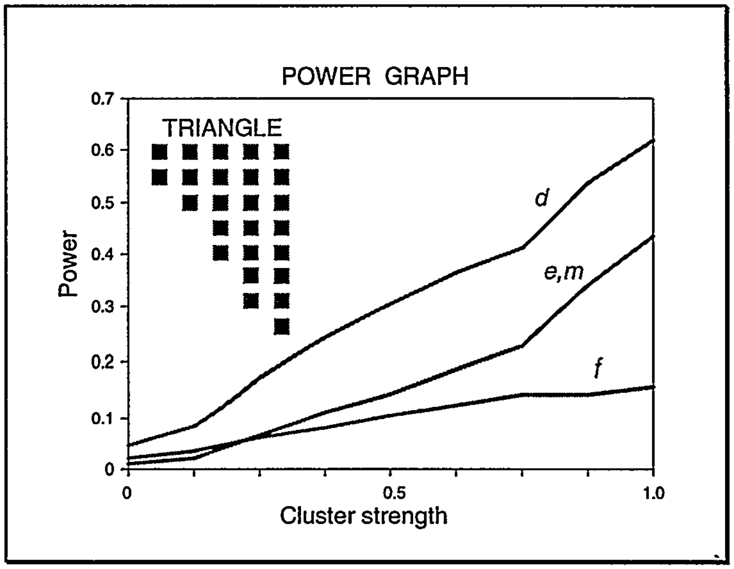
What's best depends on data shape

When averaged over different clustering models, the exact test that's most powerful depends on the shape of the data set. The *e* statistic is generally best for the configurations square and long (many short columns). For triangular shapes, the *d* statistic is generally best. For tall shapes (few columns), *e*, X^2, and *G* have the same power on average. [Statistics offering little power or violating their alpha levels are not shown on the graphs].

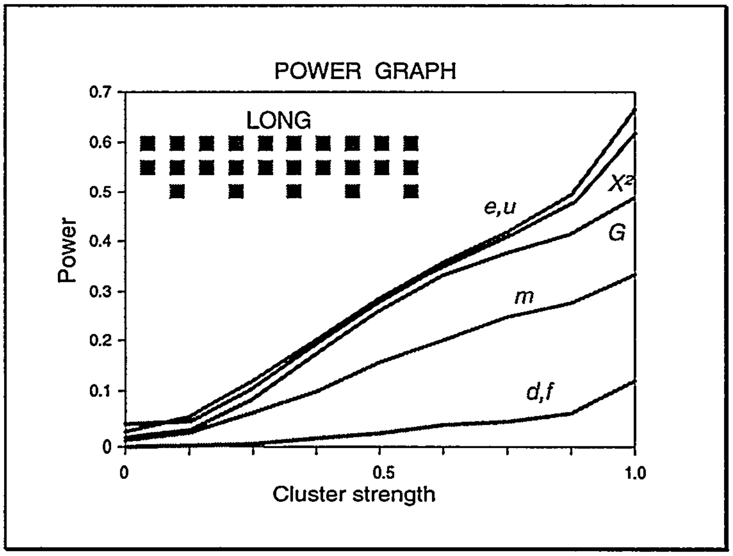
Slide 16



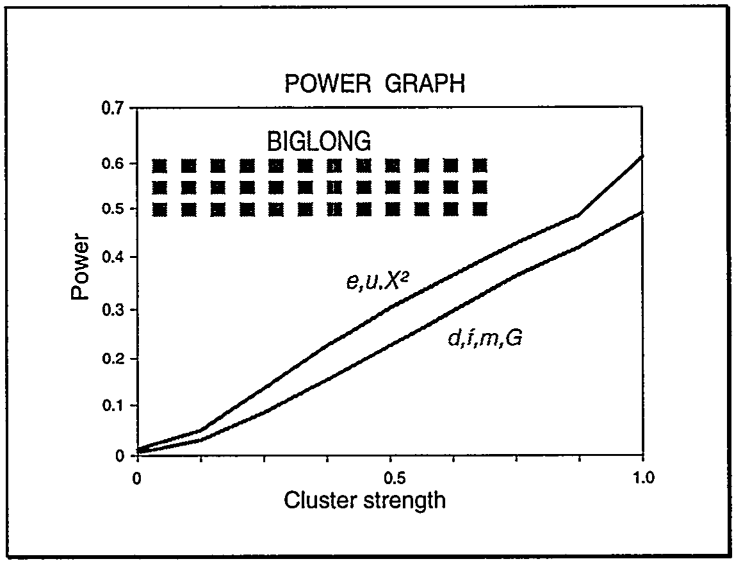
Slide 17



Slide 18



Slide 19



Slide 20

Future work

- ► Explore how the power of the exact statistics varies under different clustering mechanisms
- ► Generalize exact methods for frequency data (like cancer cases reported from hospitals)
- ► Provide exact statistics in convenient software

Implementation of Numerical Simulation Techniques in Express-Analysis of Accidents in Complex Technological Systems

G.S. Klishin
V.E. Seleznev
V.V. Aleoshin
Russian Federal Nuclear Center (RFNC)-All-Russian Research Institute
of Experimental Physics (VNIIEF)
Russia

Gas industry enterprises such as main pipelines, compressor gas transfer stations, gas extracting complexes belong to the energy intensive industry. Accidents there can result in catastrophes and great social, environmental, and economic losses. Annually, according to official data, several dozens of large pipeline accidents take place in the USA and Russia. That is why prevention of pipeline accidents, analysis of the mechanisms of their development, and prediction of their possible consequences are acute and important tasks.

The reasons for an accident are usually complicated and can be presented as a complex combination of natural, technical and human factors. In the RAO "GAZPROM," the reasons for accidents are divided into the following groups:

- Environmental interference
- Defects and drawbacks of the pipes and auxiliary equipment
- Mistakes in pipeline operation
- Damage during pipeline construction
- Unauthorized interference in gas pipe operations

The most dangerous accidents can be followed by fires or a detonating gas mixture can be formed that can result in an explosion. As a rule, these result in great destruction and even injuries or deaths.

Mathematical and computer simulations are a safe, rather effective, and comparatively inexpensive method of accident analysis. They make it possible to analyze different mechanisms of a failure occurrence and development and to assess its consequences and give recommendations to prevent it.

The difficulties in mathematical and computer simulations of pipeline accidents can be explained by

- A wide spectrum of the failure reasons and consequences
- The variety of the accident mechanisms and ways of their development
- An integrated influence of the damaging factors

In the express-analysis of the failure cases, the techniques of theoretical mechanics, of qualitative theory of differential equations, of mechanics of a continuous medium, of chemical macro-kinetics and optimizing techniques are implemented in the Conversion Design Bureau #5 (DB#5) at VNIIEF.

Both universal and special numerical techniques and software (SW) for the solution of such tasks are being developed in DB#5. Almost all of them are calibrated on the calculations of the simulated and full-scale experiments performed at the VNIIEF and MINATOM testing sites. It is worth noting that in the long years of work for the solution of such tasks there has been established a fruitful and effective collaboration of theoreticians, mathematicians, and experimentalists of the institute.

Let us consider in more detail the approaches and mathematical simulation techniques implemented in DB#5, VNIIEF for pipeline failure analysis.

Big movements, shifts, and spread of the construction elements of the pipeline equipment during an accident can be described with the help of the theoretical mechanics equations. Theoretical mechanics techniques are often used in a simplified numerical analysis of the equipment behavior in the emergency mode of operation.

For example, using theoretical mechanics the oscillations of the air column between the blades of a compressor located at a compressor gas transfer station during the surge can be described in the first approximation. The task of the surge simulation in this case can be presented as the analysis of a usual system of differential equations with the given boundary conditions. This analysis is done in accordance with the qualitative theory of differential equations. It makes it possible to evaluate surge stability and character and to predict the accident development.

Implementation of analytical and semi-empirical functions in the express analysis is quite authorized and brings good results when rare situations are being considered. In this case, there is no need to investigate complex computer models.

In the express analysis of the reasons for pipeline destruction, fires, and explosions at pipelines, for solution of the tasks of continuous medium mechanics numerical algorithms and software, both licensed and developed in VNIIEF, are implemented.

In the investigation of fires, a combination of three-dimensional finite element and one-dimensional finite difference models are implemented. Let us consider this approach using the following example: The gas pipe in the building is ruined, a combustible mixture of methane and air is formed that has filled the building inside. There is a heat source in one of the rooms of the building.

To analyze the possible ignition of the combustible mixture, there were performed non-stationary three-dimensional thermal calculations with the help of a finite-element technique. In three-dimensional thermal calculations a gas mixture was assumed as inert. This approach in the analysis of the air-methane mixture heating is quite authorized as the processes of the mixture enflaming take place in a very narrow layer adjacent to the heater. (As a rule, the thickness of the heated layer is considerably less than the distance between the adjacent joints of the finite element grid (graticule) implemented in thermal calculations.)

So, at every time-step of the finite-element technique, after three-dimensional thermal areas were calculated, the most heated micro-volumes of the combustible mixture were selected. In these volumes, the combustible mixture was considered as a mixture where exothermic chemical reactions take place.

One-dimensional, non-stationary thermal calculations with consideration of the kinetics of a chemical exothermic mixture decomposition were then performed to assess the possibility of enflaming the selected micro-volumes. Here finite-difference techniques with an adaptive grid were used.

As a rule, in an emergency at a gas pipeline, the magnitudes of one or several parameters characterizing the design of the equipment or its operation, reach their extremes. That is why, in the simulation of emergency cases at gas pipelines, optimizing techniques are widely used at VNIIEF.

In this case, a target function of the optimizing task describes critical parameters of the gas transfer system as a function of control efforts induced on the pipeline equipment. Task limitation functions reflect constructive and technological limitations of the pipeline equipment or gas transfer process. Taking into account the complexity of gas pipeline systems, the target function and the limitation functions are non-linear multi-parameter functions.

The problem of gas transportation operating costs reduction can also be presented as an optimizing task.

So, we face the need to solve a non-linear, multi-parameter task of conditional optimization that looks like,

$$F(\mathbf{X}) ==> \min, \quad G(\mathbf{X})=0, \quad P(\mathbf{X})>0, \; \mathbf{A} > \mathbf{X} > \mathbf{B},$$

where F(**X**) is a target function, G(**X**), P(**X**), are given limitation functions, **X** is a vector of controlling influences, **A, B** are the given vectors that belong to the n-dimensional Euclidean space.

For the solution of optimizing tasks a library of optimization programs has been developed in DB#5, VNIIEF. Original algorithms for the solution of linear, non-linear, and mini-maximum optimization were realized. Special algorithms to analyze the obtained solution for its extremity were developed. Many years of work with the optimization library confirmed its operability and the sufficient effectiveness of its algorithms.

Besides the analysis of different accidents at the gas pipelines, mathematical simulation techniques that were originally developed in RFNC-VNIIEF for the solution of the tasks of gas industry and pipeline transportation could be implemented in:

- The analysis of the main pipelines state
- Localization of the places of the pipeline destruction
- Creation of new generation information and control systems for the pipeline transportation.

Biography

Biographies not available.

SOFTWARE SAFETY

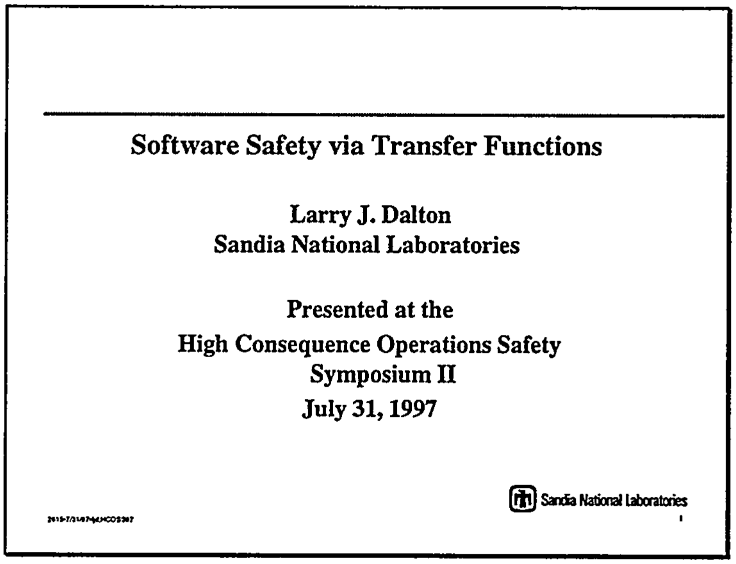
Thursday, July 31, 1997
8:30 a.m. – 12:00 p.m.

Intentionally left blank

Software Safety via Transfer Functions

Larry Dalton
Sandia National Laboratories*
Albuquerque, New Mexico

Slide 1



Software Safety via Transfer Functions

Larry J. Dalton
Sandia National Laboratories

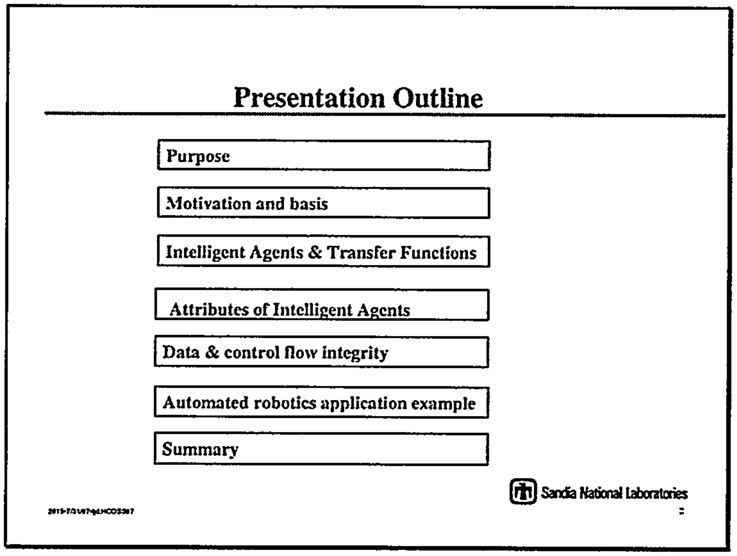
Presented at the
High Consequence Operations Safety
Symposium II
July 31, 1997

Sandia National Laboratories

2919-7/31/97-LJHCOS397

1

Slide 2



Presentation Outline

- Purpose
- Motivation and basis
- Intelligent Agents & Transfer Functions
- Attributes of Intelligent Agents
- Data & control flow integrity
- Automated robotics application example
- Summary

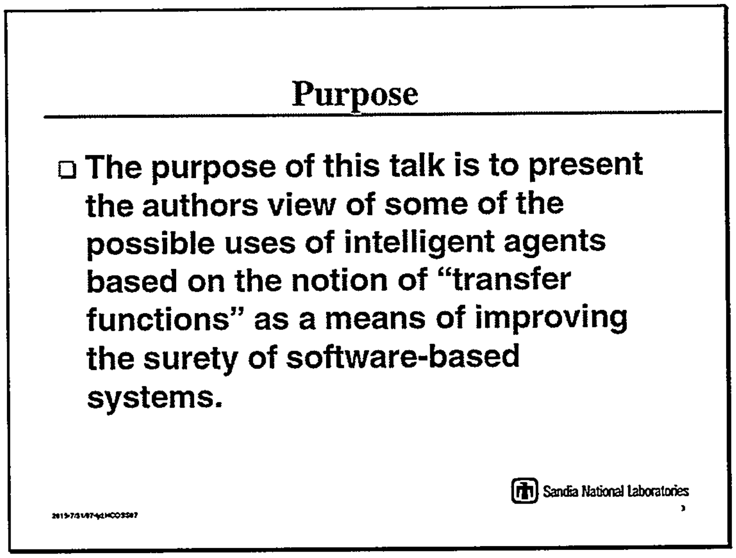
Sandia National Laboratories

2919-7/31/97-LJHCOS397

2

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

Slide 3



Purpose

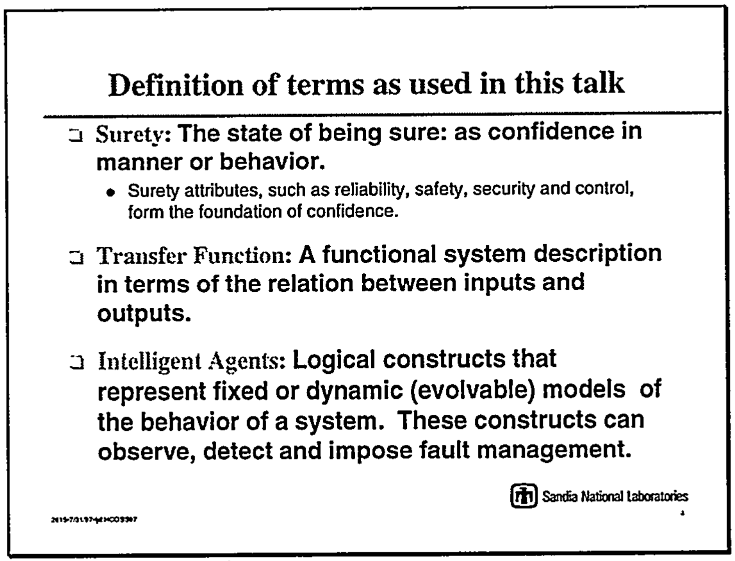
- □ The purpose of this talk is to present the authors view of some of the possible uses of intelligent agents based on the notion of "transfer functions" as a means of improving the surety of software-based systems.

2615-7/31/97-4d HCO5987

Sandia National Laboratories

3

Slide 4



Definition of terms as used in this talk

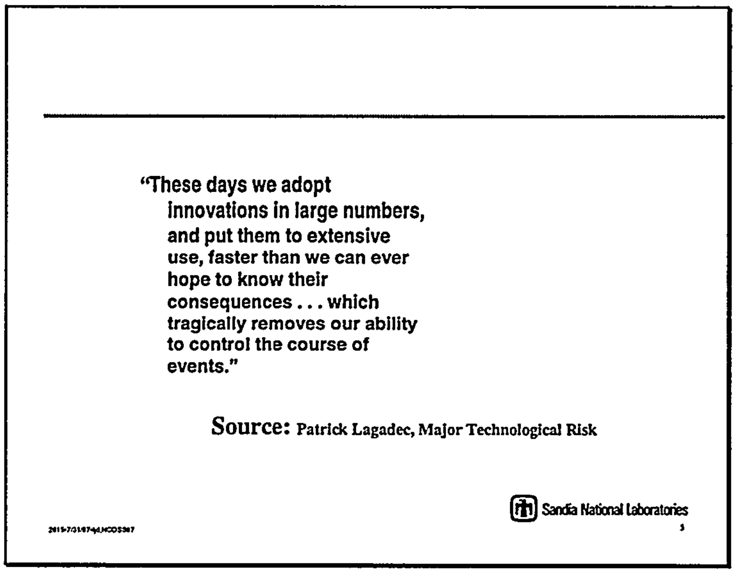
- □ Surety: The state of being sure: as confidence in manner or behavior.
  - Surety attributes, such as reliability, safety, security and control, form the foundation of confidence.
- □ Transfer Function: A functional system description in terms of the relation between inputs and outputs.
- □ Intelligent Agents: Logical constructs that represent fixed or dynamic (evolvable) models of the behavior of a system. These constructs can observe, detect and impose fault management.

2615-7/31/97-4d HCO5987

Sandia National Laboratories

4

Slide 5



"These days we adopt innovations in large numbers, and put them to extensive use, faster than we can ever hope to know their consequences . . . which tragically removes our ability to control the course of events."

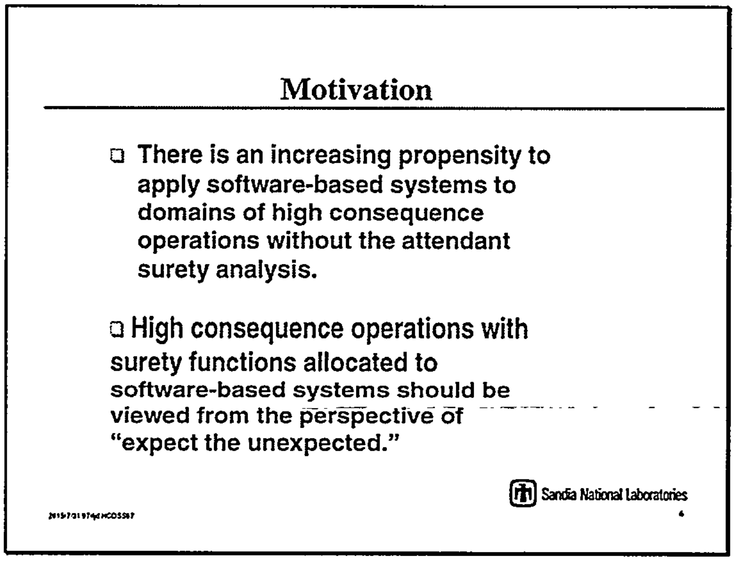
Source: Patrick Lagadec, Major Technological Risk

Sandia National Laboratories

2015-7/31/97-4(HCOS97

5

Slide 6



Motivation

□ There is an increasing propensity to apply software-based systems to domains of high consequence operations without the attendant surety analysis.

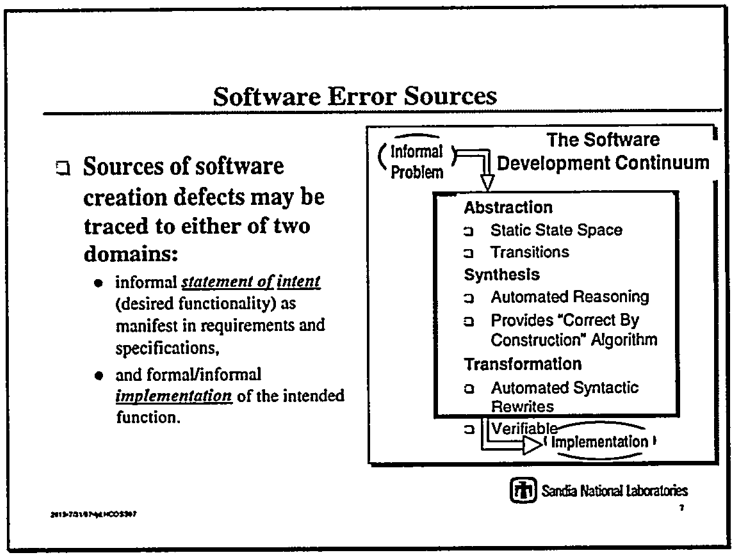
□ High consequence operations with surety functions allocated to software-based systems should be viewed from the perspective of "expect the unexpected."

Sandia National Laboratories

2015-7/31/97-4(HCOS97

6

Slide 7



Software Error Sources

- ❑ **Sources of software creation defects may be traced to either of two domains:**
  - informal *statement of intent* (desired functionality) as manifest in requirements and specifications,
  - and formal/informal *implementation* of the intended function.

Informal Problem

The Software Development Continuum

Abstraction
- ❑ Static State Space
- ❑ Transitions

Synthesis
- ❑ Automated Reasoning
- ❑ Provides "Correct By Construction" Algorithm

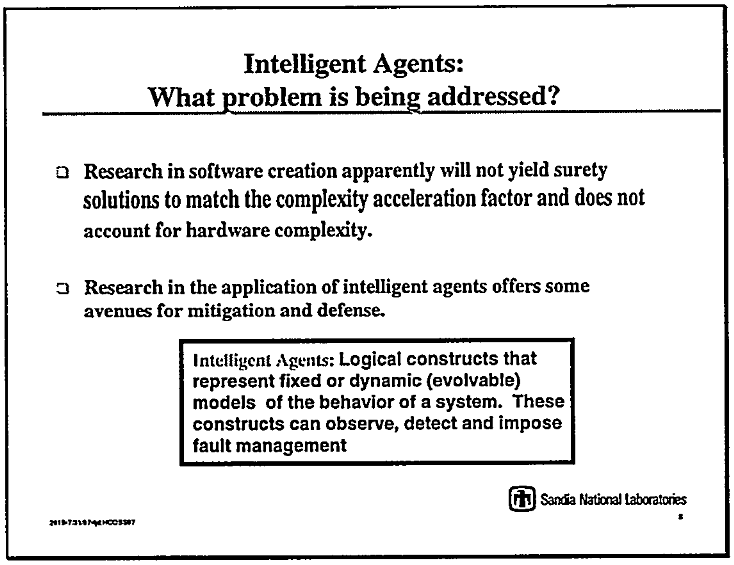
Transformation
- ❑ Automated Syntactic Rewrites
- ❑ Verifiable

Implementation

Sandia National Laboratories

[illegible] 7

Slide 8



Intelligent Agents: What problem is being addressed?

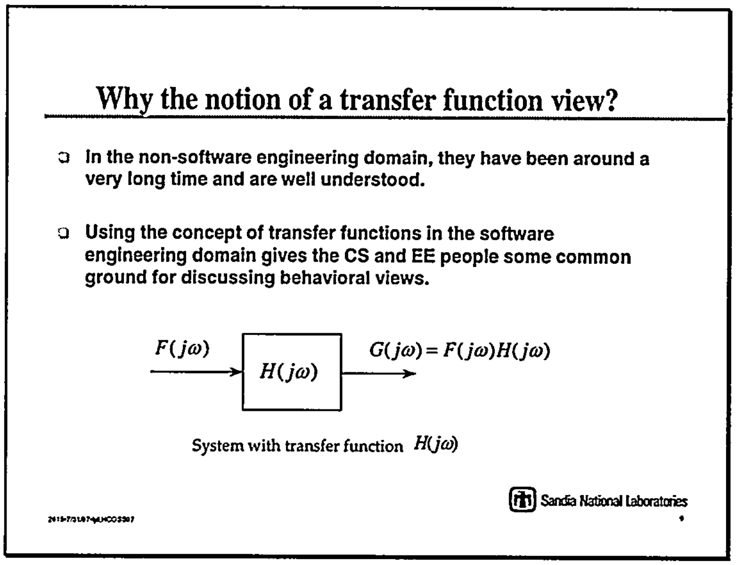
- ❑ **Research in software creation apparently will not yield surety solutions to match the complexity acceleration factor and does not account for hardware complexity.**
- ❑ **Research in the application of intelligent agents offers some avenues for mitigation and defense.**

Intelligent Agents: Logical constructs that represent fixed or dynamic (evolvable) models of the behavior of a system. These constructs can observe, detect and impose fault management

Sandia National Laboratories

[illegible] 8

Slide 9



Why the notion of a transfer function view?

- In the non-software engineering domain, they have been around a very long time and are well understood.
- Using the concept of transfer functions in the software engineering domain gives the CS and EE people some common ground for discussing behavioral views.

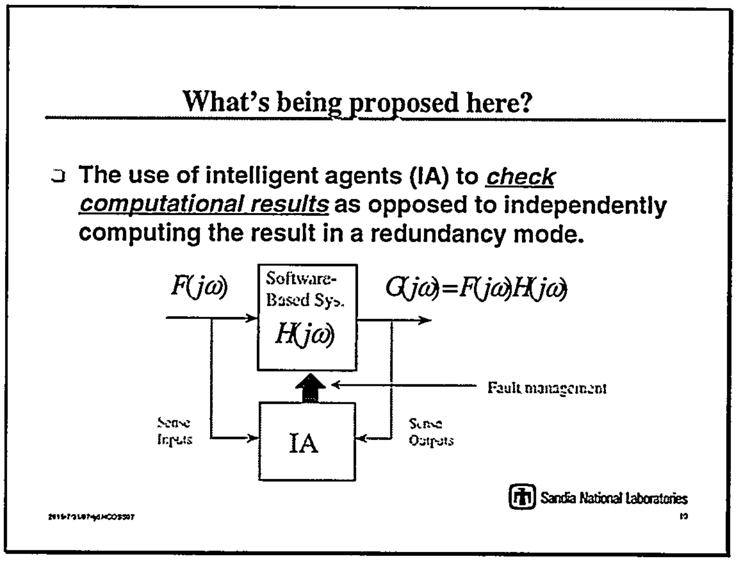
System with transfer function $H(j\omega)$

Sandia National Laboratories

[illegible]

9

Slide 10



What's being proposed here?

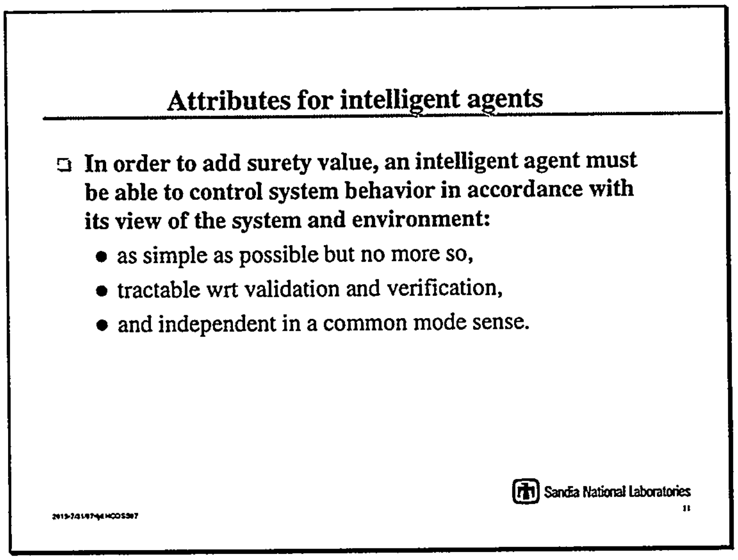
- The use of intelligent agents (IA) to ***check computational results*** as opposed to independently computing the result in a redundancy mode.

Sandia National Laboratories

[illegible]

10

Slide 11



Attributes for intelligent agents

❑ **In order to add surety value, an intelligent agent must be able to control system behavior in accordance with its view of the system and environment:**

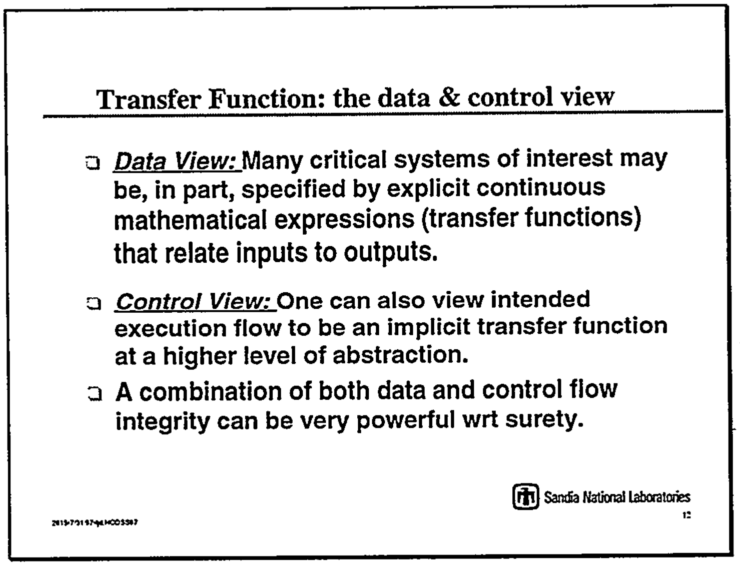
- as simple as possible but no more so,
- tractable wrt validation and verification,
- and independent in a common mode sense.

Sandia National Laboratories

11

[illegible]

Slide 12



Transfer Function: the data & control view

❑ ***Data View:*** **Many critical systems of interest may be, in part, specified by explicit continuous mathematical expressions (transfer functions) that relate inputs to outputs.**

❑ ***Control View:*** **One can also view intended execution flow to be an implicit transfer function at a higher level of abstraction.**

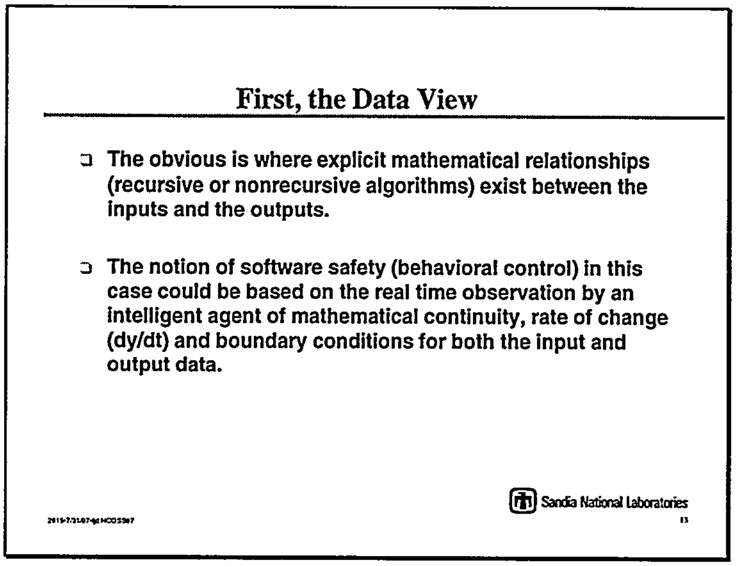
❑ **A combination of both data and control flow integrity can be very powerful wrt surety.**

Sandia National Laboratories

12

[illegible]

Slide 13



First, the Data View

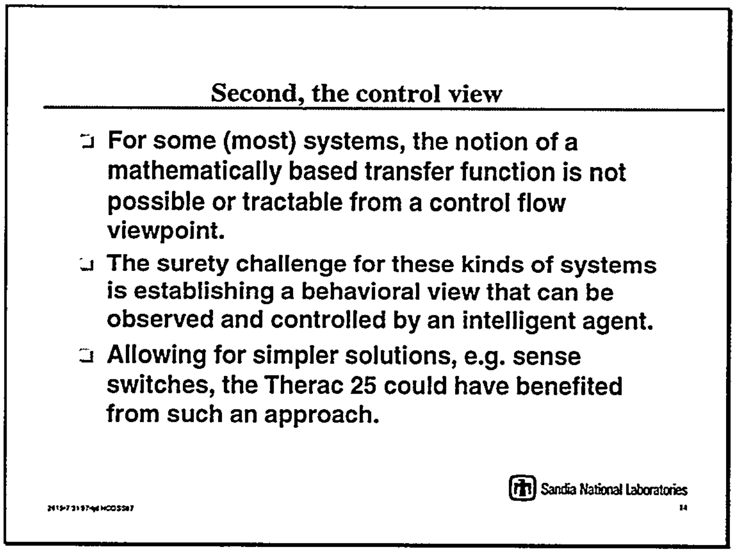
- The obvious is where explicit mathematical relationships (recursive or nonrecursive algorithms) exist between the inputs and the outputs.
- The notion of software safety (behavioral control) in this case could be based on the real time observation by an intelligent agent of mathematical continuity, rate of change (dy/dt) and boundary conditions for both the input and output data.

Sandia National Laboratories

2015-7/31/97-gd HCOSS97

13

Slide 14



Second, the control view

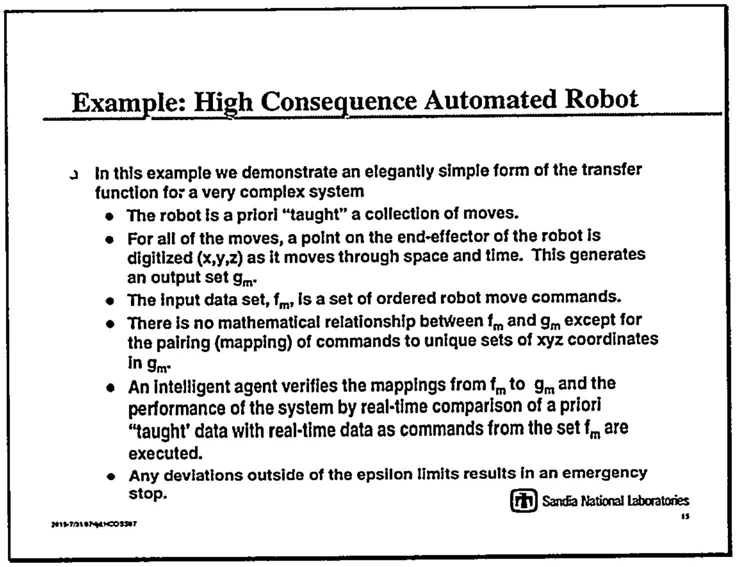
- For some (most) systems, the notion of a mathematically based transfer function is not possible or tractable from a control flow viewpoint.
- The surety challenge for these kinds of systems is establishing a behavioral view that can be observed and controlled by an intelligent agent.
- Allowing for simpler solutions, e.g. sense switches, the Therac 25 could have benefited from such an approach.

Sandia National Laboratories

2015-7/31/97-gd HCOSS97

14

Slide 15



Example: High Consequence Automated Robot

□ In this example we demonstrate an elegantly simple form of the transfer function for a very complex system

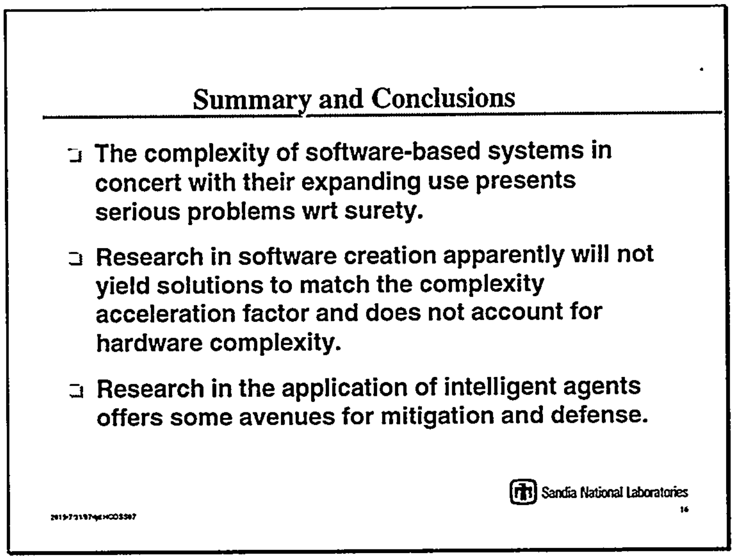
- The robot is a priori "taught" a collection of moves.
- For all of the moves, a point on the end-effector of the robot is digitized (x,y,z) as it moves through space and time. This generates an output set g_m.
- The input data set, f_m, is a set of ordered robot move commands.
- There is no mathematical relationship between f_m and g_m except for the pairing (mapping) of commands to unique sets of xyz coordinates in g_m.
- An intelligent agent verifies the mappings from f_m to g_m and the performance of the system by real-time comparison of a priori "taught' data with real-time data as commands from the set f_m are executed.
- Any deviations outside of the epsilon limits results in an emergency stop.

Sandia National Laboratories

15

2615-7/31/97-jd-HCOS597

Slide 16



Summary and Conclusions

□ The complexity of software-based systems in concert with their expanding use presents serious problems wrt surety.

□ Research in software creation apparently will not yield solutions to match the complexity acceleration factor and does not account for hardware complexity.

□ Research in the application of intelligent agents offers some avenues for mitigation and defense.

Sandia National Laboratories

16

2615-7/31/97-jd-HCOS597

Implementation of Non-Linear Programming Techniques For Solving the Optimization and Surety Problems of Gas Transfer Compressor Stations

G.S. Klishin
V.E. Seleznev
V.F. Chuchko
Russian Federal Nuclear Center (RFNC)-All-Russian Research Institute
of Experimental Physics (VNIIEF)
Russia

According to official information, more than a quarter of the world's explored natural gas resources are concentrated in Russia. The Russian gas pipeline network is long and complicated; considerable amounts of the gas extracted and electric energy are being spent to deliver gas from the field to customers along the pipelines. That is why the task of the optimum gas transportation is extremely important both from a strategic point of view, as well as for the present day.

State-of-the-art techniques of mathematical simulation allow creating optimized models of the failure-free control of main pipelines, compressor stations and their complexes. At the highest level, these models are described with the help of mathematical graph theory categories. This approach lets us reduce the expenditures on gas transportation along the gas pipeline network and its distribution among customers.

At the lowest level, the task of optimum load distribution among the gas transfer units of a compressor shop is being considered. One compressor shop can comprise three to seven units that are joined with the help of the pipelines following parallel and combined parallel-series scheme. One compressor station has two to six compressor shops.

It is assumed that a compressor shop can be equipped with different gas transferring units. It is supposed that even though the shop is equipped with only one type of gas transfer unit, the units may actually differ in performance. Figure 1 shows a typical scheme of a compressor shop.

One of the dangerous emergency situations that can occur during gas transportation through a compressor station is the surge of a compressor of a gas-transferring unit. A compressor surge is a process of pietistic fluctuations and variations of the gas flow in the compressor of a gas transfer unit. A surge appears when the operation characteristics of a compressor go out of the limits of the stable performance range.

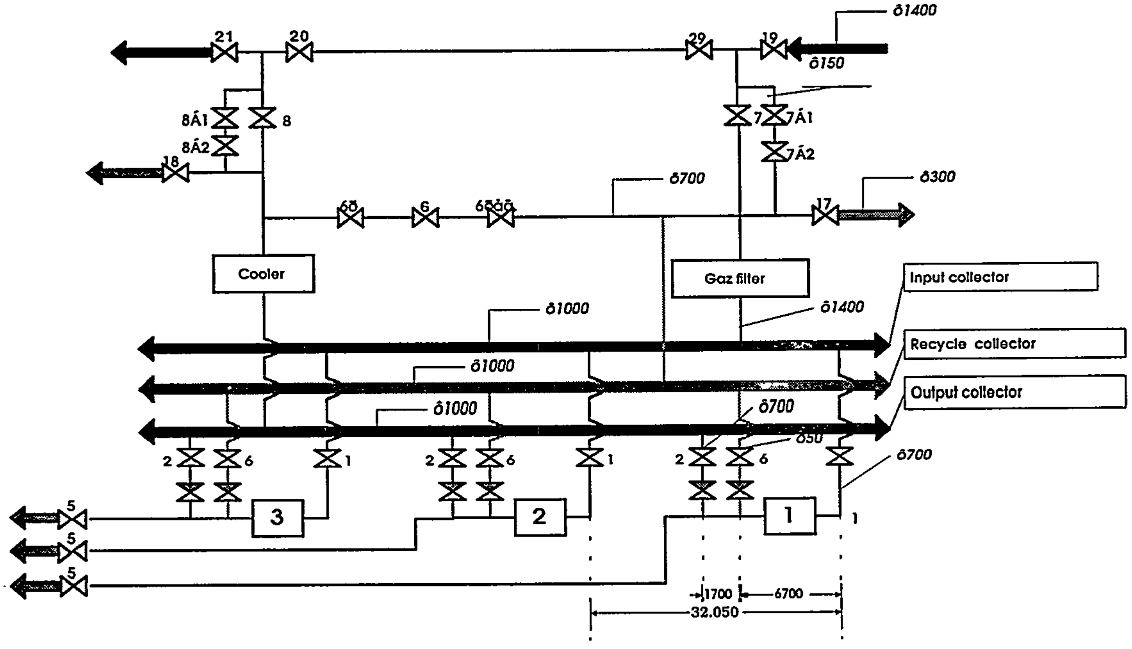


Figure 1. A typical scheme of pipeline intersection in a compressor shop (CS).

It is acceptable to depict an instant ratio of the parameters that characterize the operation of the compressor as a working point in a system of axes "compression rate-flow rate-frequency of the roller rotation." An example of the depiction of the working point of the blowing in such a system of axes is shown in Figure 2.

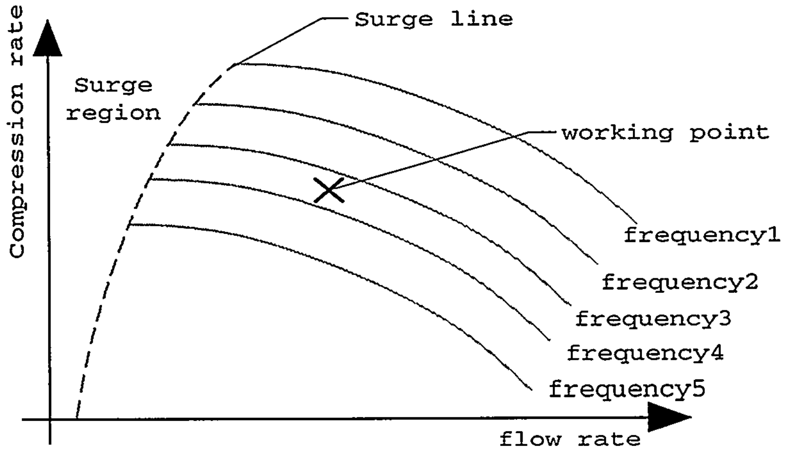


Figure 2. Blower operating characteristics.

Surge leads to the destruction of the normal operating mode of the system "a compressor - a pipeline" and the reduction of its lifetime or destruction of the equipment.

The power of the gas transferring units at the main pipelines is 6-25 MW. Fluctuations of the gas pressure in a compressor during a surge can reach comparable values. As a result of this, great forces, which can be varied in time and space, affect the compressor components. These forces cause a vibration of the construction and can lead to the destruction of the expensive gas transfer unit, auxiliary equipment, the pipelines, and a fire. As it is clear from Figure 2, to have surge-free operation of the system "a compressor-attached pipelines" it is necessary not to let the working point "fall" on the line of the surge limit.

For this, it is possible either to reduce the degree of compression or increase the gas flow through a system "a compressor-attached pipelines" or to reduce the frequency of rotation of the compressor roller. It is worth noting that the first two steps in the influence on the system are done with the help of the recycling channel. The area of the recycle channel intersection is controlled with a recycle valve. Opening of the recycle valve is done automatically with an anti-surge controller (Figure 3).

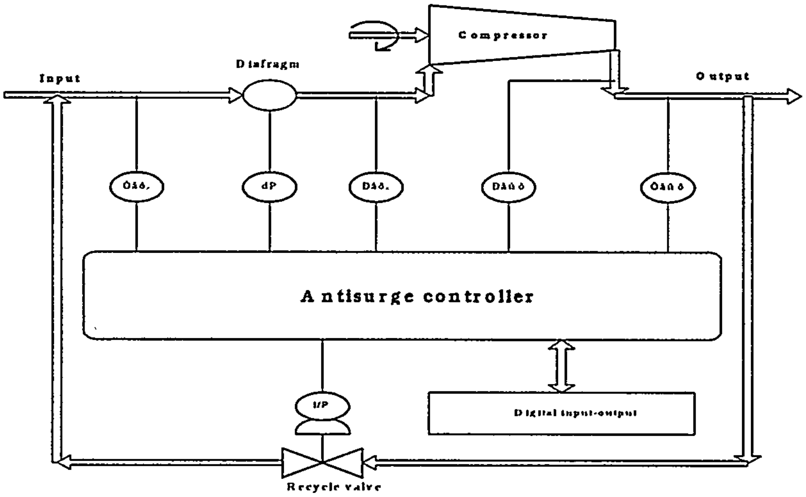


Figure 3. A schematic of the automatic control of the recycle valve.

An algorithm of the automated control of the valve opening can be developed with the help of the computer surge simulation, for example.

To investigate the behavior of the "a compressor-attached pipelines-a recycle valve" system, appropriate mathematical simulations were created. A schematic of the system being simulated is shown in the Figure 4. Gas flow in the pipelines is being described by the Sen-Venan-Vencile equations. To simulate gas transport through a compressor a Stepanov gas dynamic model is implemented.

Designations: J_i, K_i, S_i - accordingly gas flow rate, degree of opening of valves, squares of pipeline cross sections (input pipeline (i = 1), output pipeline (i = 2) and recycle pipeline (i = 3)): J - flow rate through compressor;

P_I, T_I - input parameters of system; P_{II} - output pressure.

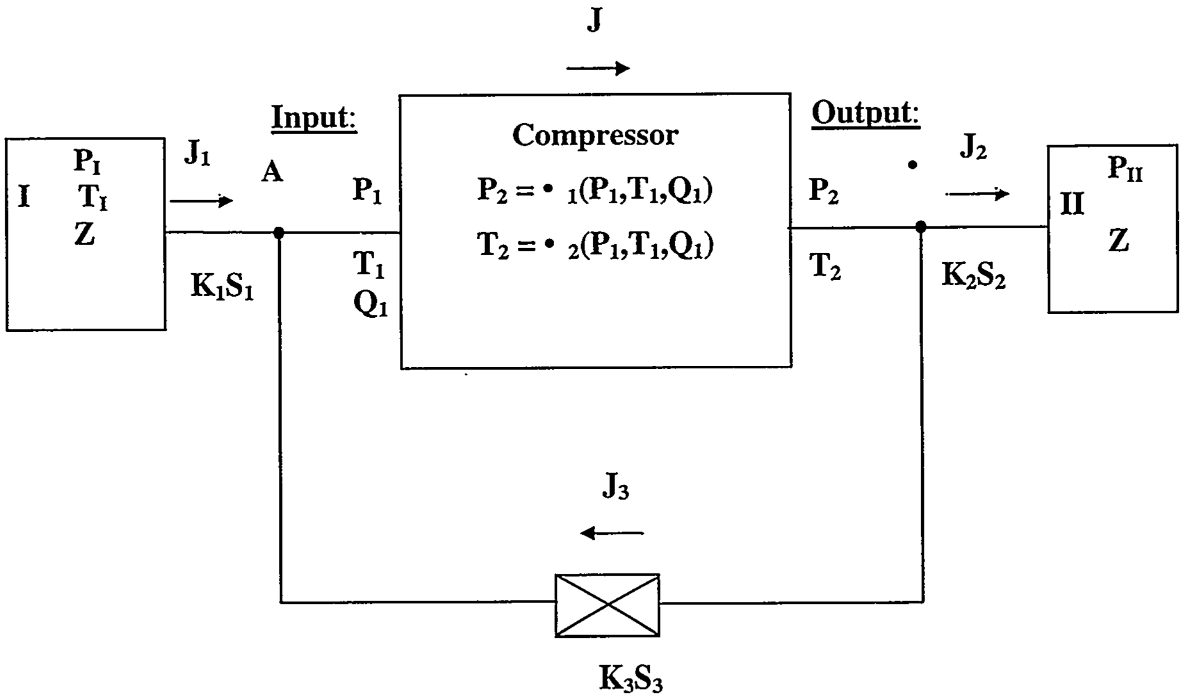
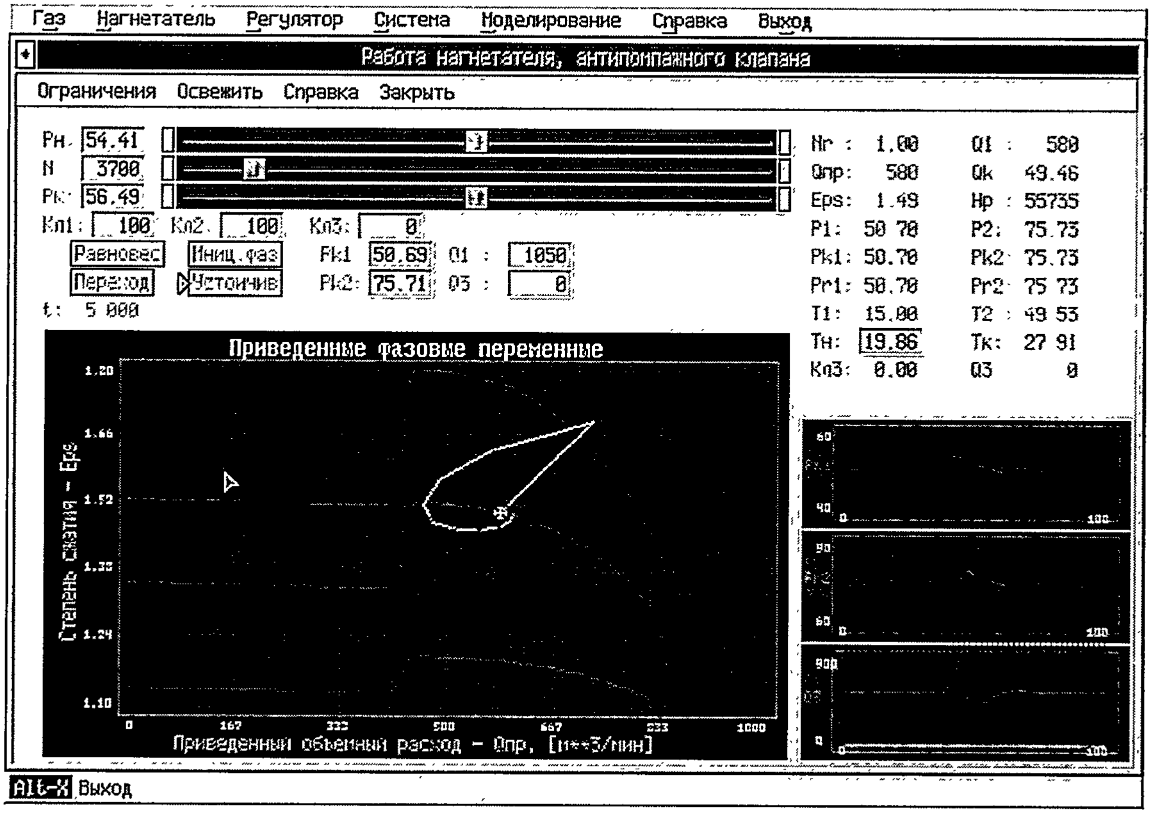


Figure 4. A schematic of the system being simulated.

Parameters of the natural gas in the system are found by solving a system of non-linear algebraic equations. Values of the functions in the equations are defined both analytically and numerically. Surge phenomena were investigated with the help of the mathematical model based on the non-stationary gas dynamic ratios, where the system under simulation was symbolically presented as a system with concentrated parameters.

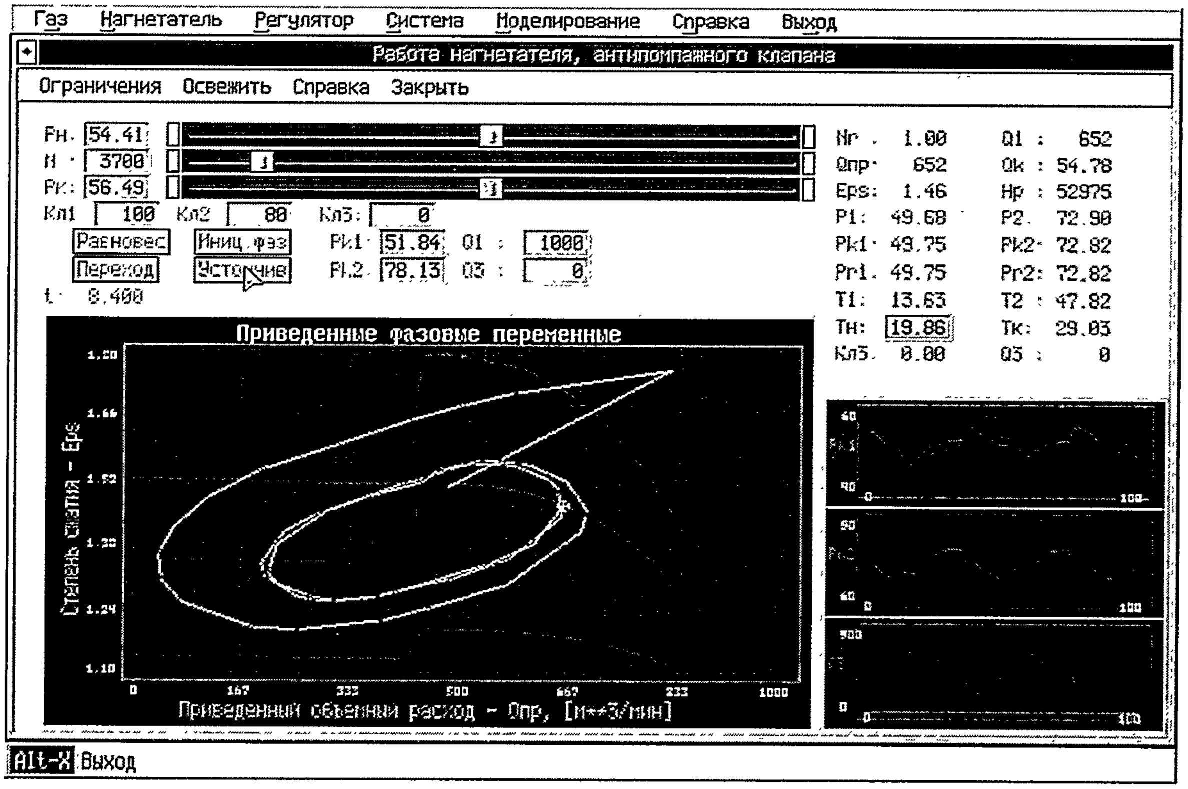
A surge simulation in this case comes to the numerical analysis of the system of ordinary differential equations having given edge conditions in accordance with the quality theory of differential equations. This allows assessing the stability of the system working point position (see Figure 2) or the character of the surge, giving the forecast of the accident situation development. The examples of the surge phenomena investigation of the units are shown on Figures 5 and 6.

A requirement for surge-free operation of a gas transfer unit is one of the main ones that limit minimizing gas transportation costs through the compressor shop and a compressor station in general. As a criterion for the optimum **load distribution among gas transfer units we determine the minimum flow of the fuel gas (in case the gas-turbine driver is used) or electric power (in electric driven case) that still allows the required pressure or a flow of the transported gas in the common collector out from the compressor unit, with simultaneously existing restrictions on the safe functioning of the shop equipment (requirements for no centrifugal blower surge, drive operation limitations and others).**



```
Pн. 54.41                                        Nr :   1.00     Q1 :    580
N    3700                                        Qпр:    580     Qk    49.46
Pк: 56.49                                        Eps:   1.49     Hp :  55735
Кл1:  100  Кл2.  100   Кл3:    0                 P1:   50 70     P2:   75.73
                     Pk1  50.69  Q1  :  1050     Pk1:  50.70     Pk2:  75.73
                     Pk2: 75.71  Q3  :     0     Pr1:  50.70     Pr2:  75 73
t:  5 000                                        T1:   15.00     T2 :  49 53
                                                 Tн:   19.86     Tк:   27 91
                                                 Кл3:   0.00     Q3        0
```

Figure 5. Stable equilibrium system state.



```
Pн. 54.41                                        Nr .   1.00     Q1 :    652
N ·  3700                                        Qпр·    652     Qk :  54.78
Pк: 56.49                                        Eps:   1.46     Hp :  52975
Кл1   100  Кл2    80   Кл3:    0                 P1:   49.68     P2.   72.90
                     Pk1· 51.84  Q1  :  1000     Pk1·  49.75     Pk2·  72.82
                     Pk2. 78.13  Q3  :     0     Pr1.  49.75     Pr2:  72.82
t·  8.400                                        T1:   13.63     T2 :  47.82
                                                 Tн:   19.86     Tк:   29.03
                                                 Кл3.   0.00     Q3 :      0
```

Figure 6. Hard mode of the excitation of the surge.

The following initial data are used:

- A scheme of the connection of the gas transfer units in a shop;
- A scheme of connection of compressor shops with a linear part of the main pipeline;
- Actual and passport parameters of the gas transfer unit;
- Values of the pressure or the flow rate in the common collector at the out of the compressor station.

While solving the task, the following must be observed:

- Limitations on the position of the working point on the compressor characteristics must be observed, they are related to the requirements on the surge-free operation (during calculations with the help of the methods described above, the stability of the working point position at every step of the optimization task solution is being evaluated);
- A design of the compressor station equipment and peculiarities of the natural gas transportation process through a compressor station are taken into consideration.

As undependable alternating signs of the optimizing signs the following is accepted:

- Natural gas parameters at different parts of the units and equipment that influence the position of the working points on the compressor characteristics;
- The position of the taps that define the configuration of the pipe intersection of the compressor shops and compressor station in general.

So, the task of the load distribution among the gas transfer units of the shop can be put as the task of the search of the minimum of the purpose function of many alternatives (Figure 4). As a purpose function, a total flow of the energy carrier to provide the necessary mode of the natural gas transportation is taken. A minimization process lies in the search of the positions of the working points of the gas transferring units that secure this mode. Values of the purpose function and limitations functions are defined numerically. To define them, numerical methods of non-stationary gas dynamics and a theory of a qualitative analysis of the ordinary differential equation systems are implemented.

A Formulation of the Task of the Optimum Control

It is necessary to minimize the purpose function of the costs changing the parameters of the control $\bar{X} = (N_1,\dots,N_n,K_1,\dots,K_m)^T$, having the given changes of the external factors - $\bar{A},\bar{B}$. At the same time limitations concerning the position of the working point of each compressor of a gas transferring unit must be observed:

$$\min \grave{I}_{\hat{E}\ddot{O}} : R^{n} \rightarrow R^{1}, Q = \left\{ \bar{X} \,\middle|\, \bar{A} \le G\left(\bar{X}\right) \le \bar{B} \right\},$$

$$\bar{X} \in Q \subset R^n, \bar{A}, \bar{B} \in R^n,$$

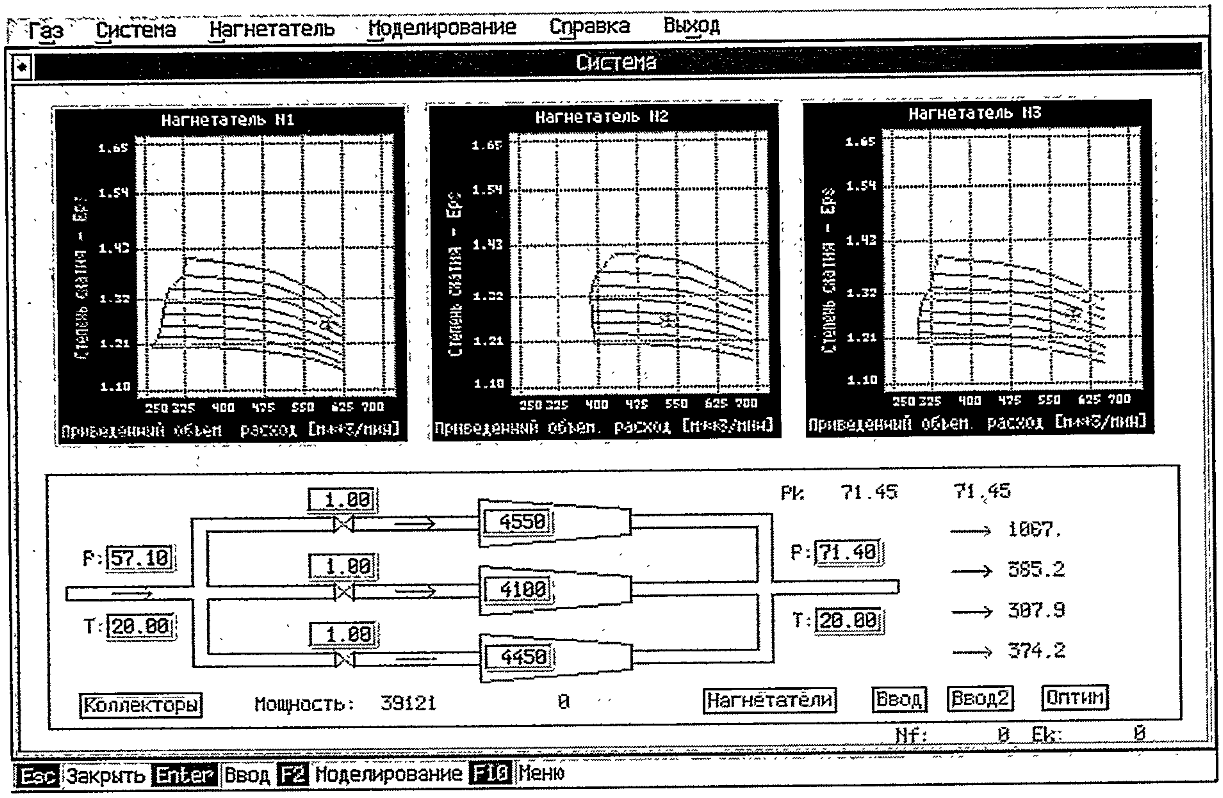
where $G(\bar{X})$ is the given function.

To solve the task set, there were implemented different combinations of the algorithms of the search the minimum of the non-linear purpose function at non-linear limitations that are based on well-known methods:

- The multiplier method;
- The linearization method;
- The Topkis-Veinot method;
- The variable metrics method and others.

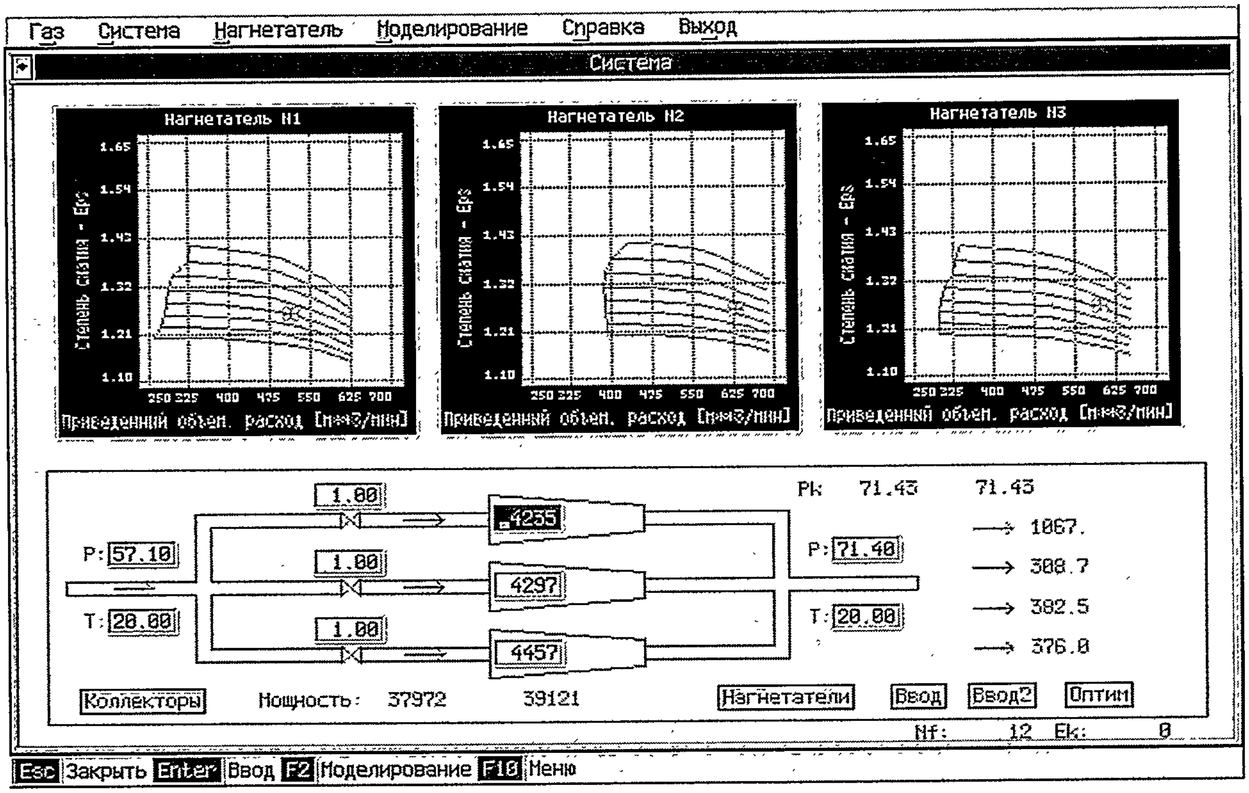
In case the solution obtained is not the point of the extreme of the purpose function because of the applied limitations, than the algorithms of minimization enumerated above will allow assessing the influence of each limitation on the absence of approximation to the purpose function extreme. Taking into consideration that every limitation is connected with technical parameters of the system or technological characteristics of the gas transportation process, there appears a real opportunity for mathematical analysis of the system operation and working out recommendations to improve in an optimal way.

Algorithms of the optimal surge-free control were developed using discussed approaches. These algorithms are implemented both for the analysis of the specific compressor stations operation and for the development of the algorithms of the computer-controlled, surge-free operation of the control equipment that is being created in VNIIEF for the gas industry. An example of the numerical simulation of the compressor shop operation of the compressor station “Morkinskaya” of the “VOLGOTRANSGAZ” subsidiary is shown in the Figures 7 and 8. In the example,”3” is a three per cent reduction in the energy costs calculated for one shop only.



P: 57.10
T: 20.00
1.00
1.00
1.00
4550
4100
4450
Pk: 71.45 71.45
P: 71.40
T: 20.00
→ 1067.
→ 585.2
→ 387.9
→ 374.2
Мощность: 39121 0
Nf: 0 Ek: 0

Figure 7. Initial position in an example.



P: 57.10
T: 20.00
1.00
1.00
1.00
4235
4297
4457
Pk 71.43 71.43
P: 71.40
T: 20.00
→ 1067.
→ 388.7
→ 382.5
→ 376.0
Мощность: 37972 39121
Nf: 12 Ek: 0

Figure 8. Final position in an example.

Biography

Biographies not available.

Intentionally left blank

Software Construction Techniques for (Ultra) High-Assurance Systems

Victor L. Winter
Sandia National Laboratories*
Albuquerque, New Mexico

The High Integrity Software (HIS) program at Sandia National Laboratories is developing tools and techniques to assist in the construction of software for (ultra) high-assurance systems. AST, an acronym that stands for Abstraction, Synthesis, and Transformation, is a formal method that is being developed within HIS.

For certain classes of problems (e.g., *single-agent* reactive systems), AST can be effectively used to automate a significant portion of the software construction and verification process. Furthermore the impact of human involvement in this phase of software construction can be controlled (i.e., limited) to such an extent so as to be (formally) verifiable.

In AST, software construction begins with synthesis in a multidimensional state space. The goal of synthesis is to construct abstract algorithmic solutions to problems from nonalgorithmic specifications (e.g., precondition and postcondition pairs). This is accomplished by using a sophisticated search engine such as an automated reasoning system to resolve (or remove) the nondeterministic choices that are present in the initial nonalgorithmic specification. In practice, the state space of real-world problems generally tends to overwhelm the capabilities of deductive synthesis techniques. In response to this difficulty, abstractions on the problem state space are used to assist synthesis in algorithm construction. In this framework, synthesis is then distributed over an abstraction hierarchy.

Complementing the abstraction and synthesis phase, refinement transformations can be applied (1) to optimize solutions that are obtained in the synthesis step, and (2) to introduce low-level (e.g., machine oriented) algorithmic details for the purpose of (ultimately) producing a machine executable implementation.

Biography

Victor L. Winter received his Ph.D. from the University of New Mexico in 1994. His dissertation research focused on proving the correctness of program transformations. Currently, Dr. Winter is a member of the High Integrity Software (HIS) program at

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

Sandia National Laboratories. His research interests include trusted software, formal semantic models (graphical-based and symbol-based), theory of computation, automated reasoning and robotics. Dr. Winter can be reached by phone in the United States at (505) 284-2696 or by email at *vlwinte@sandia.gov*.

Ensuring Critical Event Sequences in High Integrity Software by Applying Path Expressions

Marie-Elena C. Kidd
Sandia National Laboratories*
Albuquerque, New Mexico

Abstract

The goal of this work is to extend the use of existing path expression theory and methodologies to ensure that critical software event sequences are maintained even in the face of malevolent attacks and harsh or unstable operating environments. This will be accomplished by providing dynamic fault management measures directly to the software developer and to their varied development environments. This paper discusses the perceived problems, a brief overview of path expressions, and our proposed extension areas. We will discuss how the traditional path expression usage and implementation differs from our intended usage and implementation.

Introduction

The path expressions work presented in this paper is part of the Systems Immunology™ Track of the High Integrity Software (HIS) Project. The High Integrity Software project is part of the Strategic Surety Backbone of the Defense Programs Sector at Sandia National Laboratories. Although our funding and initial focus stems from defense applications, our methods will be applicable to the general high-integrity software developer.

Initially, our work will focus on path expression extensions in single processor environments and for fault detection. If our methods prove valuable, we will extend them to distributed environments and fault correction. We are currently in the early phases of applying our initial methods to real-world software projects. Another initial interest is methods that the user manually embeds in his or her software models and code. We will later concentrate on adding the extensions to the software development environment through compilers, assemblers, and modeling tools. It is important to point out that since high-integrity software is often embedded software, the compilers are often cross-compilers from a high-level programming language like C to a target processor assembly

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

language like 8051 or 68020. Also, assembly language is, at times, the only programming language used. So, our methods must be general enough to work in these varied environments.

Perceived Challenges and Problems

A major concern when developing high-consequence software is ensuring the integrity of critical event sequences. The system must be able to execute correctly, safely, and reliably even in the face of faulty hardware or software, external malevolent forces, and environmental stimuli such as lightning strikes or static. If, for example, the program counter gets corrupted, the software should not "music box" through the code from the failure point. Currently, no formalized methods exist to handle this problem. As a result, many ad-hoc methods are employed. The result is often the injection of more bugs into the software, sometimes hard to maintain software, and increased complexity.

Within Sandia National Laboratories, a recurring informal method has been used. It consists of creating a set of variables that holds information describing what events have occurred at any point in the execution of a software program. Some schemes simply assign a numeric value to each critical output event. Usually, the numeric value is derived in real-time during execution, but sometimes it is simply assigned to the variable. This is a creative and manual process done by the software developer and embedded in the code. The methods for matching an event with a value or figuring out which bits to attach to an event are mainly cleverness and trial and error. The author was part of one such effort. Clearly, a need exists for more reliable and easily employed methods for ensuring critical software event sequences in harsh and unstable environments.

Figure 1 provides an example where the sequence of events is important. Following is the sequence of events involved in making a plain cup of instant coffee. First you heat the water. When the water boils, you mix in the coffee. Then, you must wait for the beverage to cool to a temperature that is safe for consumption. There is a minor safety problem if the cooling stage is skipped. If you got distracted at just the right moment, the result might be that you burn your tongue.

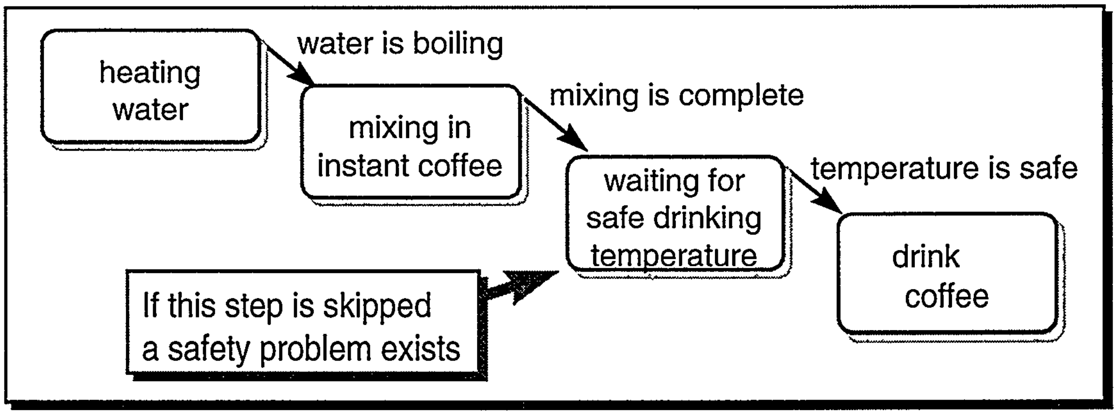


Figure 1. Example of an event sequence.

The analogy can be extended to a high-consequence computer-based system having a problem such as being hit by lightning or the hardware malfunctioning leading to a critical event being skipped. In that case rather than a burned tongue, the resulting safety problem may be the death of many innocent people.

Our work will take the informal, ad-hoc "methods" and apply existing computer science theory to create a more formal and reliable method for ensuring software event sequences. A method to attach timing to the events will also be explored. The mathematical and logical formula research may also be applicable to output signal integrity.

Introduction to Supporting Computer Science Theory

In order to understand path expressions, it is first necessary to understand its theoretical basis. Therefore, a brief refresher on finite automata and regular expressions will be addressed before discussing path expressions.

Finite Automata Basics

The review information in this section is derived from Reference 5.

A Finite Automaton (FA) is defined as a quintuple involving states and input values.

FA = $(Q, \Sigma, \delta, q_0, F)$.

- Q is the finite set of states.

Σ is the finite input alphabet.

δ is the transition function mapping $Q \times \Sigma$ to Q such that the signature of the transition function is: $Q \times \Sigma \rightarrow Q$. Using function notation, this is $\delta(q_i,a) = q_j$. This means, when in state q_i, which is an element of Q, with input a, which is an element of Σ, the resulting state, q_j, is given by the transition function, δ. Another way to describe this is that the transition function takes each possible state and input pair and defines the resulting state.

- q_0 is the start state (also known as the initial state). And, $q_0 \in Q$, which means q_0 is an element of the set of states, Q.
- F is the finite set of final states. And, $F \subseteq Q$, which means the final states, F, is a subset of the set of states, Q.

Two standard representations for finite automatons are transition diagrams represented as directed graphs and transition tables. Figure 2 displays a finite automaton in the form of a transition diagram represented as a directed graph. Notice that the circles represent states and the arrows represent elements of the input alphabet. Final states are often marked with a double circle.

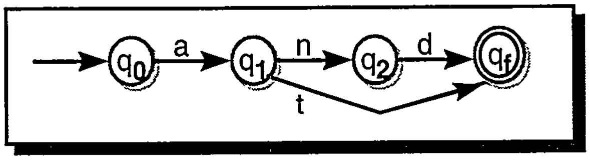


Figure 2. Example of a finite automaton.

Table 1 is the transition table associated with the transition diagram. Notice this example allows only "*and*" and "*at*" as acceptable input strings. This means that the "language," or set of strings, accepted by this finite automaton consists of "*and*" and "*at*" and nothing else. A string is accepted only when the finite automaton finishes in a final state.

Table 1. Example of a Transition Table

states in Q	inputs in Σ			
	a	n	d	t
q_0	q_1	∅	∅	∅
q_1	∅	q_2	∅	q_f
q_2	∅	∅	q_f	∅
q_f	∅	∅	∅	∅

One could visualize the input to a finite automaton as an input stream, perhaps written on a tape that arrives and is read by a reading head. As the input stream is read one character at a time, the transition diagram or table executes based on the input symbols. This is pictured in the sequence in Figure 3. Highlighting the active state simulates the "execution" of one path through the finite automaton.

We have reviewed only the very basic area of finite automata. Indeed, there are more complex and advanced areas within automata theory. However, they are not necessary for our discussion of path expressions.

Regular Expression Basics

The review information in this section is derived from Reference 5. Regular expressions are simple expressions describing languages that are accepted by an associated finite automaton. For example, the previous section gave a finite automaton that accepts the set of input strings of the form *'a' followed by 'nd' or 'a' followed by 't.'* This is a longwinded way to describe a very simple expression. Regular expressions give us a simple and compact way to describe such expressions. Table 2 gives the basic syntax of regular expressions. A and B are sets to input symbols.

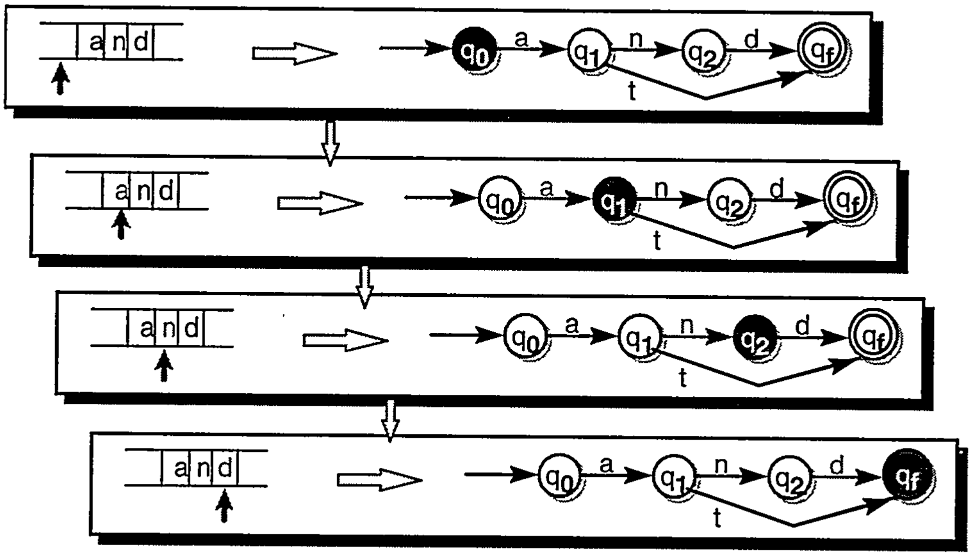


Figure 3. An execution path through a finite automaton.

Table 2. Regular Expression Syntax

Syntax	Meaning	Also denoted as:
A B	This is concatenation. It means A followed by B.	{x y I x is in A and y is in B}
A + B	This is selection. It means A or B, but not both.	{x I x is in A or x is in B}
A*	This is called Kleene Star or Kleene closure. It means 0 or more occurrences of A which is repeated concatenation.	$A^* = \bigcup_{i=0}^{\infty} A^i$
A^+	This is called positive closure. It means 1 or more occurrences of A. It is just like Kleene closure except that the minimum number of occurrences is one.	$A^+ = \bigcup_{i=1}^{\infty} A^i$
A^0	This is the empty string.	$\{\varepsilon\}$

In general, capital letters represent sets of strings and lower case letters represent set elements (strings). Here are some examples using regular expressions. Regular expressions may appear in terms of sets (capital letters) or elements (lower case letters). The "=" below is meant to mean "denotes the set."

Given A = {a} and B = {x, y, z}

- $\boldsymbol{AB}$ = {ax, ay, az}
- $\boldsymbol{x\,y}$ = {xy}
- $\boldsymbol{A^*}$ = {ε, a, aa, aaa,...}
- $\boldsymbol{A^+}$ = {a, aa, aaa,...}
- $\boldsymbol{A+B}$ = {a, x, y, z}
- $\boldsymbol{x}$ + y = {x, y}

Perhaps a more meaningful example would be to let A = {b, c} and B = {all, oat, at}.

- $\boldsymbol{AB}$ = {ball, boat, bat, call, coat, cat}
- $\boldsymbol{A+B}$ = {b, c, all, oat, at}

Here is an example of the sequence notation. Given that an average person is 60 years old, the life sequence they went through is birth then infancy then childhood and then adulthood. This could be described by the following notation: ***birth ; infancy ; childhood ; adulthood. An alternate notation is birth infancy childhood adulthood***. If we let b represent birth, i represent infancy, c represent childhood, and a represent adulthood then we can compress the notations above to ***b; i; c;*** **a** and ***b i c a***.

Here is an example of the selection notation. Common house pets are dogs, cats, reptiles, and fish. Given one common house pet, that pet is a dog, a cat, a reptile, or a fish. A notation is ***dog + cat + reptile + fish***. An alternative notation is ***dog | cat | reptile | fish***. If we let d represent dog, c represent cat, r represent reptile, and f represent fish then we can again compress the notations above to ***d + c + r + f*** and ***d | c | r | f***. Unless my understanding of animal classification is mistaken, this is true selection since a given pet can be exactly one of these types of animals with the odd cases of multiple inheritance aside.

Here is an example of the Kleene Star notation. Entering the world of "make believe," assume we have an infinite length freeway and an infinite number of automobiles. Each automobile has an associated driver. This freeway can hold zero automobiles, or one automobile, or two automobiles, . . . or an infinite number of automobiles traveling at once. Now, if we let A represent the set of all automobiles that can be on the freeway, we can represent the freeway activity as $\boldsymbol{A^*}$.

Here is an example of the repetition of 1 or more notations. We must remain in the world of "make believe" for this example. Given a functioning and infinitely large Emergency Room in a typical hospital, there should always be at least one physician on duty at all times. So, there will be one physician, or two physicians, . . . or an infinite number of physicians on duty at a given time. If we let A denote the set of possible physicians, we can represent this example as $\boldsymbol{A^+}$.

Again, we have only reviewed enough of regular expression theory to allow us to talk about path expressions. In compiler theory, regular expressions are expanded to cover very complex expressions and languages.

Path Expression Basics

A Look at Path Expressions

The following figure is a look at a basic path expression represented as a finite automaton via a directed graph. Interpreting the finite automaton produces the algebraic representation of the path, $a(bd + c(g^*)e)f$. This algebraic expression is a regular expression specifying all acceptable paths through the directed graph. This is also called a path expression since it expresses paths through the graph. This path set is interpreted as ***"a is followed by either b then d or a is followed by c followed by zero or more repetitions of g followed by e. Then, f comes last."*** Path expressions give us a more compact way to express the acceptable sequences just as regular expressions did in the earlier section. This example in Figure 4 depicts one of the many graphical models and notations found in the literature.

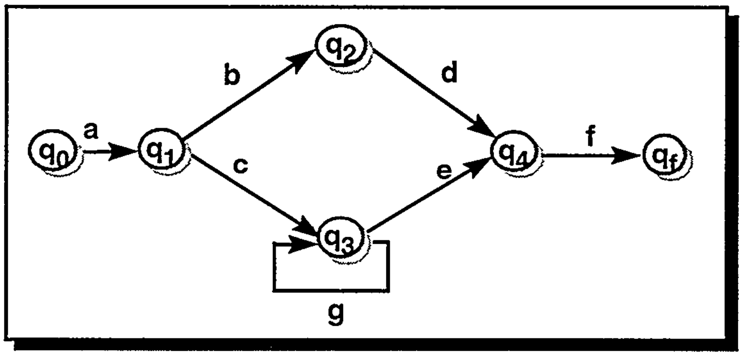


Figure 4. Example graphical representation of a path expression.

Path expressions are basically extended regular expressions that denote a specified set of paths through a graph where the graph depicts a model of flow through software code units. The uses of path expressions in the literature vary and will be discussed later in this paper. The notations found in the literature vary greatly and some with good reason. For simplicity and consistency, we will continue to use regular expression notation throughout this paper.

Current Related Path Expression Usage by Application Area

The literature on path expressions introduces many variations of path expressions. For example, regular path expressions were the first non-shuffle operator path expressions based on regular expressions and were used to describe synchronization relationships among processes sharing resources. Open path expressions were created to allow inherent unrestricted concurrency. Predicate path expressions extend regular path expressions to allow for a level of granularity beyond the process/module level and to add predicates to the decision process before performing an action. Generalized path expressions grew out of predicate path expressions and are mainly used in the verification and validation area. This list goes on.

However, for our purposes, the different ways in which path expressions are used is more important than the many specific versions of path expressions. Therefore, the term path expressions in this paper refers to the general class of path expressions except when a specific version is listed. We focus on the concurrent systems and verification and validation areas because their uses are somewhat similar to ours.

Concurrent Systems Usage

R. Campbell and A. Haberman originally introduced path expressions in 1974 to describe synchronization relationships and rules. Path expressions are initially based on regular expressions [3,4].

Traditional usage in the concurrent area, whether used on distributed processes or not, is based on synchronizing concurrent access to shared data. Resource allocation is the main objective. Furthermore, from the literature, it is clear that most traditional uses do not care about harsh environments that could throw the execution sequence "out of whack." Figure 5 depicts the general usage scenario.

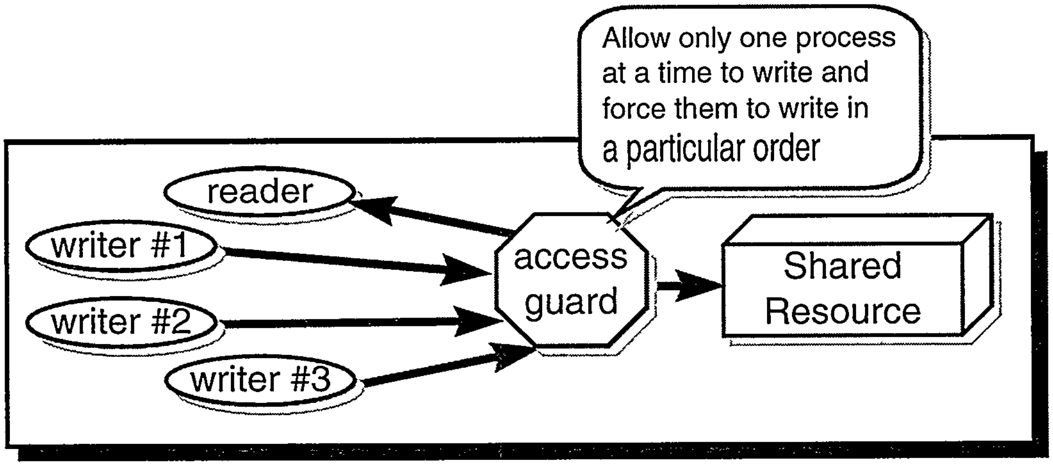

Allow only one process at a time to write and force them to write in a particular order
reader
writer #1
writer #2
writer #3
access guard
Shared Resource

Figure 5. Concurrent systems path expression usage scenario.

In this area, path expressions are derived during the analysis and design phases. They are then implemented, usually with semaphores or object oriented implementation constructs. Path Pascal and PPE ALGOL 68 [1] are programming languages that have been extended to include path expressions.

Verification and Validation (V&V) Usage

The software testing realm uses path expressions to optimize test case coverage and for creating external monitors.

Path expressions are used to select software test paths. The paths are derived from control flowgraphs of the software. Flowgraphs can be used at various levels of granularity and are based on the actual execution time flow of control through the software. A procedure for the conversion of a flowgraph into a path expression is given in the literature. Beizer has devised ways to determine the longest path, shortest path, and other specific paths through the software [2].

Another usage in the Validation and Verification area focuses on picking actual software paths and verifying that those paths occurred during execution as expected. Some methods actually implement an external path recognizer for this purpose. These methods are employed on single processor as well as distributed systems. Figure 6 shows this scenario.

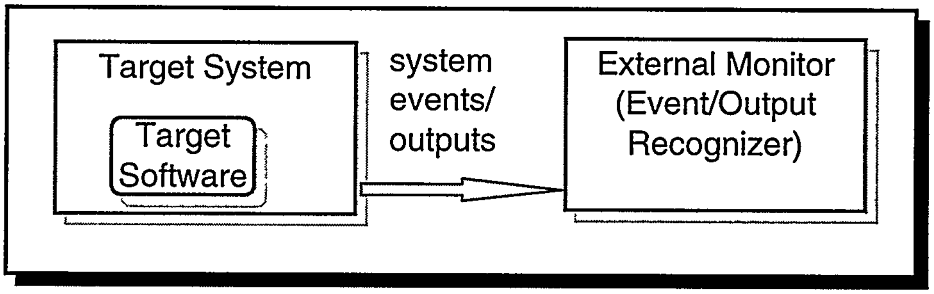


Figure 6. Verification and Validation path expression usage scenario.

Our Proposed Usage of Path Expressions

We are focusing on three main deployment methods for path expressions to ensure critical event sequences.

Path Expression Methods Implemented by the Developer

Path expression methods implemented by the developer consist of deriving path expressions from a software model and then embedding checkpoints and update points based on those path expressions into the target code. Extra software is added to the target code to verify that the correct event sequence is maintained. The granularity of the path expression is flexible and should be determined by the software requirements. Examples of appropriate software models are data flow diagrams, state-transition diagrams, and flowgraphs. All of these models chart out a type of software flow. It is the flow that path expressions will be used to enforce whether we are protecting an actual software path or a software sequence.

During the initial phase of our work, the focus will be on fault detection in the single processor environment. Later phases will deal with more complicated fault management issues and distributed processes.

Path Expression Methods in the Development Environment

Path expression methods may be embedded in the software development environment by placing them in compilers, assemblers, or other development tools. In this case, the software developer does not have to do anything extra because the compiler or other development tools do the work.

The two areas of interest are generic extensions to any language and language-specific extensions. In the language-specific area, languages like Path Pascal already exist. Extensions to Ada have also been made. However, these are for specific compilers and with quite different intents. The problem for embedded software is that other languages are used such as C or Assembly language. In these cases, the microprocessor used will dictate a subset of compilers, cross-compilers, or assemblers. Many compiler/assembler options exist and to add to the variability, commercial compiler/assembler companies constantly change their products and at times go out of business. We believe a generic set of extensions would be a superior method due to the variability and dynamic nature of the market.

Hybrid of Hardware Systems Immunology™ with the Above

The Digital Isolation and Incompatibility project, which is also part of the Systems Immunology™ track of the High Integrity Software project, is working on hardware solutions that are complementary to this work. They will provide hardware solutions that check path expression variables. Specific path expression values will enable hardware state machines that can check activity at the line-by-line of code level if desired. The hardware would then enable or leave disabled a specific hardware output based on the state machine.

This merger will handle situations where a software interlock or a hardware interlock alone is not enough protection to meet system surety requirements. One example of a threat requiring both methods is as follows: A system has software embedded in a microprocessor and at least one critical output; the operating environment has hazards that may corrupt the program counter in the microprocessor. Given that the microprocessor instructions vary from one to three bytes in length, if the program counter is corrupted it could "wake up" on the third byte of an instruction instead of the first byte.

Our Uniqueness in the Path Expression Area

Our Basic Goals

We seek to ensure critical sequence of events in unstable and harsh operating environments. Our usage of path expressions has two related, main goals. First, ensure critical event sequences with adjustable granularity. Second, provide software fault tolerance where the faults could come from the hardware, software, or the operating environment.

It may be possible to use the path expression derivation techniques from the V&V area with a flexible level of granularity (e.g. module level, object level, near line-by-line level) and to capture event sequence rather than path sequences.

The implementation techniques, however, will be different from the current implementation techniques in both areas. The implementation will consist of embedding checkpoints and update points into the target system code.

To help understand the different usage scenarios used by the concurrency area and our area, the following anthropomorphic questions may help. The basic question that is asked in a traditional concurrent path expression usage is, "May I have the shared resource now?" The answer is either, "Yes, continue" or, "No, wait until it is your turn." In our usage of path expressions, the basic question is, "Am I supposed to be here now based on order of events?" The answer is either "Yes, continue" or, "No, fail safe."

Event Sequence Expressions Versus Path Expressions

Our environment is more concerned with critical software event sequences than with the actual paths chosen between the events. Figure 7 shows an expansion of the basic path expression diagram into a path expression application. The nodes are now pieces of code that could be code fragments, objects, or entire modules. The inverted triangle is a checkpoint that could be thought of as a yield point. The large arrow is an update point that occurs after the critical output and will update the path variable appropriately. This method tracks the path that is taken to get to the events.

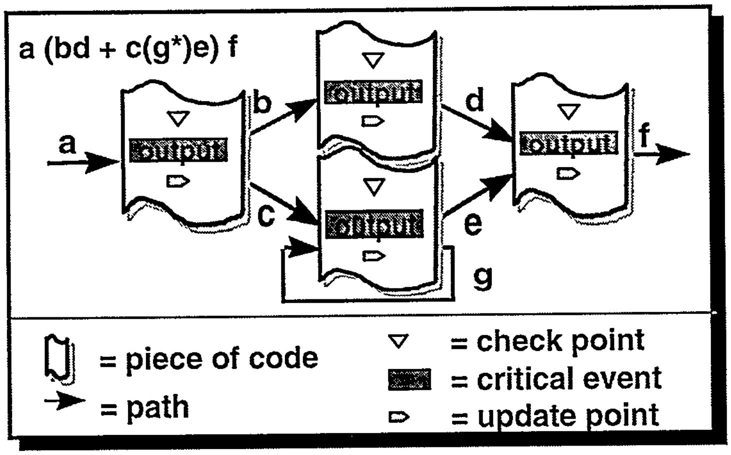


Figure 7. Our use of path expressions.

Another way of using path expressions is to use them as "event sequence expressions" where the event sequence is tracked rather than the path between the events. In Figure 8, the "event sequence expression" depicted is $a(b+c^{+})d$.

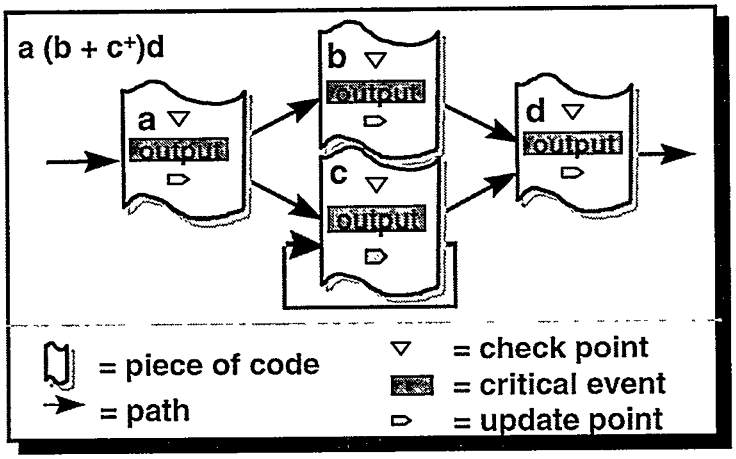


Figure 8. Our event sequence expression scenario.

Both path expressions and "event sequence expressions" use regular expressions as a foundation. The use of one or the other should be driven by what is appropriate for the software requirements. If the path is important, use path expressions. If the event sequence is important, use "event sequence expressions." These two methods are ways to derive the regular expression that will be tracked and implemented in the target code.

Path Formulas

Mathematical and logical formulas will be used to check and update path variables. Some guidelines for formula use are needed. Consideration for items such as the following will be considered: placement of check points and update points for path variables, reduction rules and state minimization, recursion, the arithmetic bounds of the processor, and synchronization issues.

Identification of Path Expression Usage in the Software Engineering Lifecycle

Consider the very basic software engineering lifecycle phases: requirements, design, and implementation. During the Requirements phase, path expressions will be derived from the analysis diagrams. During the Design phase, path expressions will be embedded into the design diagrams. Finally, during the implementation phase, path expressions will be embedded in the code as directed by the design. Figure 9 shows our usage scenario.

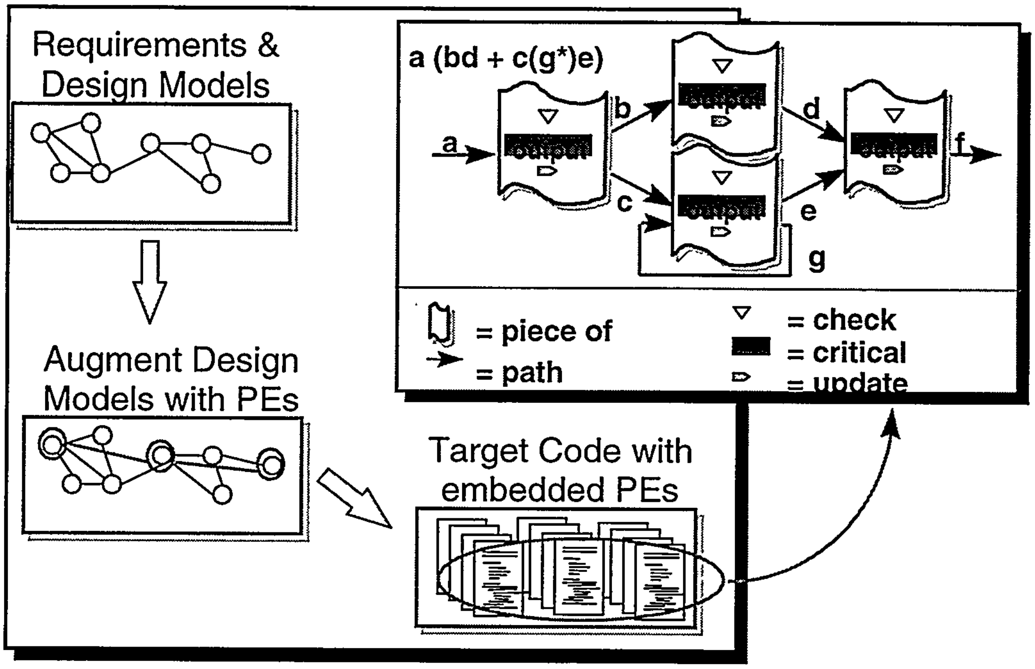

Requirements & Design Models
Augment Design Models with PEs
Target Code with embedded PEs
a (bd + c(g*)e)
a
b
c
d
e
f
g
output
= piece of
= path
= check
= critical
= update

Figure 9. Our path expression usage scenario.

The level of granularity of the event sequence is flexible. It should be the level that is appropriate to the surety requirement. This can be at the module level in some areas, above the module level in other areas, and even close to the line-by-line level in others. The similarity is that all monitoring with path expressions is internal to the code.

Conclusions

A major concern when developing high-consequence software is ensuring critical event sequence integrity. The system must be able to execute correctly, safely, and reliably even in the face of faulty hardware or software, external malevolent forces, and environmental stimuli. If, for example, the program counter gets corrupted, the software should not "music box" through the code from the failure point.

Currently, no formalized methods exist to handle this problem. So, many ad-hoc methods are employed. The possible results are introduction of more bugs into the software, sometimes hard to maintain software, and increased complexity.

Path expressions in software have been used to protect shared resources, optimize data base queries, for test case coverage optimization, and to create external test monitors. This work will extend their use to cover critical event sequence concerns in high consequence software. This is a unique extension set according to the literature and appears to be a reasonable and logical direction.

Upon completion of this work, the deliverable will be dynamic fault management methods through path expression extensions for ensuring critical event sequences in high-consequence software. These will be in the form of user embedded and compiler embedded methods. These methods will also work in distributed, multiprocessor environments.

References

1. Sten Andler, *Predicate Path Expressions: A High-Level Synchronization Mechanism,* Ph.D. thesis, Computer Science Department, Carnagie Mellon University, 1979.

2. Boris Beizer, *Software Testing Techniques*, Van Nostrand Reinhold, New York, 1990, Chapters 3 and 8.

3. Roy H. Campbell, A. N. Habermann, "The Specification of Process Synchronization by Path Expressions," Proceedings of an International Symposium on Operating Systems, Rocquecourt, France, April 1974. Lecture Notes in Computer Science, Springer Verlag, Vol. 16, pp. 89-102.

4. Roy H. Campbell, *PATH EXPRESSIONS: A technique for specifying process synchronization*, Ph.D. thesis, Computing Laboratory, The University of Newcastle Upon Tyne, Newcastle Upon Tyne, England, August 1976. Reprinted by the Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana, Illinois, May 1977.

5. John E. Hopcroft, Jeffrey D. Ullman, *Introduction to Automata Theory, Languages, and Computation*, Addison-Wesley, Reading, Mass. 1979.

Biography

Marie-Elena C. Kidd
Sandia National Laboratories
Albuquerque, NM 87185-0535 USA

Marie-Elena is a computer scientist and Senior Member of the Technical Staff at Sandia National Laboratories. During her ten years at Sandia, she has worked as a software engineer on embedded, real-time software systems for such applications as robotics, nuclear weapon components, and control systems. She has also worked on lab-wide information sharing software systems and software engineering initiatives. She has a B.S. in Computing and Information Sciences from Trinity University and a M.S. in Computer Science from Purdue University.

Intentionally left blank

The Software Engineering Journey: From a Naïve Past into a Responsible Future

Sharon K. Chapa, Ph.D.
Sandia National Laboratories*
Albuquerque, New Mexico

Abstract

All engineering fields experience growth, from early trial and error approaches, to disciplined approaches based on fundamental understanding. The field of software engineering is making this long and arduous journey, accompanied by evolution of thinking in many dimensions. This paper takes the reader along a trio of simultaneous evolutionary paths. First, the reader experiences evolution from a zero-risk mindset to a managed-risk mindset. Along this path, the reader observes three generations of security risk management and their implications for software system assurance. Next is a growth path from separate surety disciplines to an integrated systems surety approach. On the way, the reader visits safety, security, and dependability disciplines and peers into a future vision that coalesces them. The third and final evolutionary path explored here transitions the software engineering field from best practices to fundamental understandings. Along this road, the reader observes a framework for developing a "science behind the engineering" and methodologies for software surety analysis.

Introduction

True engineering consists of the tools and methods that allow practical application of a science. To use the term "software engineering" is a bit of a stretch, as today software development follows a best-practices approach, grown somewhat from early trial and error, but still a long way from the fundamental understandings that characterize a science. Engineering based on science requires a valid model of how things work, along with an understanding of computation and uncertainties. To use the term software engineering gives us a noble goal for which to strive. As the role of software in all aspects of our lives increases at an alarming pace, it is imperative to accelerate the journey which will lead us to fundamental understandings, i.e., the scientific foundations, and the tools and methods to employ them. The fundamental understandings will tell us how to relate controllable and measurable aspects of software products and processes to desired properties such as reliability. The engineering tools that accompany a science include analytic tools to measure deviation of a product from its design goals. Risk

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

analysis is the term used in this paper to represent the most general approach to computing to what degree desired software properties are achieved.

Software engineering faces some dangerous conditions stemming from its naïve past:

- Complexity is outpacing best practices
- Engineering is being practiced without science
- Existing risk analysis tools do not fit the software problem

Its responsible future depends on fulfilling urgent needs corresponding to the bullets above:

- Lifecycle tools which support better management of complexity, rationale, and change
- Scientific foundations for software reliability
- The right tools for software risk management

Moving beyond best practices will require significant developments in these areas.

In this paper, the reader travels three roads which form a part of the Software Engineering Journey from naïve past to responsible future. The responsible future on the horizon is a future where science-based analyses on processes and products are routinely used to achieve a quantifiable level of confidence in the software product. Road Number One, Security's Evolution, is of interest because it demonstrates how one discipline, security, is dealing with some very difficult paradigm shifts, and illustrates the importance of taking an effective viewpoint into a problem space. Road Number Two, Managing Risk in Multiple Dimensions, looks at approaches found in three disciplines (security, dependability, and safety) and presents a viewpoint which is useful for coalescing them into a coherent discipline called surety. Road Number Three, From Best Practices to Fundamental Understandings, introduces the emerging areas of software reliability science and risk-based software surety analysis.

Three Roads

Road No. 1.
Security's evolution from zero risk to managed risk

The computer security community has undergone an evolution of thought, which is presented here as a set of generations, each of which involves a significant paradigm shift. The community has been responding to a need to replace the traditional views of computer security and risk management with one that is broad, integrated, and useful for managing risk throughout the life of a software system. Later generations are more encompassing and tailorable than previous generations. Challenges facing the current generation include developing a broad-perspective security model, developing effective tools, and re-defining assurance to be based on measurable risk reduction rather than on compliance.

The first generation of risk management was compliance-oriented, requiring buy-in to a predefined set of risks which was assumed to apply to all systems. Mainframe computers and protection of classified information characterized this generation's environment, and risk concerns revolved around certain aspects of "CIA" (confidentiality, integrity, and availability). Notice that even this early set of risks hints at the intertwined nature of security and dependability. Not only was the set of risks fixed, but also the mitigation strategies were dictated to include access controls, encryption for network transmissions, and disaster recovery planning. Implicit in this approach was the belief that compliance eliminates risk. There was little leeway for customized, much less optimal, solutions. While restrictive, this approach succeeded in its environment. The first generation made assurance straightforward for the consumer and vendor: vendors' products were rated according to their compliance with the dictated mitigation strategies, and consumers selected target ratings according to a risk matrix which related data classifications and users' clearances. The picture was very compliance-oriented. Figure 1a illustrates the first generation.

The second generation sprung from difficulties with the first generation's emphasis on reference monitor access control and compliance. The advent of, first, networks, and then, distributed processing on those networks, was very problematic for the first generation risk mitigation approach. The techniques that had been adopted did not easily extend into these more modern environments. At the same time, there was growing concern that the first generation CIA risk model simply did not fit all applications; a need was felt for more system-specific risk assessment. Other fields, such as nuclear power and weapons, were taking a system view and using analytical risk analyses; their success provided encouragement for a risk-assessment approach. As a result of all this, a new view of security/dependability risk emerged for software systems, based on the following system components:

- Vulnerabilities
- Threats: active, passive
- Assets: data, hardware, software
- Impacts: disclosure, destruction, modification, unavailability
- Types of mitigation: avoid, transfer, reduce threat, reduce vulnerability, reduce impact, detect and respond, recover

This newer view of risk, illustrated in Figure 1b, says "A threat is realized through a vulnerability, which impacts an asset," and it recognizes a range of possible mitigation strategies. Little progress seems to have been made beyond these definitions, though, and this is due to two major roadblocks. First, an inability to measure the risk mitigation achieved by a design, and thus, to draw any conclusions about assurance. Second, lack of a coherent framework for integrating assessment of the various aspects of security and dependability, which is needed to assess tradeoffs in mitigation decisions.

While broader than the first generation's approach, this view is still limiting, because the concepts of impacts and assets do not encompass enough. This view seems to imply that the system is operating properly to begin with, and one need only prevent threats from being realized. This is still a fairly static view of systems; it does not lead the analyst to consider the full range of system lifecycle activities and states. It also fails to encompass the important progress being made on many fronts that contribute to dependable and secure software systems, such as software development and design methodologies, testing tools, new access control models, and requirements engineering. A general risk mitigation framework needs to be able to factor in the risk mitigating potential of these sorts of things as well. The second generation recognizes that simply complying with orders may not provide the needed surety, and its risk model represents a positive trend toward assessing a system's actual protection needs. However, assurance under the newer model is ill understood. Additionally, the model misses the opportunity to encourage the many emerging methodologies that contribute to sure systems. As long as there is not an assurance technique that credits good practices, developers will unfortunately sacrifice doing things right in order to apply scarce resources to doing those things that are measured.

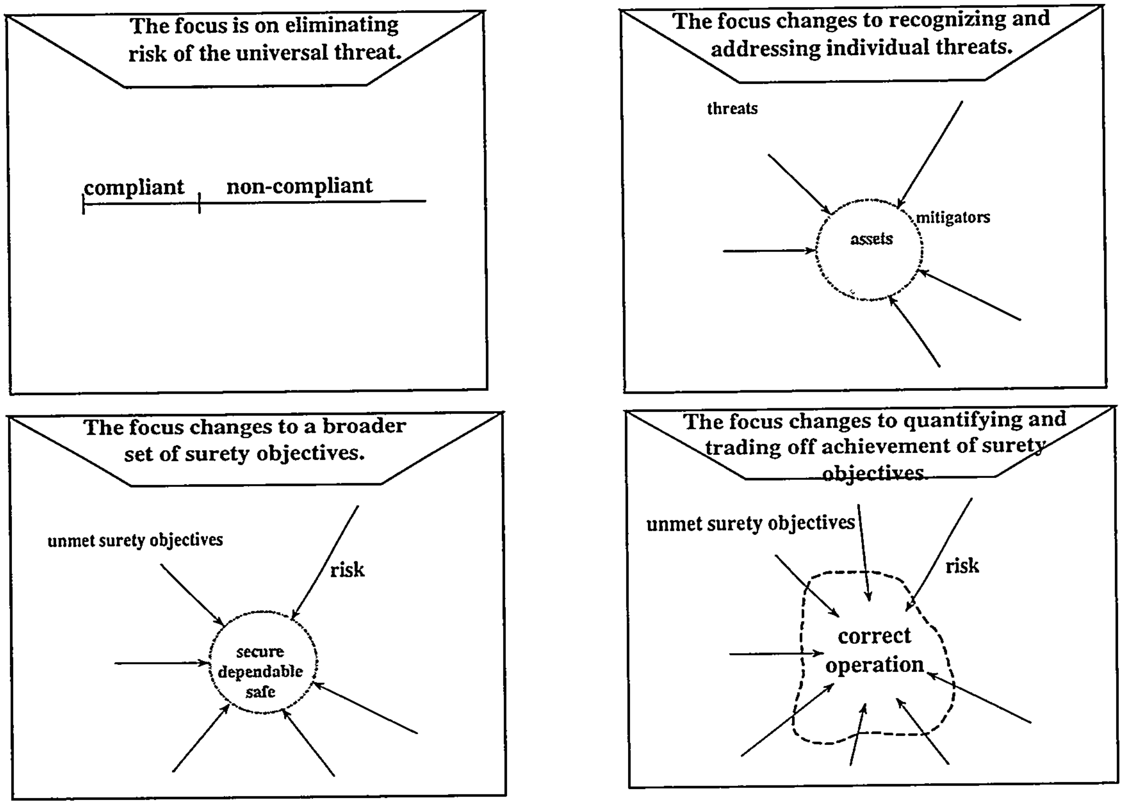

The focus is on eliminating risk of the universal threat.
compliant
non-compliant
The focus changes to recognizing and addressing individual threats.
threats
mitigators
assets
The focus changes to a broader set of surety objectives.
unmet surety objectives
risk
secure
dependable
safe
The focus changes to quantifying and trading off achievement of surety objectives.
unmet surety objectives
risk
correct
operation

Figure 1. (a) The security compliance approach assumes compliance equals zero risk. (b) The asset protection approach applies mitigation against threats to assets. (c) The managed risk approach drives down the risk of unmet surety objectives. (d) The balanced risk approach seeks an acceptable balance of risk.

The challenge before the community now is to move forward toward a third generation, with a new view that is broader than asset protection, and to develop a viable assurance approach there. The third generation requires adopting a new underlying perspective on risk and assurance. This perspective, this framework, this view into the problem space, will restrict the solutions one is able to see. Therefore, the framework must not reduce the problem to one of protecting assets, as this is simply too narrow, and must avoid kludging new ideas into a paradigm that is too narrow to do them justice. The third generation assurance mindset will encourage integrating the assessment of security with dependability and perhaps even safety. It will enable application of cost-effective measures commensurate with actual requirements. And it will allow for solutions that represent real surety as opposed to compliance. Third generation assurance will not be easy, but it could perhaps be based on degrees of risk-mitigation required along various surety dimensions for a system, as illustrated in Figure 1c.

Road No. 2.
Managing Risk in Multiple Dimensions: Safety, Security, and Dependability

In a software system, risk can have many disparate sources—faults, errors, hazards, abnormal events, unexpected environments, attacks, untimeliness, unavailability, the system development process, operational procedures, maintenance, and so on. Within the software community, separate disciplines have formed to address some of these risks, although not all have thought of their job as risk management. These disciplines include security, safety, dependability, and software engineering. Within each of these areas, there are even more specialized interests such as multi-level-security, communications security, asset protection, hazops, first principles, fault tolerance, database integrity, process maturity, testing, and configuration management. The words "risk management" conjure up very different ideas within these different interest groups.

Any single focus from the above list is clearly inadequate. Choosing a viewpoint on the problem is critically important for the problem viewpoint filters the solutions that one is able to see. Perhaps the most basic and encompassing viewpoint to take is that of **correct system operation**, achievable through an appropriate balance of all other concerns. This viewpoint can span the entire lifecycle, including the processes used for development, operation, and maintenance. It can also span all aspects of the system that might contribute to risk, such as its architecture, functions, information, interfaces, and environment. The risks to be managed can be described in terms of failure to achieve and maintain the appropriate balance of concerns, or surety objectives, for correct system operation. There is heavy interaction among risk mitigators in software systems; that is, measures applied to one objective will frequently impact others as well. Software, perhaps more than any other domain, suffers from inseparability of surety objectives, which is why an encompassing viewpoint is imperative. Three disciplines are discussed briefly below, to give a flavor for current approaches and mindsets. Then the idea of combining them under a risk-based approach is revisited.

A general, high-level approach to **safety** is to identify potential hazards in a system, and to select a protection level for each, based on a combination of probability and severity of the hazard. Protection levels can range from eliminating the hazard, to reducing it, to limiting the resultant damage. One approach to identifying hazards is to take a process view of the system. Another approach is to construct fault trees, event trees, or cause-and-effect diagrams. In any case, each hazard is analyzed for severity and probability of occurrence, which when taken together indicate the protection level that the designer should strive for. Often, there is a high-level system safety policy, or safety theme, that provides safety goals, values, and general approaches. Safety themes include such guidelines as independence to prevent common causes of failure, isolation to prevent accidental triggering of actions, and first principles that rely on the laws of nature (for example., gravity) as fail-safes. Specifying requirements related to software's role in the larger system safety design is important but difficult. Software engineering and system safety engineering are still relatively young fields. The combination of the two, that is, software safety, is in its infancy. However, developers of safety-critical software offer some general software design approaches that can make a positive, if not measurable, contribution to system safety.

The **security** need that has most influenced the computer marketplace is the need to protect classified information. The solution to this need was defined early on, in terms of a reference monitor, or kernel, which mediates all file accesses. This solution re-casts the problem as controlling accesses by subjects (processes, ultimately representing users) to objects (files). The computer security community is currently wrestling with the insufficiency of the above solution for today's environments. The solution cannot easily be extended to distributed, networked environments, and it only addresses a small part of the modern security picture. Today, intrusions, viruses, system integrity, and denial of service are major concerns. And it is arguable whether the reference monitor ever even solved the original problem, anyway, because processes accessing files are simply too narrow a part of the problem. Finer granularity of information, covert channels, inference, traffic analysis, and other forms of information flow were all left to be dealt with outside the basic reference monitor mechanism. It seems to be a case of failing to model the entire problem and instead addressing only that portion that could be neatly and formally modeled. While the historical security approach has instilled an attitude that security mechanisms can and should be pre-defined, formally modeled, and positively stated, this may not be possible in today's environment. It appears that approaches to some aspects of security may be swinging to the other extreme, totally adaptive and on-the-fly, because maybe the best that can be done is to recognize and swiftly act on intrusions, viruses, and leaks. Such ideas are a radical departure from the past. Software development and delivery processes are also receiving growing security emphasis. The goal is to eliminate opportunities for any person to subvert the software by inserting trapdoors, substituting other code, and so on.

Correctness is a primary component of software **dependability**. David Parnas suggests three complementary approaches for producing correct software: process, product, and testing. Process things include personnel certification and assessments of the software development process. Product things include examining the actual software product and related artifacts via inspections, reviews, requirements tracing, formal methods, and so on. Testing complements product review by exercising the software in its actual environment; this is still important because inspections and proofs necessarily make simplifying assumptions about the environment. An approach known as software reliability growth strives to reduce MTTF to a consumer-acceptable level, by concentrating on testing with expected operational profiles. But many argue that critical applications need a zero defects approach, as opposed to a reliability growth approach. Critical applications benefit from using testing to uncover integration problems, environmental limits, failure modes, and behaviors in unintended environments, while maximizing process and product methods to eliminate faults early and to instill robustness. There are many good ideas scattered in the literature to guide design of dependable software. Some of these have to do with increasing formality and abstraction in an effort to build the right thing and build it right. And many have to do with detecting and recovering from things gone wrong. Fault tolerance is an example of the latter. Parnas' correctness tripod can be fortified with three additional considerations. These are: manage complexity, manage change, and manage rationale. Complexity has long been understood to have an inverse relationship to correctness, yet is fast outpacing correctness techniques. It is also generally recognized that up to 90% of project effort goes into maintenance (corrections and enhancements, that is, changes), and that heaping changes upon changes creates fragile software. And, as anyone who has modified a legacy system will attest, design rationale is usually not well captured. Understanding the rationale behind design decisions is important, especially when the design reflects safety, security, and dependability requirements. Not understanding how the design meets these requirements leads to a dangerous maintenance situation.

Each of the three disciplines is trying to ensure that we build the right thing, build it right, and protect it appropriately, from the viewpoint of that discipline. "Protect" takes on the flavor of the discipline — security protects from adversaries, dependability protects from faults, and safety protects from hazards. Most critical software needs to be looked at from all three perspectives. However, what helps from one perspective may actually be detrimental from another. Decisions must be made to apply scarce resources to achieving an acceptable balance. Since each discipline takes a unique perspective on the system, starting from any one makes it difficult to do justice to all. That is why it is important to find a new central perspective that can balance all three using a system-wide view. That new perspective could be "correct operation," as long as correct is defined to include not only functional requirements, but also the safety, security, and dependability objectives of the system. This, of course, forces more explicit statement of surety objectives, which is good. And, carefully defined, "risk" could be a multi-dimensional measurement that tells how close the system is to the goal of balanced, correct operation. The system is in balance and correct when the residual risk along each dimension (requirement or surety objective) is within an acceptable limit. Figure 1d illustrates this balanced risk approach.

Road No. 3.
From Best Practices to Fundamental Understandings: the Development of Science and Analysis

The software engineering field is making the journey from trial & error, to best practices, to science-based. While best practices capitalize on important learning experiences, one must delve deeper into cause and effect, measurement and prediction, and modeling of fundamental understandings, in order to approach science. The science consists of models that relate measurable and controllable aspects of the software product and process to desired properties of the product. Software metrics offer a start in the right direction. As the science develops, many other observables in the software development process, in the static software product, and in the dynamic executing software, will be incorporated into the models. The models will grow to encompass a wider range of desired properties (aspects of quality and surety), and at the same time will become more precise. To make the scientific models useful, more engineering tools will be built for data collection and for computing to what degree a software product meets its goals in terms of desired quality and surety properties. The term risk analysis, as defined in the Introduction, is used generically to represent this computation.

Road Number Three, which lies mostly toward the future, has two stops. The first is a Software Reliability Science and Engineering Roadmap, which outlines the types of models and engineering tools that are sought for the software field. The second stop focuses on two relevant forms of risk analysis, Multi-Factor Qualification, and Software Probabilistic Risk Assessment.

Table 1 shows the Software Reliability Science and Engineering roadmap. The goals of the roadmap are threefold: greatly improved software reliability, an ability to measure software reliability, and new paradigms for design and development that bring reliability to the forefront. The roadmap addresses the following four elements, each with regard to scientific understanding, engineering tools, and new paradigms:

Table 1. The Reliability Science and Engineering Roadmap

Elements ↓	Scientific Understanding	Reliability Engineering Tools	New Paradigms
Reliability Modeling	Models relating observables to reliability properties Model effects of hardware-software interaction	Data collection tools: static & dynamic observations of the software product Analysis tools: deriving a reliability assessment from the observations Risk management decision support tools	Science-based measurement, analysis, prediction of software reliability
Architectures	Understand coupling between architectures & reliability properties Understand reliability design margins, software equivalent of over-engineering Model for composing reliability properties of components	High-reliability architectures Approaches for incorporating components with low or unknown reliability	Reusable architectures with known properties Building software systems by composition (measuring reliability properties by composition)
Lifecycle	Understand coupling between processes & reliability properties of the software product Fragility model: how	Eliciting & documenting requirements & hidden assumptions Simulations, "executable" specs	Design for maintainability & assess impacts prior to changes Model-based software engineering

Table 1. The Reliability Science and Engineering Roadmap

Elements ↓	Scientific Understanding	Reliability Engineering Tools	New Paradigms
	reliability degrades with maintenance	Process data collection tools; instrumentation of the lifecycle Compensating for low quality parts of process (e.g., non-qualified compiler)	Feedback to improve processes and models Upgrade in-place
Qualification	Couple (product measurables + test + simulation + process) to a reliability rating	Multi-factor reliability measurement Operational surveillance of fragility Regression testing & requalification	Deliver a reliability rating with the software product & monitor its degradation over time Find limits & breaking points; test the extremes; predict behavior in unexpected environment Explicitly satisfy surety, quality, reliability requirements

Reliability Modeling. This element provides the basic science behind software reliability engineering. The emphasis is on understanding what can be observed and measured about software, both statically and dynamically, and how these relate to desired reliability properties. Models must relate the software to its environment, by representing hardware-software interaction, for example. Emphasis is placed on developing the software reliability models in a form that is compatible with larger system reliability prediction and allocation.

Architectures. Software reliability architectures represent reliability-enhancing approaches to overall software system design. This element provides a quantitative link between specific architectures and reliability improvements. Specific approaches are needed for enhancing reliability around components of low or unknown reliability (for example, COTS). It is a goal to understand software equivalents of over-engineering and design margins. It is a goal also to model composition, that is, to specify how properties of individual software components compose into overall properties of a software system built from the components.

Lifecycle. This element couples metrics about software lifecycle processes to reliability properties of the software product. Lifecycle processes span everything from requirements elicitation to development environments to operational upgrades. This element addresses integration of all lifecycle tools with ongoing reliability assessment. It also presents new paradigms for managing artifacts (for example., documents) and for managing change.

Qualification. This element couples all available metrics (process, product, test, simulation, and so on) to support qualification decisions. It includes initial product reliability rating, operational surveillance of the product in the field, and regression/requalification following changes in the product or its environment.

Multi-Factor Qualification refers to the environment and tools for qualifying software according to the models developed under Software Reliability Science, pulling together all relevant data and factors from all lifecycle phases into an integrated assessment. In the past, qualifying a software product for use has relied heavily on testing. While there is growing emphasis on process and product measures, and on removing defects earlier in the process via code inspections and formal methods, there is no process today for pulling all the measurement data together into a coherent picture of the product quality. Goals for Multi-Factor Qualification include instrumenting the lifecycle for ongoing assessment, delivering a "qualification rating" along with a software product, supporting re-qualification during the operational and maintenance phases, and supporting reuse and integration of COTS. Tools will be developed to collect and manage software quality data, to apply analysis models, and to present results. Factors one could expect to be relevant include, but are not limited to: (1) static measures, such as traditional software metrics; (2) testing metrics, including reliability growth; (3) advanced software metrics applicable to object oriented, distributed, and parallel code; (4) rate-of-change metrics which assess how software changes impact quality; (5) process metrics; (6) information on the quality of the environment; (7) quality and fit of COTS and reuse pieces; (8) dynamic measures that reflect the behavior of real-time and non-deterministic systems; (9) use of formal proofs;and (10) use of simulations, interpretations, and debuggers.

Probabilistic risk assessment (PRA) is an established field whose approaches are routinely applied to assessing reliability and safety in critical systems applications such as nuclear reactors. PRA consists of a suite of methodologies using trees, graphs, tables, or block diagrams to explore causes and effects, yielding quantitative estimations of risks. In a typical use of the tools, an analyst inputs failure estimates which come from knowledge of failure modes of various parts of the system and from data on failure rates that have been collected in testing and in the field. Once a system under study is modeled with a tree or other construct, and input estimates have been entered, the model can be "solved" with the mathematics of probabilities. The inputs are combined according to a logic which models how combinations of failures can lead to unacceptable events and whether these failures occur serially or in parallel.

But how does the PRA analyst treat software components in the system? We cannot claim to understand failure modes of software as the consequences of software errors can be delayed in time and space and quite difficult to trace and data on failure rates is grossly lacking. There are two possible reactions to this dilemma. The first is to assume that the software will not fail. A dangerously erroneous assumption, but, surprisingly, one that is often made! The second is to assume the software will fail. When the software has a limited and straightforward role in the system its failure can sometimes be compensated for by hardware interlocks or failovers. This is a risk avoidance approach, essentially removing the software from the risk analysis. The avoidance approach is not always feasible, however. Many subtle failures are possible which are difficult to isolate but may have serious consequences. And, highly distributed applications make overall risk avoidance difficult or impossible. Thus, we cannot escape the need for active software risk management.

Software PRA will require new tools and models that can portray the interactions of threats/hazards/faults, risk states, and mitigators. The thought processes that go into probabilistic risk assessments are generally applicable to software. And the modeling approaches are somewhat applicable. However, a drawback to block diagrams is that they tend to favor one narrow view of the system, such as physical layout or process flow. And a drawback to table-based approaches is that they tend not to deal with interactions across components or events. Graph techniques have visual appeal over trees because they eliminate redundancy and can show the system-at-a-glance, especially when they are developed hierarchically. In current usage of graph techniques, risk quantification is based on conditional probabilities of combinations and series of events leading up to undesirable events. The logic used to combine probabilities assumes simple (and's and or's) interactions of events, and probabilities that do not vary over time. PRA is typically applied to assessing component failures in systems where these assumptions (this "theory of risk") hold. Software systems do not fit the assumptions due to their complexity and multiple, unpredictable failure modes. Software systems need a new theory of risk.

The theory of risk focuses on the function, the mathematics or logic, the calculations to be made over the graph, to measure the risk reduction that can be achieved and the remaining residual risk. It is the model of how risk states, threats, and mitigators interact to push us towards or keep us from hitting the undesirable states. The theory also includes the scales on which these things are to be measured. The traditional PRA "solution methods" are based on a theory of risk that does not fit the software situation. Thus, we seek to replace them with a new mathematical solution that works for organized complexity, for things measured on different scales, and for data with wildly varying uncertainties. The next step might be to investigate some of the newer branches of mathematics that take into account various sources of uncertainty - randomness, conflicting evidence, confusion, lack of information, and so on. This mathematics includes possibilistic, fuzzy, evidential, and Dempster-Scheaffer. The "theory of risk" development discussed here is not applicable solely to software. It applies to any system that is characterized by organized complexity. In fact, software is always part of a larger system and the boundaries of analysis can be set inside or outside the software portion.

Conclusion

In this paper, the reader has traveled what originally seemed to be three distinct paths in the history (and future) of software and its surety properties. However, looking back, the paths have more commonality than might have been expected. The security road demonstrated that changes in infrastructure and environment could invalidate solutions by radically changing the problem space. The early view of security was seen to be evolving from a compliance phase, through an assets protection phase, into some yet undiscovered but broader look at security and dependability that will facilitate assurance.

The safety + security + dependability road explored the need to balance competing objectives. A viable, enabling viewpoint into the problem space was seen to be key to achieving this. Thus an enabling and encompassing viewpoint is the current goal of both roads! The science and analysis road looks toward better foundations for approaching software as a systems science. The cornerstones of system science are models and measurements that can assess how close a system is to its design goals. This road goes in a direction compatible with the other two, but reaches further for the analysis capability that enables assurance and the balancing of competing objectives.

While separate communities of experts have concerned themselves with traveling each road, one can see that their thinking really merges at two junctions, as illustrated in Figure 2.

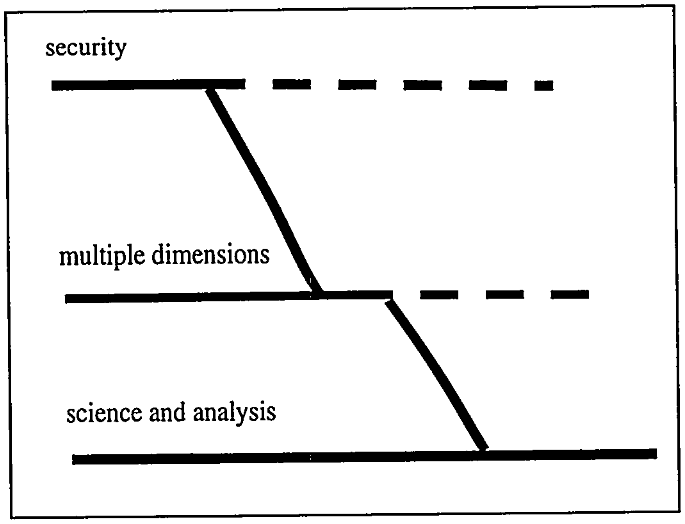


Figure 2. The three roads merge.

Suggested Reading List

Abrams, M. D. and M. V. Zelkowitz, "Belief in Correctness," *Proceedings of the 17th National Computer Security Conference*, October 1994.

Ayyub, B. M., et al., (ed.) *Analysis and Management of Uncertainty, Theory and Applications*, North-Holland, 1992.

Capability Maturity Model for Software, Version 1.1, SEI-93-TR-024, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 1993.

Carr, M. J., et al., *Taxonomy-Based Risk Identification*, SEI-93-TR-006, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, June 1993.

Dyer, M., *The Cleanroom Approach to Quality Software Development*, Wiley, 1992.

Everett, W. W., et al., *Reliability by Design*, AT&T order code 010-810-105, 1990.

Federal Criteria for Information Technology Security, Published by NIST and NSA.

Fletcher, S. K., et al., "Software System Risk Management and Assurance," *Proceedings of the New Security Paradigms Workshop*, La Jollä, CA, August 1995.

Fletcher, S. K., et al., "Understanding and Managing Risk in Software Systems," *Proceedings of the Eleventh Annual Computer Security Applications Conference*, New Orleans, LA, December 1995.

Fletcher, S. K., "Managing the Risk of Using Software in Critical Systems," *Proceedings of the Twelfth Annual American Defense Preparedness Association Security Technology Division Joint Government-Industry Security Technology Symposium*, Williamsburg, VA, June 1996.

Fletcher, S. K., "Risk Management - What About Software?" and "Are Safety, Security, and Dependability Achievable in Software?" *Proceedings of the 14th International System Safety Conference*, Albuquerque, NM, August 1996.

Goel, A. L., "Software Reliability Models: Assumptions, Limitations, and Applicability," *IEEE Transactions on Software Engineering, Volume SE11,12*, December 1985.

Gowen, L. D. and J. S. Collofello, "Design-Phase Considerations for Safety-Critical Software Systems," *Professional Safety*, April 1995.

Jae, M., and Apostolakis, G. E. "The Use of Influence Diagrams for Evaluating Severe Accident Management Strategies," *Nuclear Technology, Volume 99*, 1992.

Jansma, R. M., et al., *Risk-Based Assessment of the Surety of Information Systems*, SAND96-2027, Sandia National Laboratories, Albuquerque, NM, July 1996.

Kang, K. C. and M. G. Christel, *Issues in Requirements Elicitation*, SEI-92-TR-012, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 1992.

Lamia, W. and G. Pandelios, *Introduction to Software Development Risk Management*, SEI-93-TUT-SEPG-6, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 1993.

Leveson, N. G., *Safeware: System Safety and Computers*, Addison Wesley, 1995.

Lim, J. J., et al., "Can Information Surety be Assessed with High Confidence?" *High Consequence Operations Safety Symposium* (poster paper), Albuquerque, NM, July 1994.

Lubars, M., et al., *A Review of the State of the Practice in Requirements Modeling*, MCC Technical Report Number RQ-169-92, Microelectronics and Computer Technology Corporation, Austin, TX, 1992.

Meadows, C., "Applying the Dependability Paradigm to Computer Security," *Proceedings of the New Security Paradigms Workshop*, La Jolla, CA, August 1995.

Neumann, P. G., *Computer Related Risks*, Addison Wesley, 1995.

Parker, D., "Restating the Foundation of Information Security," *Proceedings of the 14th National Computer Security Conference*, Washington DC, October 1991.

Parnas, D. L., et al., "Assessment of Safety-Critical Software in Nuclear Power Plants," *Nuclear Safety 32-2*, April-June 1991.

Proceedings of the 4th International Computer Security Risk Management Model Builders Workshop, (sponsored by NIST and University of Maryland), August 6-8, 1991.

Radley, C. F., *Software Safety Progress in NASA*, NASA Contractor Report 198412, October 1995.

Rushby, J., *Critical System Properties: Survey and Taxonomy*, SRI-CSL-93-01, SRI International, Menlo Park, CA, May 1993.

"Software Development Risk Management: An SEI Appraisal," *SEI Technical Review '92*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 1992.

Trusted Software Methodology, Volume 1, SDI-S-SD-91-000007, June 1992.

Wright, D. L., *Nuclear Weapon Reliability Evaluation Methodology*, SAND93-0704, Sandia National Laboratories, Albuquerque, NM, 1993.

Wyss, Gregory D., et al., "Toward a Risk Based Approach to the Assessment of the Surety of Information Systems," *American Society of Mechanical Engineers Pressure Vessels and Piping Conference, Topical Meeting: Risk and Safety Assessments: Where Is the Balance?*, Honolulu, HI, July 1995.

Wyss, Gregory D., et al., "Probabilistic Logic Modeling of Network Reliability for Hybrid Network Architectures," *Proceedings of the 21st Annual IEEE Conference on Local Computer Networks*, Minneapolis, MN, October 1996

Wyss, Gregory D., et al., "Risk and Reliability Assessment for Telecommunications Networks," *Proceedings of the International Topical Meeting "Probabilistic Safety Assessment '96" (an American Nuclear Society meeting)*, Park City, UT, Sept. 29-Oct. 3, 1996.

Wyss, Gregory D., et al., "Information Systems Vulnerability: A Systems Analysis Perspective," *Proceedings of the American Defense Preparedness Association Joint Security Technology Symposium*, Williamsburg, VA, June 1996.

Biography

Biography not available.

Intentionally left blank

The Role of Microelectronics and Software in a Very High Consequence System[*]

Malcolm Jones, B.Sc., Ph.D.
Hunting - BRAE Ltd (AWE)
Reading, Berkshire, United Kingdom

Abstract

Microelectronics and associated software are playing an ever increasing role in systems and these include systems which are potentially hazardous. Their attractiveness arises from their potential for low cost and for enhanced flexibility, speed, compactness, and reliability. For these reasons, a very large effort has gone into, and continues to go into the development of high integrity microprocessor based systems and their software. This effort has been directed towards 'complete English' specifications, 'perfect mapping' into machine requirements and 'perfect implementation' in current hardware technologies. Similar systematic and formal approaches have also been applied to software generation. The 'holy grail' is represented by the acquisition of 'fully specified and characterised' systems in which all possible outputs 'are known' for all possible input conditions. Such approaches have now become highly automated through supporting software packages and a great deal of progress has taken place in terms of the generation of high integrity systems and defensive software. These techniques have been applied to both commercial hardware and to custom designed Reduced Instruction Set Computer (RISC) based systems.

The evolution of these techniques and technologies has resulted in extensive and successful application in high consequence systems, e.g., aircraft control, chemical and reactor plant management, etc. These are active systems that manage the safe normal running of processes and identify the need for, or manage the intervention of, alternative safety actions if the normal processes run into fault conditions. However, microprocessors and software systems are never perfect (response to all inputs not fully characterised), there may be remnant faults in the hardware/software and the system will become unpredictable in its response when exposed to abnormal (unscheduled) conditions, e.g., excess thermal, mechanical, chemical, radiation environments. There is a saving grace in that there is usually 'a man in the loop' together with a multitude of sensors which indicate, in a timely fashion, that all is not well so that the system can be 'manually switched into a safe configuration' or even switched off. Redundancy of safety systems is standard in such cases. However, even then, history has sadly indicated that we can still make costly mistakes.

Microelectronics and software have also found their way into passive systems that do not have a man/regulator effectively in the safety loop and some of these systems come into the very high consequence category. For these cases, alternative approaches are deemed necessary. This paper discusses how safe microelectronics/software strategies can be applied to such passive systems.

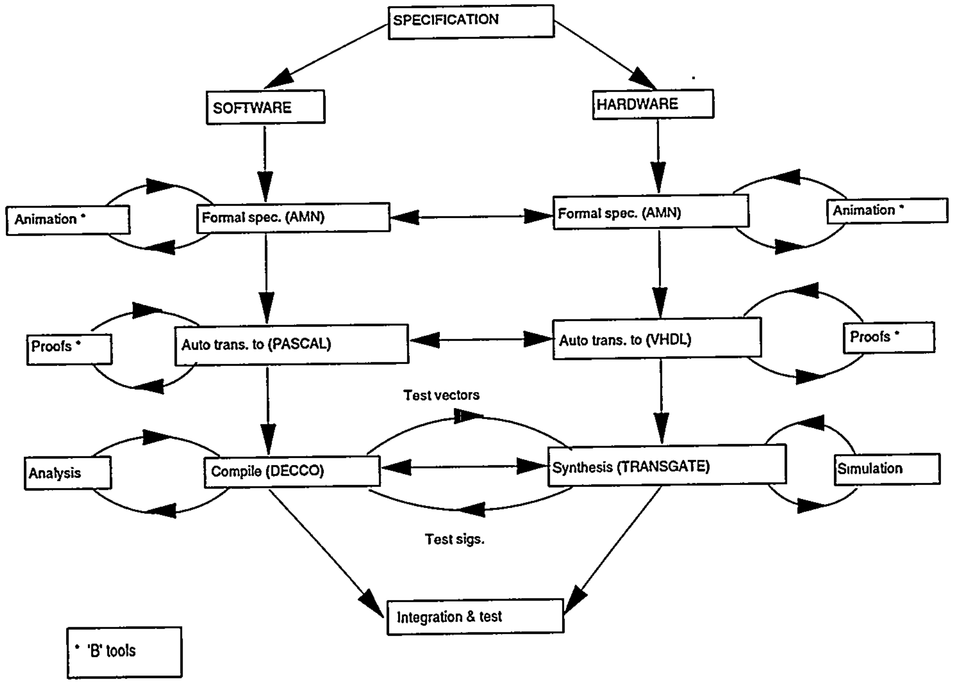


FIG. 1 HIGH INTEGRITY HARDWARE/SOFTWARE FORMAL DESIGN METHODOLOGY

Introduction

The passive safety system under discussion here is resident in an overall system that is purposely designed to produce a catastrophic event but only under 'fully authorised' circumstances. In its passive state it remains safe. Hence, safety in this context is associated with the strategy of only authorising the safety system to function in the 'unsafe mode' as a result of a series of unique inputs. All other inputs will lead to either no action or failsafe action.

Active safety systems, on the other hand operate on a different strategy. The overall system is not designed to cause a disastrous event but can result in such, if the active control systems fail to operate in the desired manner. Such a system normally operates at 'an output level' which is beneficial and not harmful, but safety failures can result in 'harmful' levels. For example, a nuclear reactor, in its normal state of operation produces useful power in a controlled fashion, and is maintained in this state through a number of continuously operating safety management systems, including its sensors. Failure of such systems, including the ultimate protection of a timely shut down, can lead to disaster. Of course such arrangements have protection in depth in terms of system redundancies, man in the loop and layers of physical protection to mitigate against the consequence of uncontrolled events. The systems that maintain aircraft safely in the air (together with the sensors that warn of potential failures) represent another potent example. Hence, operation of the active safety systems do not rely on unique inputs but rather demands the simplest and most reliable inputs to ensure that failure to switch on and 'continue' is low. In fact, in this case, 'uniqueness' should only apply to the set of circumstances which could/would lead to safety system failure.

In an ideal world with an ideal design, there would never be such a unique set of circumstances.

Microelectronics Software and Safety

Microelectronics and software have found their way into potentially hazardous systems which do not have a man/regulator effectively in the safety loop and one of these systems comes into the very high consequence category. The 'holy grail' is represented by the acquisition of 'fully specified and characterised' electronic/software systems in which all possible outputs 'are known' for all possible input conditions. Such approaches have now become highly automated through supporting software packages, as exemplified by Figure 1. A great deal of progress has taken place in terms of the generation of high integrity systems and defensive software. These techniques have been applied to both commercial hardware and to custom designed Reduced Instruction Set Computer (RISC) based systems. Although electronic hardware and software are now highly reliable in normal environments, they can nevertheless become unpredictable under abnormal environment conditions and for the very high consequence system under consideration here, this is unacceptable. Some of the concerns often voiced when microelectronics and software are advocated as an intrinsic part of safety in such systems are:

(1) Items are too small to see and physically understand.

(2) The functional characteristics (relationships) are complex and exist only on paper and even then may not be complete.

(3) The functional characteristics (relationships) take on an 'infinite' number of possibilities in the presence of faults (e.g. abnormal environments) and the safety proving process will become massive.

(4) Safety panels will need electronic expertise at the highest level to deal with the complex issues involved and this will not always be widely available.

For these reasons, the goal should be that electronic systems would only act in a 'mailing' role for unique information, rather to act in an 'autonomous' decision and control function role. That is, there is a need to find a methodology for 'explicitly' taking microelectronics, and its associated software, out of the principal safety analysis. **Of course one can only approach this ideal goal.**

A Demanding Safety Requirement

The safety requirements for most potentially hazardous technologies are derived from two general measures:

(1) The balance of benefit against hazard.
(2) The risk level compared with other technologies

Such measures are more difficult to apply to the subject of this paper because:

(1) The measure of benefit is somewhat subjective and may change with time.
(2) It is not clear that a very high consequence technology can be legitimately tied to a generally accepted risk criterion.

(Risk = event rate × consequence)

Because of the potentially massive consequence associated with the system under consideration, the safety rules are appropriately onerous, to the extent that the inadvertent event should not be capable of occurring. Of course, nothing is impossible. In engineering language, the requirement is that the inadvertent event should be extremely unlikely per unit lifetime (where extremely unlikely if of order 10^{-9}). In order to budget for risk in a balanced way, this is interpreted in terms of at least three unlikely and independent failures per unit life, where unlikely is of order 10^{-3}. A failure is identified in terms of a major technical safety failure, a significant abnormal environment (accident) or a major procedural safety failure.

From a mathematical point of view, extremely unlikely is obviously not equivalent to 'it cannot happen.' However, there is a credible limiting engineering number for which a case, and a realistic supporting logic, can be made, and the figure of 10^{-9} lies very much in this regime. This criterion also puts one comfortably in the same category of frequency as massive natural disasters. For example, some estimates for a catastrophic meteorite impact with the earth lie in the 'once every 500,000 year' category.

In addition there is a complementing **As Low As Reasonably Practicable (ALARP)** requirement, which tells us to keep on trying.

The bottom line is that we have to satisfy an extremely demanding safety requirement.

‘Uniqueness’

The term ‘Uniqueness’ represents something of a corruption of the English language but, in the current context, is taken as a measure of the improbability of inadvertent acquisition of safety critical enabling ‘information.’ This information may be in the form of electronic data, physical environments (or their sensor representations) or a sequence of system events. As far as electronic data is concerned, inadvertent acquisition may arise as a result of inadvertent external entry or through inadvertent ‘internal’ generation. Unique environments and system event sequences are chosen on the basis they (and their sensor representations) are unlikely to occur in the absence of intentional and authorised use of the system.

As will be noted later, these unique attributes will eventually be processed into unique drive sequences. A drive sequence may be derived solely from externally supplied data or through a combination of supplied data and the processing of environment and event sequence data. Assessment of the ‘uniqueness’ of a drive sequence is, to some extent, a subjective process, but the general goal is that of demonstrating an inadvertent occurrence rate of $< 10^{-6}$ per unit life for a reasonable spectrum of credible unscheduled conditions and faults.

Environments

The response of a system will depend on the physical environments that it may encounter, and its ability to respond to their occurrence, particularly if there is time for human decision making and action ‘in the loop.’ Environments are usually split into two categories:

> Normal - those that are associated with the normal state of the system, either internally or externally generated, and for which it is designed.
>
> Abnormal - those not associated with the normal state of the system, either internally or externally generated, and for which it is not designed.

In the active system, abnormal environments can arise through both internal and external sources. In the passive systems under consideration here, they are mainly associated with external generation.

The response to the detection of an abnormal environment will depend on whether it constitutes a danger or not. For example, a reactor system monitoring the onset of an uncontrollable abnormal environment may generate the response of an emergency shut down of the reactor either by automatic or manual means. Such processes (and their sensors) are designed with redundancy in mind and are also required to operate under abnormal environments (at least to some level) in order to minimise the chance of a failure of the shut down action. A fire in the engine of an aircraft can be detected and extinguished, and the engine shut down together with isolation of the fuel flow and electrical power to that area. However, positive control responses may not always be successful and such failures are backed up with systems that are aimed at mitigating against the level of consequence. For example, containment systems are built into reactors and emergency procedures set down for aircraft and, in particular, the last ditch ejector seat and parachute in military aircraft. However, disasters can still occur and allowable risk is a balance of need, cost and tolerance.

The potential hazard, from the passive system under consideration here is massive. Further, there are two categories of abnormal environment:

(1) The external abnormal environment over which one has control prior to it affecting the system i.e. it can be 'turned off' or the system can be removed from its influence.

(2) The accident or natural disaster environment to which the system is exposed, and where there is little or no ability to intervene to protect the system.

It is obviously the latter case that causes most concern. In addition, there is very little scope for mitigating against the consequences of the unwanted event. Hence the overall safety strategy must be based on 'robust' design, protection and careful siting.

Unique Information Control and its Application

The basic approach is that of only enabling the safety systems (to change to a less safe state) on the acquisition of, and response to, 'unique' information. There are standard techniques for the construction of 'unique' signal sequences such that their inadvertent generation is relatively remote. However, a fundamental problem arises in terms of the character of the discriminating or decoding mechanism necessary to maintain the 'uniqueness' level through the safety system. For example, the micro-electronics system might be highly discriminating in its own right in checking for the correct sequence, but the end result is typically a simple enabling signal, e.g., the driving signal to some simple mechanical switch. In this case, concern lies in the fact that the final output is a relatively simple event- much simpler than the original 'unique' authorising sequence – and it is hard to provide the necessary assurance, that such a final event has a sufficiently low probability of occurrence. This is particularly so when abnormal environments have to be included. This is seen as the Achilles Heel of a system that bases its safety rationale on exclusively electronic arguments. The problem can be overcome through an approach which requires a complete set of explicit response actions in 'unique' order – matching the 'uniqueness' of the authorising signal sequence in a one for one manner – and where such a sequence of actions is as unlikely to occur inadvertently, through fault, procedural error or environment, as the authorization signal sequence itself. That is, the uniqueness requirement is not diluted anywhere in the operation of the safety system. One method of achieving this is through the application of electro-mechanical unique signal discriminator devices.

Electro-Mechanical Discriminator Requirements

The generic requirements for such an electro-mechanical discriminator device, are as follows:

(1) It must be explicitly robust to abnormal environments - unlike microelectronics.

(2) It must remain safe in the absence of the correct driving instruction or driving sequence.

(3) The required 'uniqueness' of its discriminating action should match that of the instruction sequence.

(4) It should be robust to discriminator by pass threats, e.g., should not be single failure safety critical.

Electro-Mechanical Discriminator Classes

Only two philosophically different, two dimensional electro-mechanical discriminator classes have been identified so far at AWE, and a single example of each type developed:

Two Dimensional Maze Concept: This incorporates a pin in a groove which, at any position, has a choice of two directions of movement; one (correct) which allows the mechanism to continue to progress towards full actuation (from safe to enabled), and the other (incorrect) which causes irreversible and safe lockup.

Two Dimensional Manifoil Concept: The manifoil wheels have two possible directions of rotation at any time. This mechanism has a very low probability of reaching the enabled position even if signals continue to be applied over a very long period (like trying to open a manifoil lock in the absence of information). Further, it only allows the exact minimum number of steps necessary between start (safe) and normal enablement (unsafe) to accrue. Any excess above this count leads to irreversible and safe lockup.

Many possible variants, based on these two concepts, are possible.

In principle, one could extend the number of 'dimensions' in the discriminator, e.g., 12 for the maze:

6 Translational
6 Rotational

There has been a somewhat philosophical debate as to whether extra dimensions (above 2) increase safety or otherwise and of course the practical difficulties of implementation increase with the number of dimensions. In addition, there is always the 'balance of safety' issue, that is, in attempting to enhance one aspect of safety, another aspect may be degraded. This often happens when complication increases.

A Practical Example of an Electro-Mechanical Discriminator

The discriminator mechanism depicted in Figure 2a is based on a manifoil system. It has the following properties:

(1) It is made from stainless steel parts and is housed within a crush proof (stainless steel) case and is hence, designed to be robust to abnormal mechanical events. The material properties are well known (predictable response) up to a high stress level. Beyond this, the most likely response is a failsafe jamming of the mechanism and grounding of principal electrical power contacts.

(2) The use of organic material is minimised in order to avoid gas build up (high-pressure generation) or electrical tracking paths in abnormal thermal environments.

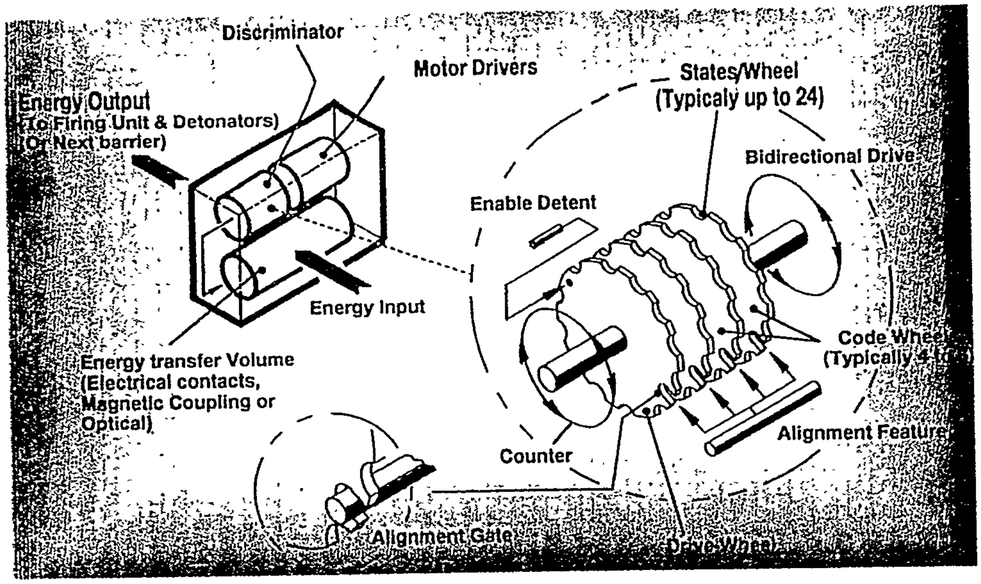


Figure 2A. The Manifoil Discriminator.

(3) The mechanism can make step movements in either clockwise or anticlockwise directions with each step dictated by one element of the 'unique' drive sequence supplied to the electrical actuator (a stepper motor).

(4) No movement is possible unless a detent is positively held off, by powering a second electrical actuator.

(5) The clockwise and anticlockwise movements of the mechanism turn the manifoil wheels, which can only move in unison when linked in the direction of movement.

(6) Only when all of the manifoil wheels are correctly aligned with a fixed reference, can a linking bar (which normally locks safe the power transfer mechanism) become engaged with the driving mechanism, and which then enables the device to move from the safe to the enabled state on further drive inputs to the stepper motor.

(7) The mechanism also counts the number of steps taken from the initial safe setting of the manifoil and, if the count exceeds the minimum necessary to reach the final enabled state, the mechanism is irreversible locked up in a safe state. Hence, the unique code and matching driving sequence, is necessary to take the manifoil system to the enabled state.

(8) Even if the counting mechanism fails, the discriminator has a high degree of protection against spurious signals. For example, the typical maximum step response rate of the mechanism is of the order of 1kHz. If spuriously produced code contents changed at this rate in the driver's register, then with suitable manifoil design, the probability of correct full manifoil wheel alignment would **only rise to the order of 10^{-3} after 100s of hours**. In fact, the actuator that holds off the detent would be designed to burn out (with resulting fail-safe locking of the mechanism) on a much shorter time scale. Further, the number of steps executed during this elongated period could well have worn out the mechanism, leaving it in a failsafe state. Of course this threat assumes that inadvertent power is continuously available over the extended period.

Figure 2b illustrates the principle of the pin in the maze discriminator.

Choosing the Discriminator Drive 'Pattern'

There are 3 potential safety attributes in the 'unique' sequence or drive signal sequence

- The sequence length.
- The sequence 'pattern.'
- The sequence element format.

Only the first two attributes are given any credence for safety assurance, because the ability to produce the third will have already been built into the system and could be inadvertently switched on, e.g., the electrical drive format that enables the maze

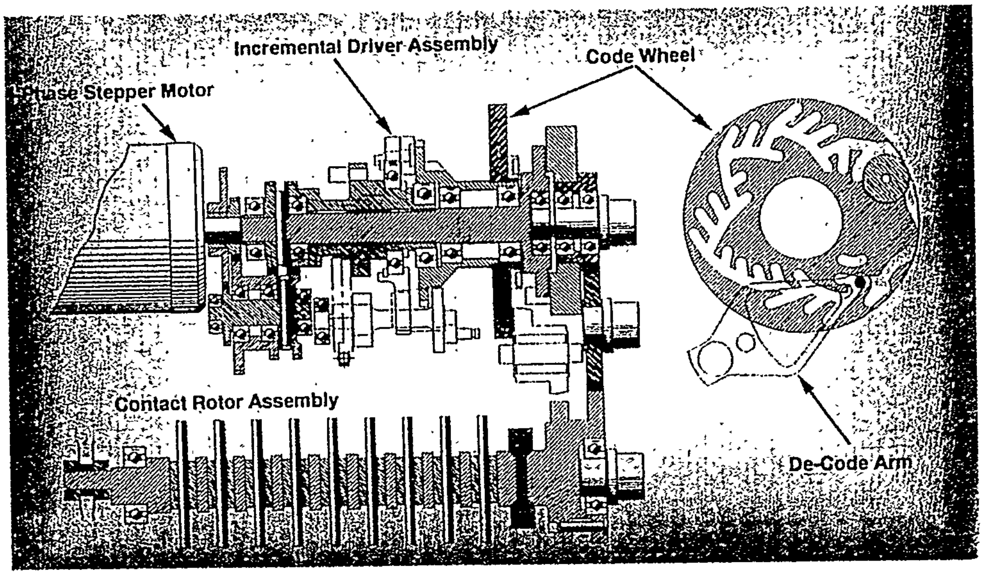


Figure 2B. The 'Pin in a Maze' Discriminator.

mechanism to take a single step in the maze. We take little safety credit for the normal absence of power and electronic activity.

There is a sensible limit to the length of a sequence, in terms of limiting the complexity and volume of the mechanical discriminator, without unduly reducing its robustness and at the same time enabling it to function rapidly when required.

The sequence 'pattern' is chosen to minimise its (worst case) chance of inadvertent generation either through random, independent or dependent (pattern) biases in the system.

Take the example of a 2 dimensional system with sequence elements of type A and B

The sequence AAAAAA.... (length n) is as unlikely to occur as any other from a random statistical point of view, with probability of occurrence

$$P = (1/2)^n$$

but equal numbers of As and Bs are better if we include the possibility of 'unknown' independent biases towards A or B (and a 100% inadvertent bias towards A represents the worst case for the above sequence choice). In the absence of dependent biases, **the above occurrence probability is then retained for n/2 As and Bs**, for the worst case independent bias condition:

$$P(A) = P(B) = 1/2$$

{here P(A), P(B) are the independent probabilities of an A or B appearing next in the sequence}.

The sequence ABABABA..... satisfies the above condition, but is vulnerable to 'unknown' dependent biases. For example, the dependent nearest neighbour relations represent the worst case

$$P(A/B) = P(B/A) = 1, P(A/A) = P(B/B) = 0$$

{Where P(A/B) is the dependent probability of a B following an A}.

The criterion for equal number of As and Bs must now be supplemented with criteria for maximising the protection against these unknown dependencies (nearest neighbour, next nearest neighbour, etc., correlations) that is, making the sequence as 'patternless' as possible.

For maximum protection against the worst case nearest neighbour dependency, the above overall sequence occurrence probability, $(1/2)^n$, is retained if:

There are equal numbers of occurrence of the pairs AA, AB, BA and BB when taken in order along the sequence.

and caters for the worst case dependency case of

$$P(A/A) = P(A/B) = P(B/A) = P(B/B) = 1/2$$

If we include relationships stretching over m neighbours, then maximum protection occurs if:

There are equal numbers of occurrence of all permutations of length m (2^m) when taken in order along the sequence.

Figure 3 shows the dependent bias properties for the example of the near ideal 24-element sequence

ABAAAABAABAABBBBABBBBAAB

and, in particular, how (for the worst case dependence relations) the inadvertent occurrence probability varies with the assumed 'length' of the neighbour relationship.

These rules can be generalised to sequences having arbitrary numbers of different signal types (degrees of motion of the discriminator):

A,B,C,D .....etc

Factors which can Undermine the 'Unique' Sequence Logic

Of course the 'Unique Information' concept represents 'an ideal' which can only be approached in any practical application.

It is assumed that power is available, and that the microelectronic system is active in some general undefined way that is, no safety credit is taken for the absence of power or for the known (designed) functionality of the microelectronics and associated software (which is particularly true for abnormal environments).

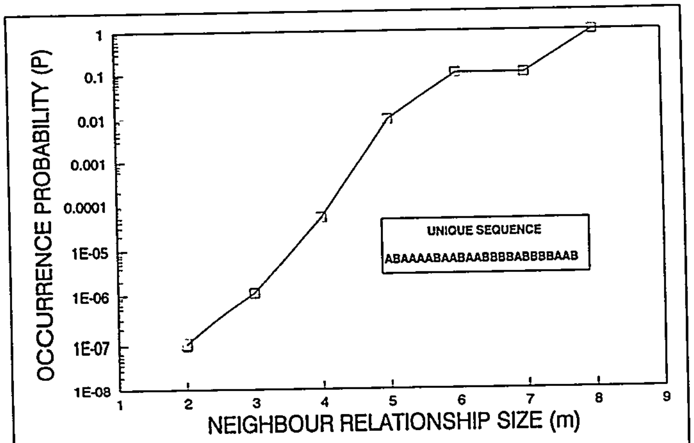


FIG. 3. WORST CASE INADVERTENT OCCURRENCE CHARACTERISTIC.

Figure 3. Worst case inadvertent occurrence characteristic.

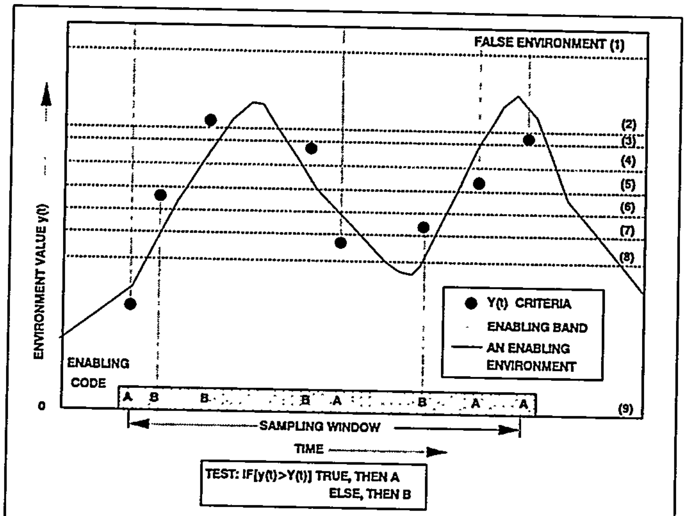


FIGURE 4. ENVIRONMENTAL TEST ALGORITHM.

Figure 4. Environmental test algorithm.

There are two basic safe methods by which the unique information can be made available to a system:

(a) By authorised manual insertion into the system.

(b) By construction from a unique authorising set of 'environments' or 'system events.'

The Cardinal Rules necessary to ensure that there is no undermining or dilution of the 'Unique' sequence/discriminator approach are:

(1) The unique sequences should not be pre-stored (on line) in the system prior to requirement.

(2) Accidental insertion should be as unlikely as the inadvertent generation of the sequence.

(3) Any inadvertent or subsequently rescinded authorised insertion, can be positively negated.

(4) The system should not contain any information that could lead to the generation of the 'unique' sequence by a simpler process.

(5) The system, in processing the information, does not at any stage dilute its uniqueness.

(6) Ideally, the unique sequence should be sent one element at a time.

(7) The procedure for generating 'unique' sequences from 'unique' environment and event sets should not dilute the uniqueness' principle.

Not Pre-Stored: The reason for the first rule is obvious. If such 'unique' information is pre-stored and accessible to the electronic system, then the assurance arising from the 'uniqueness' principle is lost because it could be released inadvertently through a 'relatively simple' fault. In principle, one needs to ensure that this information does not reside in any of the components of the entire system which can credibly communicate with the discriminator controller, and this can be a wide ranging issue (noting again that one has to cover the potentially unpredictable interrelationships under abnormal environment conditions). For example, it appears sensible to overwrite all of the 'non encoded,' non-volatile stores with safe information at the final stage of manufacture. Chips containing the 'unique' sequences could well have been built in for test purposes during development and manufacture and then 'not taken out.' There are techniques for limiting the scope for this problem, through not 'effectively' using the enabling sequence during testing. The discriminator controller can use a 'test' conversion algorithm during the testing phase, which is replaced by another for full manufacture, making any previous external test chip sterile. Of course, those designers responsible for the 'more limited controller region' will still have to ensure that these changes are made. **This illustrates another important principle, that of making the safety strategy as independent as possible from external (to the sequence controller) 'inadvertent' influences.**

Unlikely Insertion: Typical measures to avoid inadvertent insertion are strongly biased towards procedures. For example, the use of pre-encoded ROMs and locked out reader ports etc. Such approaches provide robust arguments against inadvertent insertion, even for the case of abnormal environments.

Negation: Ideally one would want to ascribe no internal storage, but this would mean step by step operation of a potentially, non-reversible mechanical discriminator, as the sequence was externally entered, one element at a time. Of course we don't want this. Hence, storage of the sequence is unavoidable and we need to place it where it can be best controlled and where we can exercise maximum independence from the rest of the system. The latter should act merely as a post box passing the sequence through, one element at a time, and having a capacity to store no more than one element of the sequence. Ideally, the sequence memory in the controller should be of volatile nature that is, with information loss on removal of power. If volatile storage is not possible (or if some latent ghost image cannot be discounted) then a safe and confirmed overwrite procedure has to be adopted.

An Inadvertent Simpler Process: One example of this concerns the inverse sequence. Overwriting a memory with a safe sequence does not mean the inverse of the 'unique' sequence. A simple fault may invert it. For example, the A step and B step drive signals may be stored in two locations. The unique sequence may be represented by a sequence of fetching instructions to the two signal locations. An inadvertent inversion of the 'fetch direction' could turn an inverse sequence into the enabling drive sequence.

Uniqueness Dilution During Processing: 'Uniqueness' can be degraded by data compaction and this can occur in a number of ways, when information overloading is a problem. The 'external' input could be in the form of a simpler much shorter sequence of elements, each of which calls up a pre-stored sub block of the 'unique' sequence. For example, a sequence of 4 external elements may each call up a block of 6 correctly sequenced elements of a 24 element 'unique' sequence. We have diluted the 'uniqueness' level in the system. Such a problem could arise in the context of keypad input where only 4 keys are available or where the operator doesn't want the complexity of having to deal with more than 4 keys in a given sequence.

This problem could appear in another form where, for data handing reasons, the original 'unique' sequence, of say 24 elements, is compacted, into say 4 items of information, at an intermediate stage and is then reconverted at a later stage. The conversion process gives rise to a dilution of the overall level of 'uniquenes.'

Further issues arise if the system involves encryption processes where a unique safety code might fortuitously, be encrypted into something much simpler before being decrypted. The much simpler encrypted form would have a much higher probability of inadvertent generation. Of course there is a general transparency problem here in that encryption keys are secure and can be changed on a regular basis. On the other hand, safety systems need not be associated with encryption processes.

A Single Message at a Time: Unique signal information can be passed from one part of a system to another as a single message containing the complete sequence or as a set of separate messages each containing one element of the sequence. The latter represents the more cumbersome approach but it does have distinct safety advantages in that:

(1) Only single element storage is required by other than the final controller region.

(2) Any compaction or encryption/decryption procedures are now only performed on single elements of the sequence and hence, has little effect on the overall 'uniqueness' properties.

'Unique' Environment Set Conversion: This relates to the process whereby the correct authorising set of environments and system events are converted to a 'unique' safety signal sequence, and which must only occur in the presence of the correct set. The guiding principle must be that of 'no pre-knowledge' of the sequence. Further, there must be no stored information or algorithms (ghosts) which could lead to correct sequence generation in the absence of the 'full set' of enabling environments and system events.

For example, an approach which lets out a pre-stored sequence on seeing the correct environment set would fail on two counts,

(a) Pre-stored information
(b) Single fault release.

Another pitfall would arise if the checker, in fault mode, were to compare an authorising template with itself, rather than with a sensor output.

The sequence should be generated on an element by element test of the environment and event set, against a prescribed set of criteria. Even here, there are pitfalls. For example, a system that checked every element of the set for correctness and then produced a correct sequence element, for each 'correct' result, would not meet the 'uniqueness principle.' This is because the checker could be stuck on logical 'true' (or a logical 'false' generating the inverse sequence). This again represents a 'single fault' weakness. One could extend this approach to a set of independent checkers with the correct signal element only produced if all agree that the criterion is met. If the agreement is checked by an AND gate then the single fault concern would be transferred to the AND gate. Hence, the output of the checkers would have to be processed in another way. However even then, this approach leaves us with two problems:

(1) The algorithm that decides whether a 'true' is an A or B at any point in the sequence, may contain within itself information about the correct sequence.

(2) A completely wrong environment may lead to the inverse of the sequence.

Alternatively, the 'stuck on true,' problem can be overcome by employing an algorithm built into the checker/generator sequence which is as unique as the environment set itself. For example, the correct 'unique' sequence generation should be based on registering equal numbers of 'correct' and 'incorrect' test results by the checker with the 'embedded correct/incorrect checker pattern' following the same dependence construction rules that governed the 'unique sequence' itself.

Consider the following simple illustrative example. Eight measurements, y(t), are made on an environmental sensor at fixed time points. The correct sequence ABBBABAA must only be generated if all the y(t) lie within the band criteria (effectively the Y(t) test values) shown in Figure 4. The strategy is based on a single test:

IF[y(t)>Y(t)] TRUE: THEN A: OTHERWISE B

The response of the system to some faults and false (non-authorising) environments is given in Table 1. The selection of fixed level false environments, together with the limited length sequence, is simply for the purpose of illustration.

Note that none of the faults or environments above led to the sequence or its inverse and that the algorithm contains no knowledge about the correct sequence.

The above discussion is by no means exhaustive, but rather serves to give an insight into the type of problems and pitfalls associated with this topic.

The Environmental and Event Set

The environmental and event set, in its broadest sense, not only includes sensor outputs but also the registering of a sequence of system 'events' that need to occur in the correct sequence and at the correct times. Of course this set will, in itself, need to exhibit the properties of uniqueness with regard to inadvertent generation.

Some general requirements are:

(1) One must look for independence between the events (that is, that they only appear as a result of a set of distinct authorising actions, rather that a series of events which can automatically follow given the first under unauthorised/fault conditions).

Table 1 - Response to Faults and Incorrect Environments

Fault or false environment (Figure 4)	Sequence generated/ Correct sequence	Number of differences
Stuck on true	AAAAAAAA ABBBABAA	4
Stuck on false	BBBBBBBB ABBBABAA	4
Environment (1)	Equivalent to 'stuck on true'	
Environment (2)	AABAAAAA ABBBABAA	3
Environment (3)	AABAAAAB ABBBABAA	4
Environment (4)	AABBAAAB ABBBABAA	3
Environment (5)	AABBAABB ABBBABAA	4
Environment (6)	ABBBAABB ABBBABAA	3
Environment (7)	ABBBABBB ABBBABAA	2
Environment (8)	ABBBBBBB ABBBABAA	3
Environment (9)	Equivalent to 'stuck on false' (e.g. sensor output failure)	

(2) Uniqueness in the environments and system events themselves (together with the completeness of the set). There will certainly be some environments and system events, which in themselves, will not be sufficient to confirm the true picture.

(3) Tightness in the definition of the environmental set criteria. In the example above, the tightness lay in the test points which 'banded' the enabling environment. The

tighter the specification, the more discriminating the system. However, tightness will tend to conflict with flexibility and reliability.

(4) Performance reliability of the sensors and communications systems. This is particularly important if it is difficult to achieve (2).

Summary

Although great strides have been made in the application of intrinsically safe microelectronics and software to potentially hazardous systems, there are still applications where the consequences are deemed to be potentially so severe, in terms of personnel, financial and political cost, that alternative approaches are necessary. In this case, the strategy has been to take microelectronics and software out of the principal safety arguments in order to underwrite safety with sufficient confidence, particularly for abnormal environments. Such an approach, for a system that spends its life essentially in a passive state, has been described. This approach is based on the concept of unique information control, coupled with complementary electro mechanical unique signal discriminators.

The rules for unique signal construction have been given, together with some 'in principle' electromechanical discriminator concepts, with illustrations of their implementation.

Of course, the real world seldom allows implementation to be as pure and ideal as the principle, and there are many issues that need attention in order to get to a satisfactory solution. For this reason, some of the pitfalls that can undermine the unique information approach have been identified, with indications of how they can be avoided or minimised. These cover examples of inadvertent storage of such information, inadvertently generation by processes or faults that are not sufficiently unlikely, or cases where such information if supplied to the system may be inadvertently left in.

A successful implementation of this approach depends very much on a consistent strategy across the whole of the potentially interacting electronic system. One prerequisite for this will obviously be a shared knowledge of the strategy and its principles of implementation with all of the designers, together with a supporting commitment to ensure that the strategy is not undermined in any area.

Acknowledgements

The author gratefully acknowledges the help given by members of the Warhead Electrical Department at AWE in the preparation of this paper and also to members of the Surety Organisation at the Sandia National Laboratory in the US for their helpful advice and support.

Biography

Malcolm Jones, Atomic Weapons Establishment,
Reading, Berkshire,
United Kingdom,
Postal code RG74PR
Fax 0118 9815320
Phone 0118 9827967

Malcolm is currently the Scientific Adviser to the Director of Warhead Engineering at AWE and has, for some considerable time, been responsible for, amongst other things, the development of advanced warhead system safety concepts, together with the assessment of their safe implementation. His previous post was Head of the Warhead Electrical Safety Group.

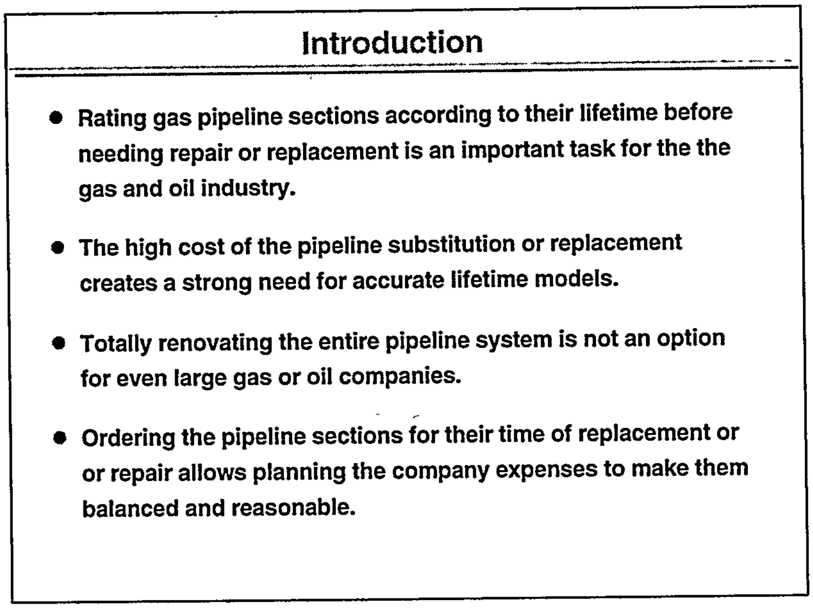
Malcolm joined AWE in 1967, after Graduating (BSc) from the University of Wales in 1964 with first class honours in physics, followed by a Ph.D. (1967) in solid state physics, from the same establishment. His career at AWE has taken him through a wide range of scientific and engineering topics, but he has maintained a continuous association with electrical based systems. He is an adviser to a number of UK Ministry of Defence and AWE safety bodies.

Intentionally left blank

Technique for Pipeline Section Maintenance Based on Numerical Analysis of External and Internal Diagnostic Data

G.S. Klishin
V.E. Seleznev
A.A. Mukashev
Russian Federal Nuclear Center (RFNC)-All-Russian Research Institute
of Experimental Physics (VNIIEF)
Russia

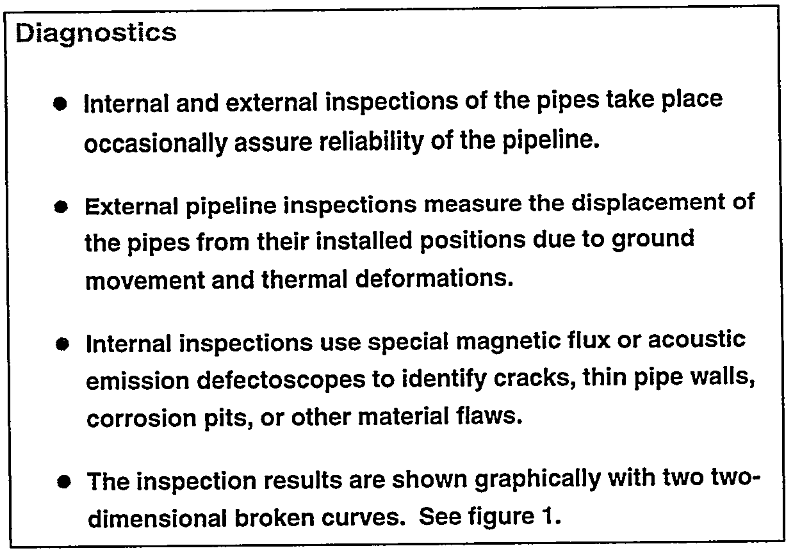
Slide 1



Introduction

- Rating gas pipeline sections according to their lifetime before needing repair or replacement is an important task for the the gas and oil industry.
- The high cost of the pipeline substitution or replacement creates a strong need for accurate lifetime models.
- Totally renovating the entire pipeline system is not an option for even large gas or oil companies.
- Ordering the pipeline sections for their time of replacement or or repair allows planning the company expenses to make them balanced and reasonable.

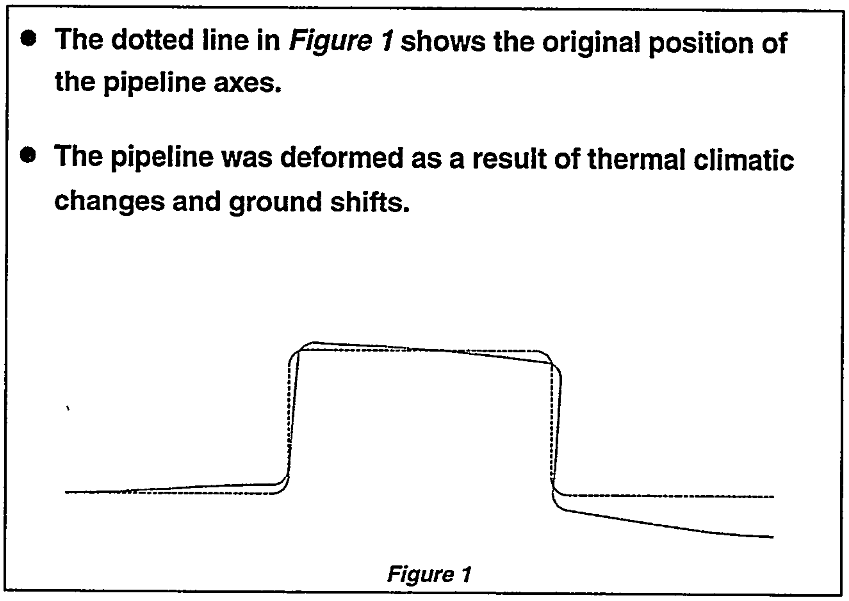
Slide 2



Diagnostics

- Internal and external inspections of the pipes take place occasionally assure reliability of the pipeline.
- External pipeline inspections measure the displacement of the pipes from their installed positions due to ground movement and thermal deformations.
- Internal inspections use special magnetic flux or acoustic emission defectoscopes to identify cracks, thin pipe walls, corrosion pits, or other material flaws.
- The inspection results are shown graphically with two two-dimensional broken curves. See figure 1.

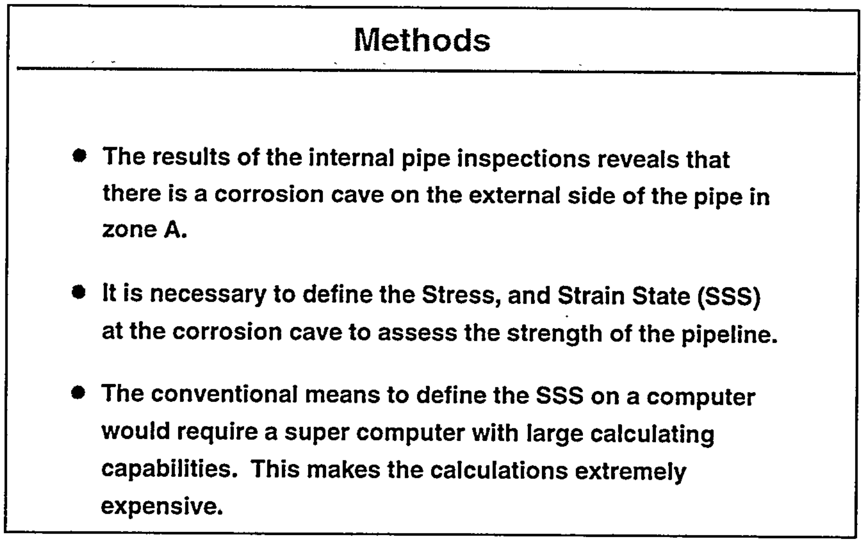
Slide 3



- The dotted line in *Figure 1* shows the original position of the pipeline axes.
- The pipeline was deformed as a result of thermal climatic changes and ground shifts.

Figure 1

Slide 4



Methods

- The results of the internal pipe inspections reveals that there is a corrosion cave on the external side of the pipe in zone A.
- It is necessary to define the Stress, and Strain State (SSS) at the corrosion cave to assess the strength of the pipeline.
- The conventional means to define the SSS on a computer would require a super computer with large calculating capabilities. This makes the calculations extremely expensive.

Slide 5

A Better Way

- To define the SSS in a defective zone, a simple beam model of the whole section (500 m long) is considered (Fig. 2).
- This beam calculation is performed rather quickly and allows assessment of the general distribution of stress in the pipeline and define the most loaded parts.
- The calculation results are used to form boundary conditions for solving the second stage task of local stresses near a defect.
- On the second stage a pipeline section with the curve of 20m, where the defective zone is located, is considered.

Slide 6

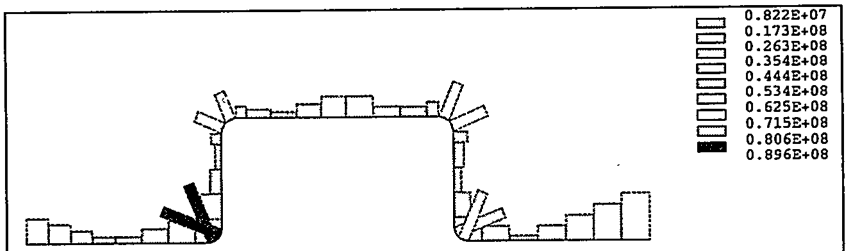


Figure 2 - Stress intensity at the pipeline section.

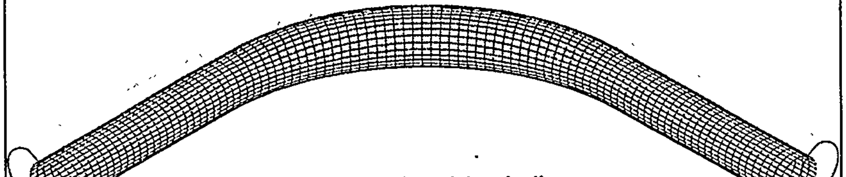


Figure 3 - Deformation of the pipeline curve where a corrosion defect is located.

Slide 7

Methods - Cont.

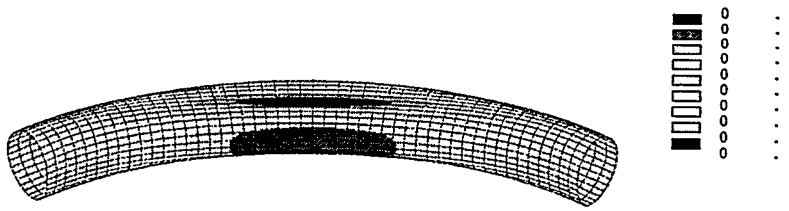


Figure 4 - Stress intensity at the external side of the pipeline curve where a corrosion defect is located.

- On the third and final stage, a picture of the SSS in the defective zone is calculated with the help of a detailed finite element model adjacent to the flaw in the pipe section (Fig 2.).

Slide 8

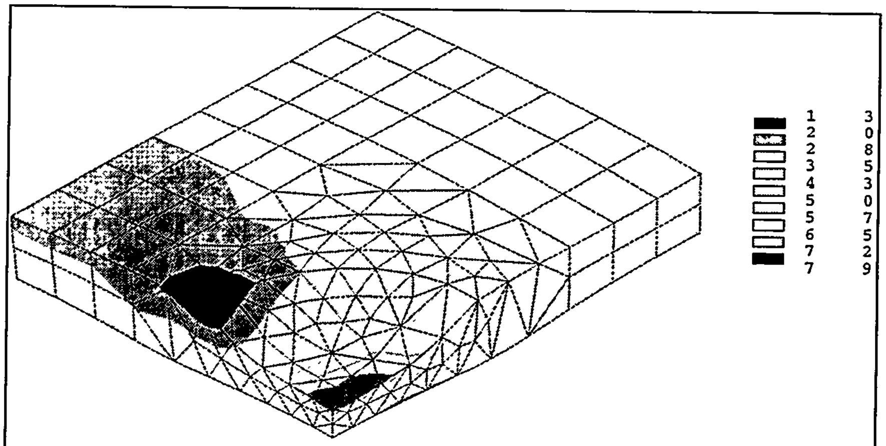
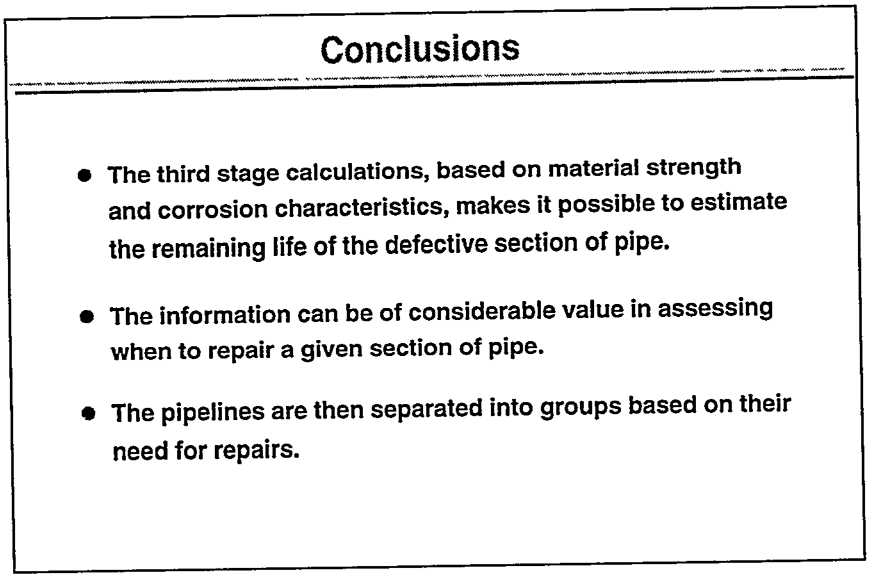


Figure 5 - Stress intensity in the defective zone.

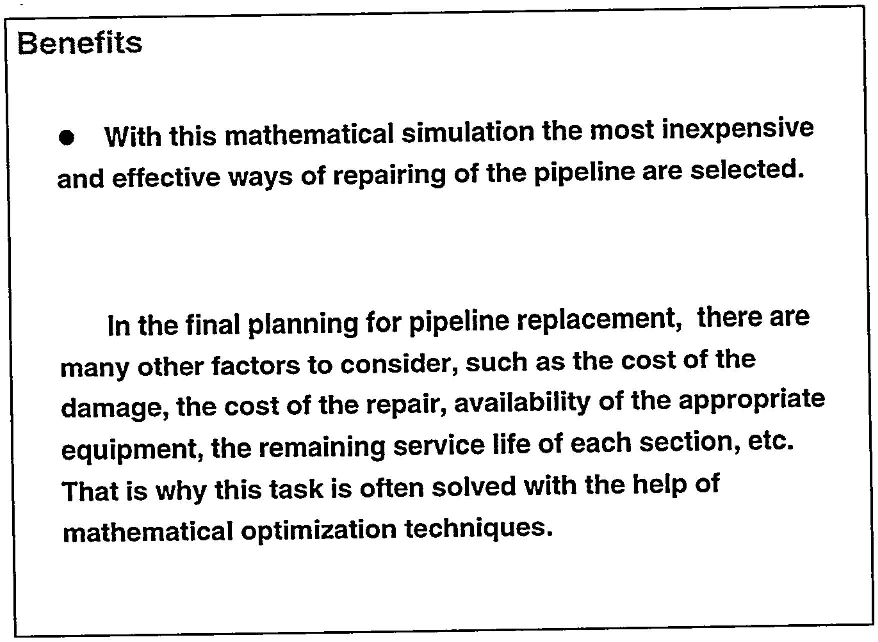
Slide 9



Conclusions

- The third stage calculations, based on material strength and corrosion characteristics, makes it possible to estimate the remaining life of the defective section of pipe.
- The information can be of considerable value in assessing when to repair a given section of pipe.
- The pipelines are then separated into groups based on their need for repairs.

Slide 10



Benefits

- With this mathematical simulation the most inexpensive and effective ways of repairing of the pipeline are selected.

In the final planning for pipeline replacement, there are many other factors to consider, such as the cost of the damage, the cost of the repair, availability of the appropriate equipment, the remaining service life of each section, etc. That is why this task is often solved with the help of mathematical optimization techniques.

INTERNATIONAL SURETY CENTER

Intentionally left blank

Concept on the Establishment of the International Surety Center for Energy Intensive and High Consequence Systems and Infrastructures

G. S. Klishin and V. E. Seleznev,
Conversion Design Bureau
Russian Federal Nuclear Center (RFNC)-All-Russian Research Institute
of Experimental Physics (VNIIEF)
Russia

V. J. Johnson and P. I. Pohl
Sandia National Laboratories*
Albuquerque, New Mexico

Background

The natural gas production and distribution industry in the Russian Federation has become a major customer of the atomic laboratories formerly charged with the design responsibilities for the USSR nuclear weapons program. The gas industry has found that the large reserve of technical talent combined with the resources and test facilities at RFNC-VNIIEF can and is helping to solve many difficult technical problems in safety and reliability of natural gas pipeline distribution systems. Studies by the VNIIEF analysts coupled with fact-finding studies in the United States have shown that the difficult, costly, and potentially very dangerous technical problems raised by the aging gas industry infrastructure in Russia are symptomatic of other surety problems that are facing the international community.

Understanding the significance of the natural gas industry infrastructure issues and generalizing them to broader Russian and world surety concerns allowed the RFNC-VNIIEF leaders to enlist the Ministry of Russian Federation for the Atomic Energy and to address the leaders of Sandia National Laboratories with a proposal to create an *International Scientific and Technical Surety Center for Energy Intensive Systems.*

A proposal to create an international center was included in the Gore-Chernomyrdin Commission (Report of the Nuclear Energy Committee of the Joint Russian-American Commission on Economic and Technological Development, Washington, D.C., February 1997). The Minister for the Atomic Energy of Russian Federation V. Mikhailov and

* This work was performed at Sandia National Laboratories, which is operated by Lockheed-Martin Corporation for the United States Department of Energy under Contract DE-AC04-94AL85000.

Acting United States Secretary of Energy, C. Curtis signed the Report. The Report states that the main goal of establishing the center will be coordination of the efforts of the Russian and American parties to address surety problems in engineered system with the intent of reducing impact to humans and the environment (the Report, Section 5, p.10). This goal clearly envisions a scope beyond the gas and oil industry to one in which other appropriate surety issues will be addressed.

To implement the goal of the Gore-Chernomyrdin Commission, a working meeting to discuss the creation of the Center was held in Albuquerque, New Mexico on April 28 through May 1, 1997, where a delegation of the RFNC-VNIIEF and SNL representatives met to find a common understanding of the objectives and structure for the Center. The result of this meeting is a Memorandum of Understanding signed by Radii I. Il'Kaev, Director of Russian Federal Nuclear Center - VNIIEF, and C. Paul Robinson, President of Sandia National Laboratories, pledging collaboration on developing an *International Surety Center for Energy Intensive and High Consequence Systems and Infrastructures.* Further discussions have led to some draft plans for structure and direction. The remainder of this talk is a description of the collaboration efforts to date.

Objectives

The first objective of this Center is to convert the intellectual and facility reserve built for nuclear weapons programs to the complex system surety problems of the international community. A second objective is to create an information conduit for communicating across the international community concerned with these important systems. The third objective is for Sandia and VNIIEF to coordinate teams of partners among the surety community to identify and solve appropriate system surety problems.

Title

The title highlights specific areas of mutual interest we determined are important in the establishment of this Center. "Surety" has similar, but sometimes subtly different meanings to different parts of the community that we wish to include as partners or collaborators in this effort. We define Surety as "confidence that a system will perform in acceptable ways in both intended and unintended circumstances." In addition to safety and security, this definition allows inclusion of issues on quality and reliability that impact the operation of complex systems. "Energy Intensive Systems" is a phrase used extensively in Russia to refer to systems that store or move a large amount of energy. Uncontrolled release of that energy could result in expensive loss of resources, life, or damage to the environment. "High Consequence Systems and Infrastructure" is an American phrase that is frequently used to describe complex systems ranging from nuclear weapons to transportation systems for people and products to electronic financial systems: any system which, if operated or if it failed in an unintended way, could result in extensive environment, human, or resource loss. In short, the name was chosen carefully to include, not exclude difficult problems.

Participants

We will embrace the participation of the international surety community. While VNIIEF and Sandia are taking a lead role in initiating this effort, we welcome and require participation and partnering with a large community of industrial, academic, professional, and government organizations. A cross-cutting approach will assure that the right stakeholders are assembled to address each different surety problem.

Early Russian participants are GAZPROM, the Russian natural gas consortium and the VNIIEF Conversion Design Bureau. The expertise provided by VNIIEF is optimal control analysis, structural analysis, failure case express analysis, and development and manufacture of gas industry control equipment.

Presently, active Sandia participants include the following groups, listed with their areas of expertise and a few of their more important recent non-weapon surety work:

The Nuclear Energy Technology Center, providing expertise in risk assessment and distributed system surety analysis. Current projects include the risk assessment of the vulnerabilities of distributed telecommunication systems and the application of Model Based Risk Management techniques to the oil and gas industry.

The Surety Assessment Center, providing expertise in system analysis and passive safety (first principles) methodology. Current work includes contributing to the FAA Maintenance and Inspection Program surety enhancements, developing Fuzzy mathematics application to surety problems, risk assessments and passive safety/risk assessment analysis of a centrifuge system.

The Applied Energy Technology Center provides expertise in oil and gas exploration, extraction, and storage technologies. General capabilities in geology and geotechnology and also available in this center.

The Information Systems Engineering Center, providing expertise in electronic system and telecommunication surety. Current work includes Prosperity Games on infrastructure with American industry, government, and institutions.

Several additional Sandia Centers that are organized into the Reliability Science and Engineering Council will be important contributors to the Joint Center as the projects and contacts develop. This Council was originally organized around the science of reliability, but is now re-organizing around the science of surety.

Initiation

A phased approach is being laid out for establishing the Center, which builds off of current efforts at VNIIEF and SNL. We are following in the trail-blazing path of the Russian/American Fuel Cell Consortium (RAFCO). Like RAFCO, Sandia and VNIIEF will provide joint Directors plus joint chairs for technical and strategic councils.

In Phase I, the VNIIEF/Sandia collaboration will focus on the gas and oil industry pipeline distribution systems. VNIIEF and Sandia are planning to co-host a workshop this fall or winter that will focus on identifying the surety problems associated with these systems. To participate in this workshop, please contact Mr. Gary Polansky or me. We will establish a foundation based on projects and contacts that VNIIEF and Sandia already possess. Several projects are either ongoing or have been proposed in this area at VNIIEF and Sandia. The projects and proposals include:

- Analytic and experimental evaluation of existing and newly developed operational diagnostic techniques for pipelines;
- Development of automated operational diagnostics data handling techniques for pipeline networks;
- Creating computer models of pipelines based on the results of operational diagnostics data and experimental research;
- Development of new algorithms for optimum accident-free gas flow through compressor stations and distribution pipelines;
- Development of simulation and test-site techniques to evaluate the environmental impact of construction and operation of gas industry pipelines and facilities.

The results of these projects should lead to:

- Improved pipeline safety and security
- Reduced environmental impact of natural gas infrastructure
- Reduced threat to life of industry workers and surrounding communities
- Reduced costs of gas transportation
- Reduced costs of pipeline and facility repairs.

We plan to create and operate an Internet page to provide a conduit for communicating surety information to the community.

In Phase II, projected to begin late in 1998, we plan to further broaden the connection of this Center with the global community by facilitating connections between the air transportation community, the nuclear energy community, and/or the telecommunications industry and parts of the international safety community. Once again, we can start with projects and contacts already available to VNIIEF and Sandia. Sandia is currently partnering with each of these communities on projects and we are planning to assist in building broader partnerships, as they will be effective for solving problems.

In Phase III, we should see the Center established as an organization recognized as an effective communication entity that helps to bring people and organizations together to address major technological issues.

Finance

The initial phases of this collaboration is expected to be funded by various sources internal to SNL and VNIIEF and by sources external to these organizations. Both SNL and VNIIEF will incorporate projects and contracts already funded. We anticipate external funding from organizations such as the Initiative for Proliferation Prevention, (IPP) and International Science and Technology Center, (ISTC). Ultimately, we anticipate direct contracts for each project. These projects will be self-supported by the stakeholders. Stakeholders may be industry, government institutions, universities, and professional organizations.

Potential Issues

Issues such as intellectual property rights, language differences and geographical distances between partners are not believed to be significant. There are several practicing models to address intellectual property rights, most notably IPP and RAFCO. Language differences are being removed as English is becoming the standard language of business. We have seen through three years of Sandia and VNIIEF cooperation in other areas that language is not a significant barrier. Finally, the geographical distances continue to contract as electronic communications continue to develop.

Conclusion

We believe that the Russian, US, and indeed, the global community has a large number of energy intensive and high consequence systems and infrastructure issues that can best be solved by an international community of scientists and engineers teamed with government and industrial entities. The representatives of VNIIEF and Sandia National Laboratories are initiating a collaboration that will address some of these difficult and high consequence problems.

Biography

G. S. Klishin

Biography unavailable

V. E. Seleznev,

Biography unavailable

P.I. Pohl

Phillip Pohl has a PhD in Chemical Engineering and is a Principle Member of Staff in the Nuclear Waste Management Programs Center. He has been with Sandia since 1990 where he has worked in Molecular Computer Modeling, Environmental Restoration and Infrastructure Surety. Prior to working at Sandia, Dr. Pohl was employed at the Pacific Northwest Laboratory, where he worked primarily in Envionrment and Waste Management Programs.

Victor Johnson

Victor J. Johnson is a Technical Staff Manager at Sandia National Laboratories. He has been with Sandia since 1980, working primarily in unique signal safety device design and nuclear weapon surety. Mr. Johnson has served two years as a special technical advisor to the Defense Programs Office of the Department of Energy in Washington, D.C. and is currently serving as the Strategic Programs Deputy to the Vice President of Production at Sandia.

Internal Distribution

5	MS 0490	Perry E. D'Antonio
1	MS 0101	Paul Robinson
1	MS 0102	John C. Crawford
1	MS 0319	Carl Vanecek
1	MS 0405	David D. Carlson
1	MS 0405	David E. Bennett
1	MS 0405	Kevin Maloney
1	MS 0405	Mary L. Young
1	MS 0405	Michael A. Dvorack
1	MS 0405	Michael P. Bohn
1	MS 0405	Nancy J. Dhooge
1	MS 0405	Roger Breeding
1	MS 0405	William H. McCulloch
1	MS 0419	Joe A. Baxter
1	MS 0428	Thomas S. Edrington
1	MS 0428	William C. Nickell
1	MS 0449	Phil Campbell
1	MS 0451	Laura R. Gilliom
1	MS 0481	Keith Ortiz
1	MS 0482	Kazuo Oishi
1	MS 0490	Angela Campos
2	MS 0490	Arlin Cooper
1	MS 0490	Debra Buttry
1	MS 0490	Daryl Isbell
1	MS 0490	Edwin Mauldin
1	MS 0490	Ronald D. Pedersen
1	MS 0490	Stanley D. Spray
1	MS 0490	Tonimarie Huning
1	MS 0491	John M. Covan
5	MS 0491	John V. Hancock
1	MS 0491	Mark E. Ekman
1	MS 0491	Michele Caldwell
1	MS 0491	Richard E. Smith
1	MS 0492	Clinton G. Shirley
1	MS 0492	Daniel A. Summers
1	MS 0492	David R. Olson
1	MS 0492	Douglas Loescher
1	MS 0492	Gary A. Sanders
1	MS 0492	James F. Wolcott
1	MS 0492	Kenneth C. Chen
1	MS 0521	Thomas J. Young
1	MS 0535	Larry J. Dalton
1	MS 0535	Raymond S. Berg
1	MS 0535	Victor Winter
1	MS 0627	Fred G. Trussell
1	MS 0627	George C. Novotny
1	MS 0633	Paul N. Demmie
1	MS 0637	Kyu S. Paek
1	MS 0637	Paul Konnick
1	MS 0638	Dwayne L. Knirk
1	MS 0638	Karl S. Ricker
1	MS 0638	Michael A. Blackledge
1	MS 0715	Christopher E. Olson
1	MS 0720	Phillip Pohl
1	MS 0720	Susan Carson
1	MS 0746	Laura Painton
1	MS 0747	Gregory D. Wyss
1	MS 0747	Kelly Hays
1	MS 0755	Daniel S. Horschel
1	MS 0755	Diana Blair
1	MS 0755	Mark Ivey
1	MS 0759	Bruce Berry
1	MS 0761	Rudy V. Matalucci
1	MS 0766	Doris E. Ellis
1	MS 0769	Dennis Miyoshi
1	MS 0829	Eric Grose
1	MS 0829	Heather W. Allen
1	MS 0829	Kathleen Diegert
1	MS 0829	Marcey L. Abate
1	MS 0835	Vicente J. Romero
1	MS 0860	Lorenzo Salgado
1	MS 0865	Marvin E. Morris
1	MS 0872	Victor J. Johnson
1	MS 0932	Wayne Burton
1	MS 0985	John H. Stichman
1	MS 1010	Margaret Olson
1	MS 1042	Jerry Hands
1	MS 1042	Merri Lewis
1	MS 1042	Yvette Harrison
1	MS 1070	R. E. Bair
1	MS 1072	Brent T. Meyer
1	MS 1115	Bob Alexander
1	MS 1138	Richard L. Perry
1	MS 1138	Sharon K. Chapa

1	MS 1138	Stephen D. Denman
1	MS 1231	Roger L. Hagengruber
1	MS 1237	Hank M. Witek
1	MS 1237	Patrick F. Chavez
1	MS 1380	Christie Stanley
1	MS 1380	Mary Monson
1	MS 9018	Central Technical Files, 8940-2
2	MS 0899	Technical Library, 4916
2	MS 0619	Review and Approval Desk, 12690 for DOE/OSTI

External Distribution

1 Bohumil Albrecht
SA-ALC/NWI
DoD
1651 First Street, SE
Kirtland AFB, NM 87117

1 Alfred V. Alderete
SA-ALC/NWIE
DoD
1651 First Street, SE
Kirtland, AFB, NM 87117-5617

1 John Andersen
65 Mercer Lane
Edgewood, NM 87015

1 Gilbert M. Baca
U.S. Air Force, NWI
1651 First Street, SE
Kirtland AFB, NM 87117

1 Thomas R. Baltes
SA-ALC/NWI
U.S. Air Force
1651 First Street, SE
Kirtland AFB, NM 87117

1 Farid Bamdad
DNFSB
625 Indiana Avenue, NW, Suite
700
Washington, DC 20004

1 Robert N. Bettis
Harmon Industries Inc
31003 E Argo Road
Grain Valley, MO 64029

1 Sandro Bologna
ENEA-CASACCIA]Via
Anguillarese 301
00060 Rome, Italy

1 J. Brackett
DSWA
6801 Telegraph Rd.
Alexandria, VA 22310

1 Thomas H. Brady
FCDSWA/FCPSN
1680 Texas Street, SE
Kirtland AFB, NM 87117-5669

1 Mark S. Burton
AFSC/SEWA
9700 G Avenue
Kirtland AFB, NM 87117

1 Ian Campbell
GPS Gas Protection Systems, Inc.
11686 Holly Street
Maple Ridge, BC V2X SH1
Canada

1 Edsal Chappelle
SA-ALC/NWI
DoD/U.S. Air Force
1651 First Street, SE
Kirtland AFB, NM 87117-5617

1 William P. Childress
Tybrin Corporation
745-D Beal Parkway, NW
Ft. Walton Beach, FL 32547

1 Jerry Childs
BDM International
1801 Randolph Road, SE
Albuquerque, NM 87106

1 Manny Comar
U.S. Department of Energy
19901 Germantown Road
Germantown, MD 20874-1290

1 Raymond Conrad
Lockheed Martin
9211 Corporate Blvd. 4A18
Rockville, MD 20850

1 Richard D'Orazio
Lucent Technologies
600 Mountain Avenue
Murray Hill, NJ 07974

1 Richard Davis
Vanderbilt University
400 24th Avenue South, Rm. 247A
Jacobs
Nashville, TN 37212

1 Jon L. Davis
Los Alamos Technical Associates
2400 Louisiana, NE, Bldg. 1, #400
Albuquerque, NM 87110

1 Robert B. Dobbs
SA-ALC/NWI
U.S. Air Force
1651 First Street, SE
Kirtland AFB, NM 87117

1 Gerald Dransite
Mine Safety & Health
Administration
U.S. Dept. of Labor
Box 251
Triadelphia, WV 26059

1 Steven A. Eide
INEEL
P.O. Box 1625
Idaho Falls, ID 83415-3850

1 Thomas Enger
Facility/Safety
Special Devices Inc
3431 N. Reseda Circle
Mesa, AZ 85215

1 James A. Ernst
United Defense LP
4800 East River Road M/S M387
Minneapolis, MN 55421-1498

1 Denise A. Fattor
FCDSWA/FCPS
1680 Texas Street, SE
Albuquerque, NM 87117-5669

1 Scott Ferson
Applied Biomathematics
100 N. Country Road, Bldg. B
Setauket, NY 11733

1 David Fike
Pantex Plant
Mason & Hanger Corporation
P.O. Box 30020
Amarillo, TX 79120-0020

1 Stewart R. Fischer
Los Alamos National Laboratory
P.O. Box 1663 M/S K557
Los Alamos, NM 87545

1 Terry H. Fogle
Los Alamos National Laboratory
M/S K403
Los Alamos, NM 87545

1 John S. Foster, Jr.
TRW
One Space Park, Bldg E-1, Room
5010
Redondo Beach, CA 90278

1 Robert T. Francis II
National Transportation Safety
Board
490 L'Enfant Plaza East, SW
Washington, DC 20594

1 Floyd R. Gallegos
Los Alamos National Laboratory
LANSCE-6 M/S H812
Los Alamos, NM 87545

1 Gilbert Garcia
SA-ALC/NWI
DoD/U.S. Air Force
1651 First Street, SE
Kirtland AFB, NM 87117-5617

1 John Garrick
PLG Inc
4590 MacArthur Blvd. #400
Newport Beach, CA 92660

1 Thomas K. Gibson
Tybrin Corporation
745-D Beal Parkway, NW
Ft. Walton Beach, FL 32547

1 Svetlana V. Gontcharova
RFNC-VNIIEF
607190 Nizhny Novgorod Region,
Sarov
Zhelezhodorozhnaya Str, 22a
Russia

1 Eugene G. Grewis
U.S. Department of Energy,
Retired
P.O. Box 970
Tijeras, NM 87059

1 Yacov Y. Haimes
Center for Risk Management of
Engineering Systems
University of Virginia
University of Virginia, Thornton
Hall
Charlottesville, VA 22903

1 James J. Hairston
Boeing Defense & Space Group
P.O. Box 3999 M/S 8Y-95
Seattle, WA 98124-2499

1 Christopher A. Hart
Federal Aviation Administration
800 Independence Avenue, SW
Washington, DC 20591

1 Richard E. Heck
UNOCAL
P.O. Box 4551
Houston, TX 77210-4551

1 Kay Houghton
Los Alamos National Laboratory
P.O. Box 1776 M/S F684
Los Alamos, NM 87545

1 Walter T. Hurt
System Safety 4.1.10.2 Bldg 1668
NAWCAD
48359 Standley Road, Unit 4
Patuxent River, MD 20670-1902

1 Ron Hyer
Los Alamos National Laboratory
P.O. Box 1663
Los Alamos, NM 87545

1 Jeff Irwin
U.S. DOE, Kirtland Area Office
P.O. Box 5400 MS-0184
Albuquerque, NM 87185

1 Theresa M. Isaacson
SA-ALC/NWIE
DoD/U.S. Air Force
1651 First Street, SE
Kirtland AFB, NM 87117-5617

1 Hank C. Jenkins-Smith
Department of Political Science
Univeristy of New Mexico
Albuquerque, NM 87131

1 Claes G. Johansson
Systecon
Box 5205
S-10245 Stockholm, Sweden

1 Margaret Ann Johnson
2530 SE 19th Place
Homestead, FL 33035

1 Malcolm Jones
AWE/Hunting BRAE
Room 117, Bldg D2, AWE,
Aldermaston
Berkshire, UK RG7 4PR

1 Orval E. Jones
12321 Eastridge Drive, NE
Albuquerque, NM 87112-4604

1 Joseph F. Judeikis
Mine Safety & Health
Administration
U.S. Dept. of Labor
R.R. 1, Box 251
Triadelphia, WV 26059

1 Peter T. Katsumata
Booz-Allen & Hamilton
523 West Sixth Street, Suite 650
Los Angeles, CA 90014

1 Kenneth L. Kiper
North Atlantic Energy Service
Corp
P.O. Box 300
Seabrook, NH 03874

1 Herbert Konkel
Los Alamos National Laboratory
P.O. Box 1663 M/S K557
Los Alamos, NM 87545

1 Olga Lambros
DoD-OASD (C3I)
U.S. Department of Defense
6000 Defense Pentagon, Room
3E151
Washington, DC 20301-6000

1 David O. Lee
DSWA
6801 Telegraph road
Alexandria, VA 22310-3398

1 Nancy Leveson
University of Washington
P.O. Box 352350
Seattle, WA 98195-2350

1 James D. Lloyd
NASA
300 E. Street, SW
Washington, DC 20546

1 Roger Lounsbury
Safety & Licensing Branch
Atomic Energy of Canada Ltd
Chalk river, Ontario KOJ 1J0
Canada

1 Richard Main
Lawrence Livermore National
Laboratory
P.O. Box 808 M/S L-703
Livermore, CA 94551

1 Tim Margulies
908 Marine Drive
Annapolis, MD 21401

1 Steven C. Martin
U.S. General Accounting Office
441 G Street, NW
Washington, DC 20548

1 Ronald G. Martinez
Los Alamos National Laboratory
P.O. Box 1663
Los Alamos, NM 87545

1 Al Matteucci
SA-ALC/NWIE
DoD/U.S. Air Force
1651 First Street, SE
Kirtland AFB, NM 87117-5617

1 Roger L. McCarthy
Failure Analysis Associates, Inc.
149 Commonwealth Dr.
Menlo Park, CA 94025

1 Richard W. Mensing
Logicon RDA
6940 S. Kings Highway
Alexandria, VA 22310

1 Ronald E. Morin
HQAFSC/SEW
U.S. Air Force
9700 G Avenue, SE
Albuquerque, NM 87117-5670

1 Peter Neumann
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025

1 Elisabeth Pate-Cornell
IE-EM Department
Stanford University
Terman Engineering Center, Room
351
Stanford, CA 94305-4024

1 Paul B. Pattak
Science Applications International
Corporation
20201 Century Blvd., 3rd Floor
Germantown, MD 20874

1 Mauro Pedrali
European Commission-Joint
Research Centre
Via E. Fermi
21020 Ispra, Italy

1 Stephen Pickett
Harmon Industries
3016 Kansas Avenue
Riverside, CA 92507

1 Chuck Piechota
Lockheed Martin Federal Systems
685 Citadel Dr. East, Suite 400
Colorado Springs, CO 80909

1 Donald K. Riddle
Lockheed Martin Federal Systems
9970 Federal Drive
Colorado Springs, CO 80921

1 Douglas Rigdon
DOE/Albuquerque Operatiions
P.O. Box 5400
Albuquerque, NM 87185

1 Catherine Rivera-Lyons
Los Alamos National Laboratory
P.O. Box 1663 M/S E549
Los Alamos, NM 87545

1 Timothy Ross
Department of Civil Engineering
University of New Mexico
Albuquerque, NM 87131

1 Frank Rowsome
U.S. Department of Energy
DOE/HQ DP-45
19901 Germantown Rd, MD
20874-1290

1 John Rushby
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025

1 Scott D. Sagan
Stanford University
320 Galvez Street
Stanford, CA 94305

1 Donna T. Schultz
SA-ALC/NWIE
DoD/U.S. Air Force
1651 First Street, SE
Kirtland AFB, NM 87117-5617

1 Richard L. Schwoebel
12010 Dusty Rose Road, NE
Albuquerque, NM 87122

1 Stephen L. Seiffert
Seiffert Consultant
9437 Thornton, NE
Albuquerque, NM 87109

1 Vadim Seleznev
RFNC-VNIIEF Arzamas-16
607190 Nizhny Novgorod Region,
Sarov
Zhelezhodorozhnaya Str, 22a
Russia

1 Roger C. Shaw
Software Systems Department
ERA Technology Ltd
Cleeve Road, Letherhead
Surrey, England

1 Sandra Smith
NSA/DoD
9800 Savage Road
Ft. Meade, MD 20755

1 John C. Snider
FCDSWA/FCPSA
1680 Texas Street, SE
Kirtland AFB, NM 87117-5669

1 Bill Stevens
P.O. Box 339
Arroyo Seco, NM 87514

1 Robert Stoddard
Lawrence Livermore National
Laboratory
P.O. Box 808 M/S L-125
Livermore, CA 94551

1 Victor F. Strachan
Litton Aero Products
21050 Burbank Blvd.
Woodland Hills, CA 91367

1 Lindia S. Summers
SA-ALC/NWIE
DoD/U.S. Air Force
1651 First Street, SE
Kirtland AFB, NM 87117-5617

1 Ray C. Terry
Naval Air System Command
48359 Standley Road, Unit 4 Bldg.
1668
Pax River, MD 20670-1902

1 William Valentino
MDS&DS-KSC, F110
McDonnell Douglas Space &
Defense Sys.
P.O. Box 21233
Kennedy Space Center, FL 32815-
0233

1 Kenneth Villareal
SA-ALC/NWI
DoD/U.S. Air Force
1651 First Street, SE
Kirtland AFB, NM 87117

1 Kurt Walecki
Booz-Allen & Hamilton Inc
523 West Sixth Street, Suite 650
Los Angeles, CA 90014

1 Craig S. Walker
Thiokol Corporation
Box 707
Brigham City, UT 84302-0707

1 Niles T. Welch
Raytheon Electronic Systems
528 boston Post Road (5-2-546)
Sudbury, MA 01776

1 Ted Wieskamp
Lawrence Livermore National
Laboratory
P.O. Box 808 M/S L-125
Livermore, CA 94551

1 Daryl J. Wilson
Dept. of Defense
9800 Savage Road
Ft. Meade, MD 20755

1 Donald C. Wunsch II
Department of Electrical
Engineering
Texas Tech University
Box 43102
Lubbock, TX 79409-3102

1 Francis Zelesky
Francis Zelesky, Inc.
22308 Whitehall Drive
winter park, FL 32792

1 Wayne C. Christensen
Project Manager
Institute for Safety Through
Design
PO BOX 303
Crystal Lake, IL 60039-0303