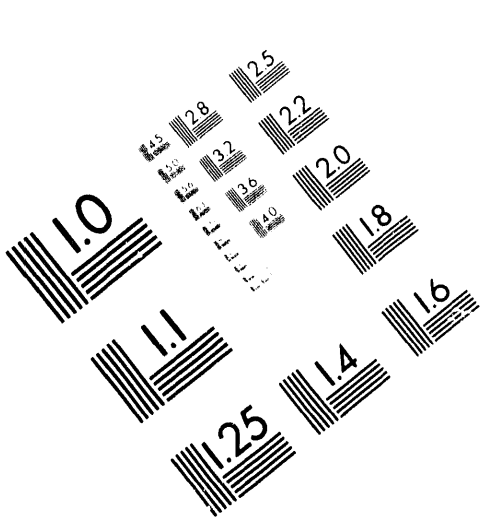
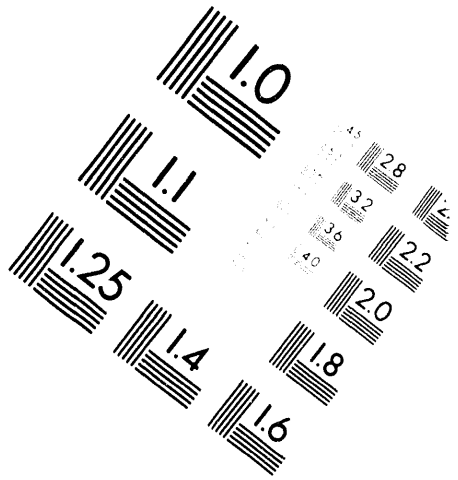


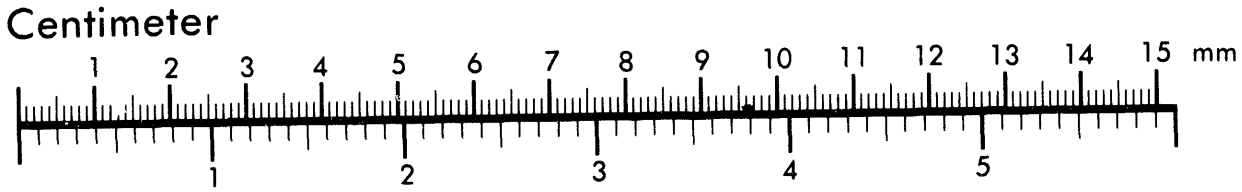
AIIM

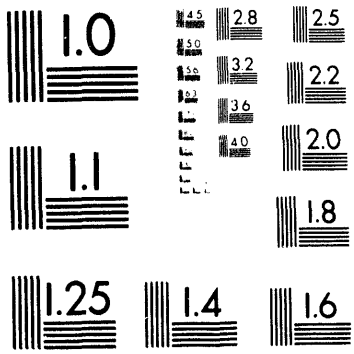
Association for Information and Image Management

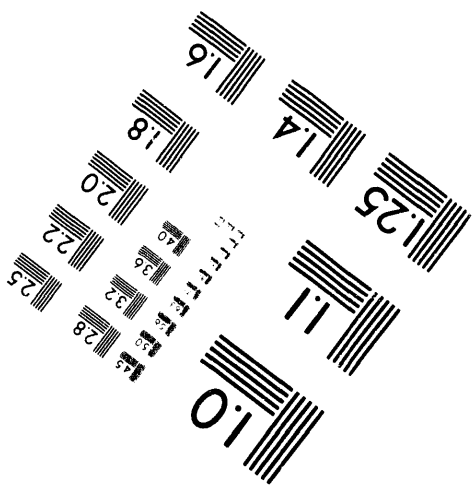
1100 Wayne Avenue, Suite 1100
Silver Spring, Maryland 20910

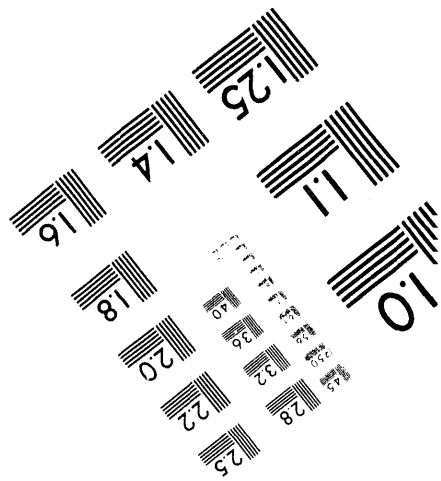
301/587-8202











MANUFACTURED TO AIIM STANDARDS
BY APPLIED IMAGE, INC.

1 of 1

CONF-9406159--3

SAND94-2098C

HIGH CONSEQUENCE SYSTEM SURETY

Issue 1
July 11, 1994

Gary T. Randall
Sandia National Laboratories
Mailstop 0319
Department 2645
Albuquerque, NM 87185-0319
USA

phone: (505) 844-6187
fax: (505)844-3593
e-mail: gtranda@sandia.gov

This work is supported by the United States Department Of Energy under contract DE-AC04-94AL85000

High Consequence System Surety

Issue 1
July 11, 1994

Abstract

High Consequence System Surety is an ongoing project at Sandia National Laboratories. This project pulls together a multi-disciplinary team to integrate the elements of surety into an encompassing process. The surety process will be augmented and validated by applying it to an automated system handling a critical nuclear weapon component at the Mason & Hanger Pantex Plant. This paper presents the development to date of an integrated, high consequence surety process.

High Consequence System Surety

Acknowledgment

This paper is the result of a team effort. High Consequence System Surety team members continue to meet and contribute in the development of a surety process. I would like to acknowledge and thank the High Consequence System Surety team.

Maria Armendariz, 6613
Jim Campbell, 6613
Joe Chiu, 12336
Elmer Collins, 12335
Larry Dalton, 2615
Bill Drotning, 2171
Mark Ekman, 12324
Ed Fronczak, 12334
Jack Gallagher, 2645
Steve Giles, 2615
Roxie Jansma, 9415
Todd Jones, 6411
Sabina Jordan, 5822
Stan Kawka, 5122
Tom Kerschen, 12335
Scott Nicolaysen, 2645
Gary Randall, 2645
Stu Rogers, 12326
Sharon Trauth, 13311

Introduction

The Surety Components and Instrumentation Center at Sandia National Laboratories, 2600, is managing a program for approaching surety from a systems viewpoint and applying that approach to a Department Of Energy need. The project is named High Consequence System Surety (HCS^2) and began in February 1994. The HCS^2 team is composed of representatives from a variety of organizations involved with surety at Sandia. The team meets often in developing a process that integrates the elements of surety into an encompassing process. Once the process is defined, it will then be applied to an automated system being proposed for installation at the Mason & Hanger Pantex Plant. The application of this process is expected to begin in the fall of 1994. This paper presents the team's work with a cautionary note that the process discussed continues to evolve.

Project Vision and Goal

The formation of the High Consequence System Surety project began with a vision. That vision is:

To Provide Seamless System Surety
For High Consequence Operations

In support of this vision, the HCS^2 project goal is:

To Develop A General High Consequence
System Surety Process And Validate It By Applying
It To An Automated Operation In The Handling Of
Special Nuclear Materials

Definitions

Definition of what the team means by the words used in the vision and goal statements is in order. First, what is surety? According to Webster's, surety is the state of being sure: a: sure knowledge b: confidence in manner or behavior. The traditional definition within the nuclear weapons complex and the military is that surety includes safety, security and use control. Sandia's Surety Assessment Center, 12300, includes reliability and quality as part of this traditional definition of surety. The HCS^2 project keeps to the traditional definition of surety with a few minor changes. The word "use" in "use control" is dropped to make the term more general in nature when addressing non-nuclear weapon audiences. HCS^2 also addresses reliability and quality as essential components of a system. Safety, especially in weapons, employs such concepts as isolation, incompatibility, inoperability, and independence. Security is the denial of unauthorized access where control is to provide positive measures to both assure authorized use and assure against unauthorized use. Reliability is the probability that an item will perform a required function under stated conditions for a stated period of time and quality the conformance to customer requirements and expectations. These five areas; safety, security, control, reliability and quality are referred to throughout this paper as the elements of surety.

What does seamless mean? Seamless is meant as the integration of all aspects of surety without gaps. The interaction between the surety elements is as important, if not more so, than any one individual element. A gap might very well be one of addressing only safety aspects of a system while not realizing another important aspect such as security.

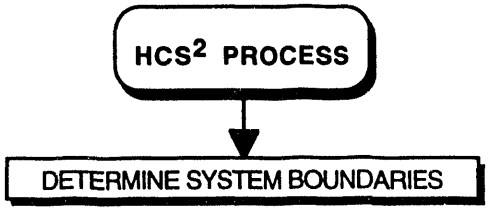
The term system is used to emphasize that this is an encompassing approach. Operations often consist not only of hardware but of software, procedures, and facilities. A systems approach is one of evaluating all aspects of the operation; recognizing that hardware, software, procedures, facilities, etc., are all interrelated.

High consequence varies as to the operation and the customer. The occurrence of a nuclear detonation is obviously of high consequence, but probably as significant a consequence to a manufacturer of silicon wafers is their investment in those

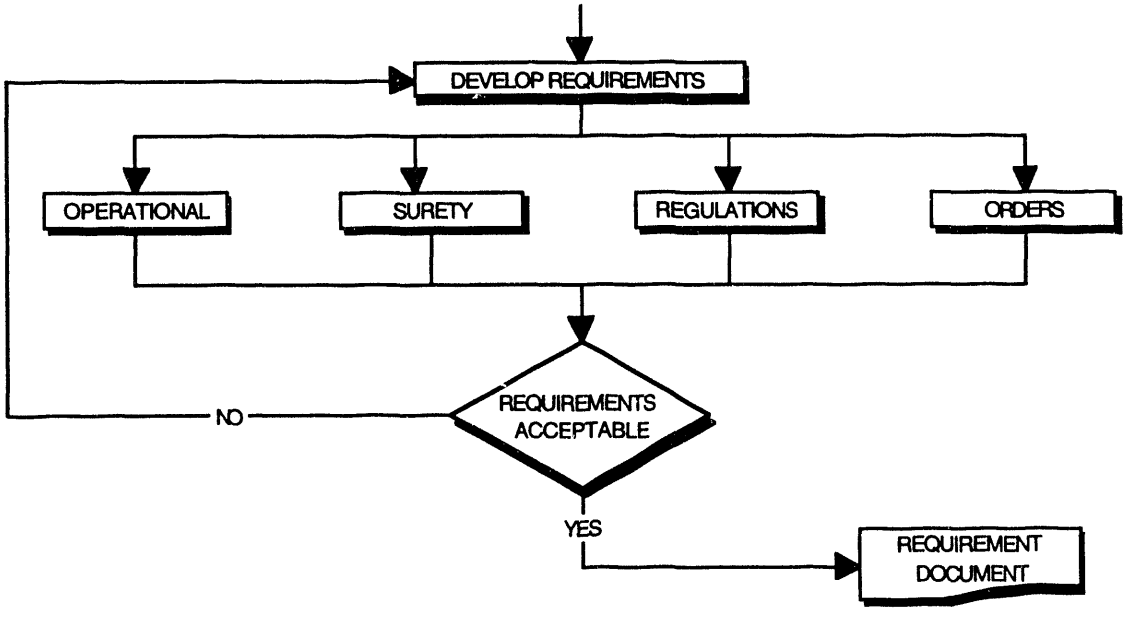
wafers if something should happen to them during manufacturing. High consequence is the combination of an event's probability of occurrence and of the event's severity. Analysis of a component in the system may show a high risk of failure, but the consequence may be of such low severity to the overall system if it does indeed fail that the combined result is not a high consequence.

High Consequence System Surety Process

The diagram in the Appendix shows our High Consequence System Surety process. The process flow follows.

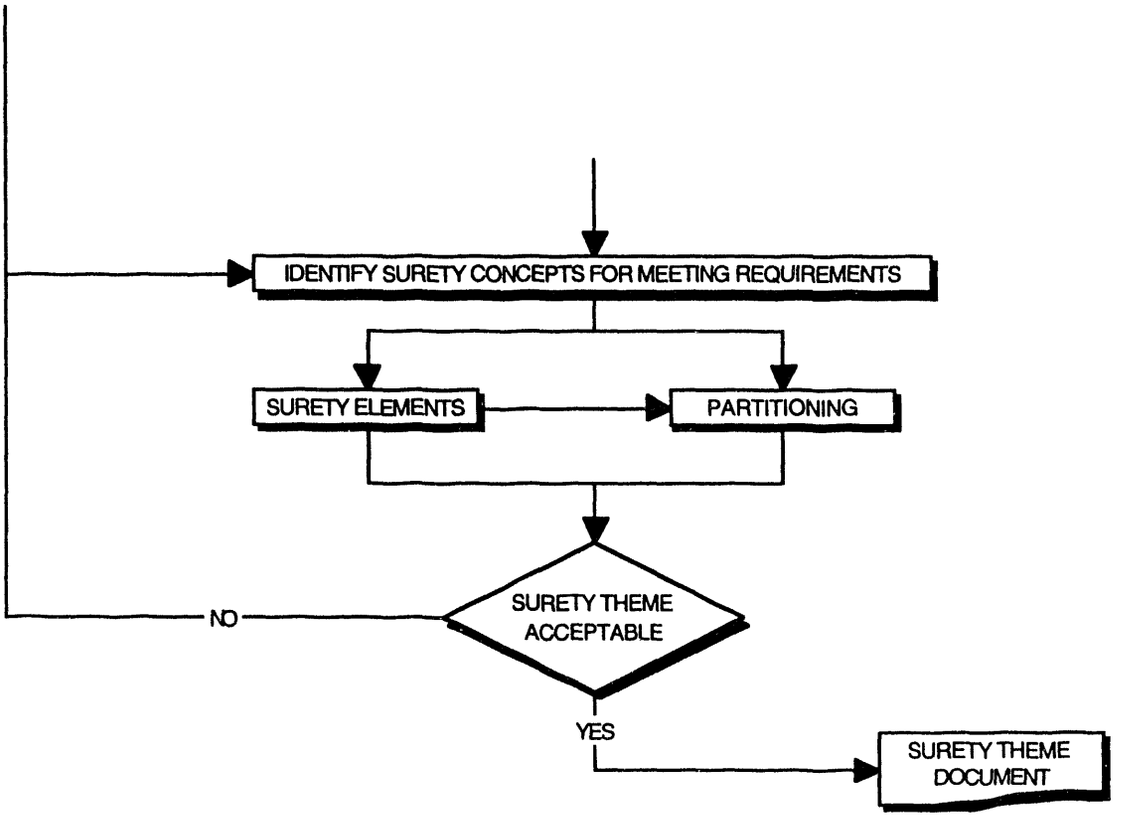


The first step in the process is to define the boundaries of the system. A clear understanding of the extent of the system is essential for developing system requirements. Depending on the system boundaries, the relative importance between the elements of surety will vary.



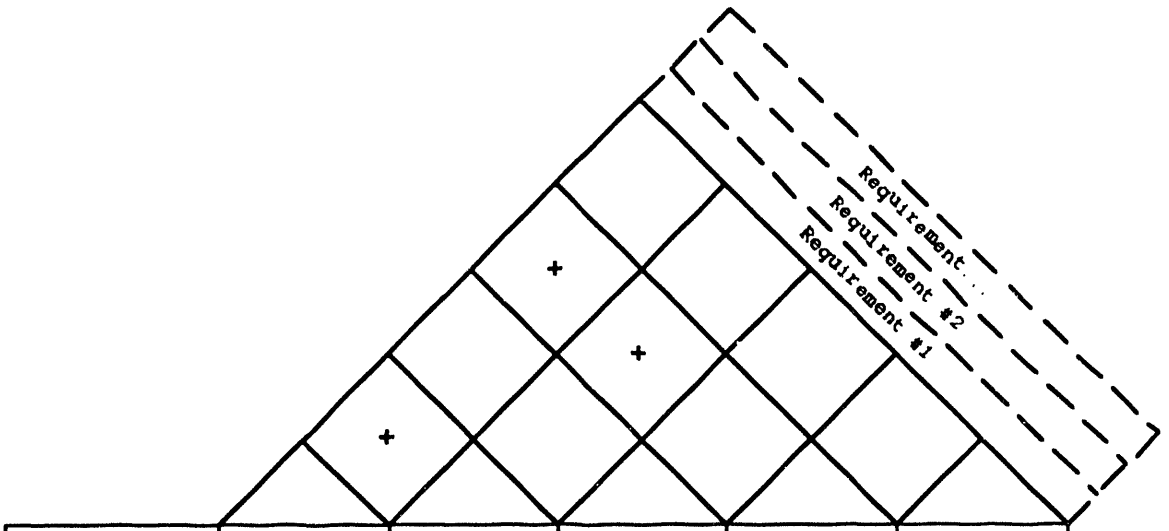
Next is to start developing the requirements. A concurrent team approach with representatives from both the system designers and surety experts should be formed. The purpose of this team is to identify traceable requirements. Traceability is important to demonstrate a quality process such that throughout the process the work being done is clearly attributable to a customer's requirement and is

measurable. Requirements for the system's performance can be developed with respect to its operation, surety elements, regulations and orders. The HCS^2 process focuses on the surety elements as an area of requirements that might not normally receive the attention that, for example, the operational requirements do. Regulations and orders for a system will vary depending on the owner of the system. For the nature of the work performed by Sandia, Department Of Energy orders and other government regulations are important. The process of developing these requirements is an iterative process as shown by the decision loop. The requirements should be acceptable to all team members. To help develop requirements, techniques such as Quality Function Deployment (QFD), which aids in the early detection of needs, deficiencies and conflicts, can be used. The resulting agreement is detailed in a requirement document, written by the system owners.



After the requirements for the system are defined to the best extent possible, the team identifies surety concepts for meeting those requirements. Each surety element is used to identify surety issues as early as possible and to develop conceptual principles and approaches to be used in meeting those requirements. This activity starts to show how the surety elements interact. This activity also shows that, given the system and its requirements, possibly not all of the surety elements will be important. A couple of techniques can be used to help uncover the surety concepts.

One might be a QFD-type tool where the top portion of the "house" is of particular value. If the requirements are listed against the various elements, the interactions can be explored in a systematic manner (see Figure 1).



REQUIREMENT	SAFETY	SECURITY	CONTROL	RELIABILITY	QUALITY
Requirement #1	✓	✓		✓	
Requirement #2			✓		✓
Requirement #3	✓		✓		✓
Requirement #4	✓	✓			✓
Requirement #5				✓	
Requirement...	✓				

Figure 1. QFD-Type Tool

Another possible tool would be a technique such as one being proposed in nuclear weapon use control[1] (see Figure 2). This technique is similar to the above in that the requirements (in this case requirements of all the surety elements rather than just use control requirements) are listed against the surety elements. It differs in that stages are added. Stages possibly represent differing states of the system in time.

---

[1] Security and Use Control Assessment Department, 12334, "Use Control Theme Development," January 13, 1994.

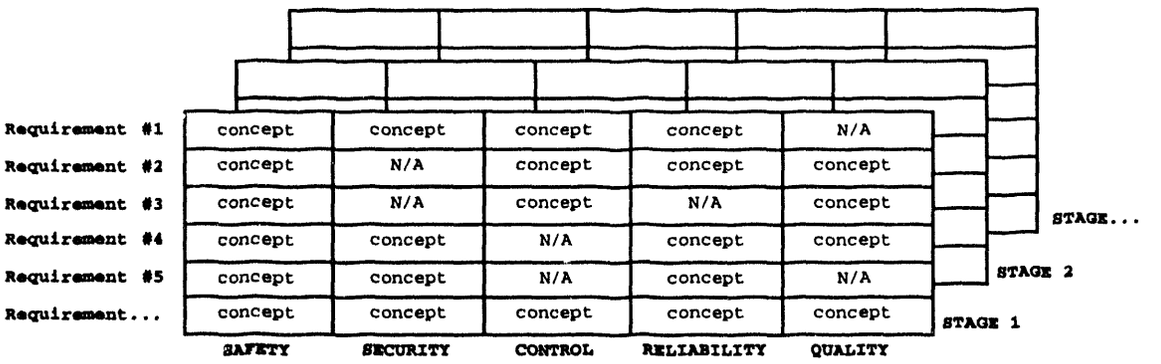
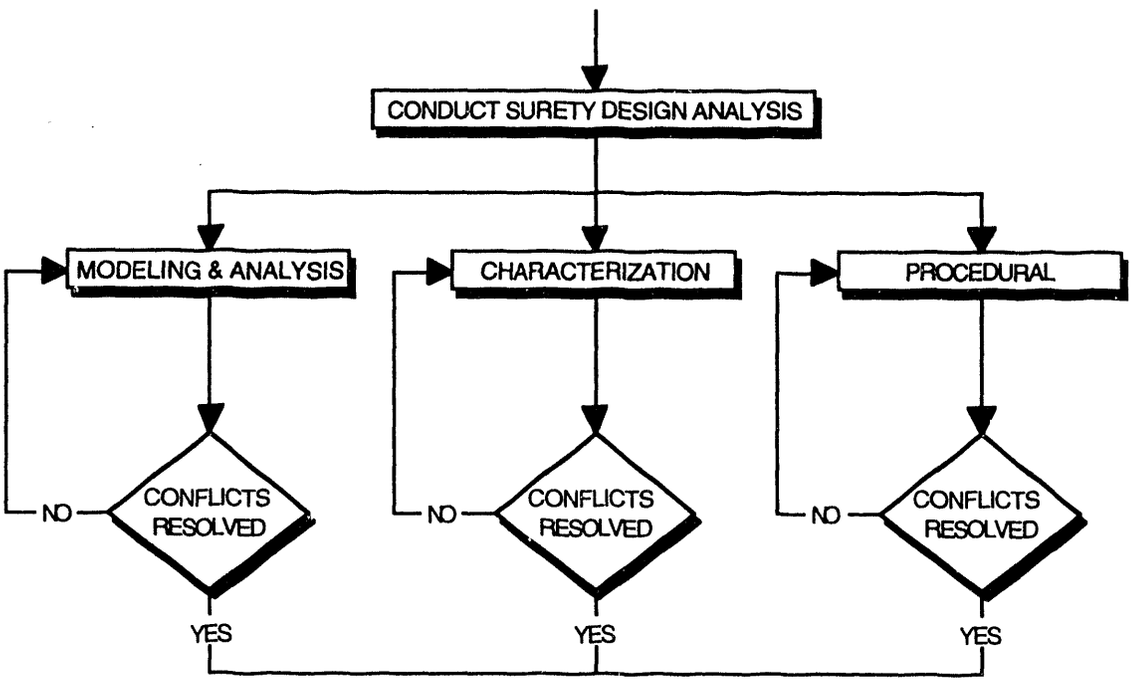


Figure 2. Use Control Theme-Type Tool

These techniques, by partitioning the surety elements against requirements, not only help to provide a consistent methodology to ensure nothing has been overlooked, but also identify and justify areas where no concepts are needed.

The process shows an iterative loop. The rigor of such techniques may require that the team re-address various surety concepts or even re-evaluate some system requirements. The result of identifying surety concepts is a surety theme. A document that details how each surety element addresses a system requirement.



After identifying which surety elements are important in the system, the next step is to start conducting surety design analysis; that is, to quantify the system. This fundamental analysis helps to identify potential problems, design errors,

process capability limitations, components that dominate risk or reliability and other issues. The analysis can conceptually be separated into three areas: modeling and analysis; characterization; and procedural. Several tools and techniques can be used to aid in quantifying the system, each one in essence representing a process of its own. A few examples follow.

Probabilistic Risk Assessment (PRA) uses tools and techniques to evaluate the safety of a system. This process involves first gathering data and becoming familiar with the system. Reviews of the design, process flow, documents, procedures, requirements, and standards occur. An operations analysis is performed where potential failure modes, sources of energy, and preliminary abnormal environments are identified. Then preliminary hazard matrices are developed followed by developing accident scenarios and system modeling. Event trees and fault trees are used as applicable. The integration of the event tree frequencies with fault tree probabilities aids in determining the dominant risk contributors and rank ordering of those risks. PRA provides information on which components really matter, have a higher vulnerability, and will potentially provide a greater safety enhancement in the system. Also, this modeling provides a validation of intuition.

Reliability modeling is a technique used to understand and characterize a product's design, using mathematical expressions, for quantifying its reliability. The Manufacturing Systems Reliability Department, 6613, at Sandia has developed reliability modeling software. This software, called RAMP (Reliability Analysis & Modeling Program), uses common cause analysis, failure analysis, fault trees, and failure mode, effects and criticality analysis (FMECA) to help identify those factors that dominate reliability, predictive uncertainty, and sensitivity. RAMP performs both repairable and non-repairable analyses. This design-for-reliability tool integrates data management, model development, model analysis (with uncertainties) with graphical output.

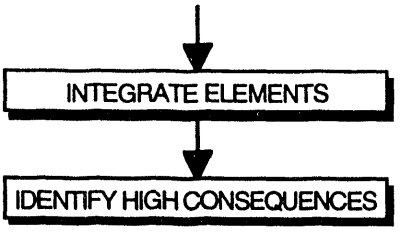
In the area of security, the protection system development process is used. First, the objectives are determined by defining what the adversarial threat is and what the target is (what is to be protected). Consideration of these objectives leads to protection system designs that employ countermeasures, such as, physical security, personnel security, procedural security, hardware security, software security and communications security. The design is then evaluated using vulnerability analysis, which includes the use of computer tools in the case of facility protection design.

Information surety is another process, one that encompasses many other surety aspects. Information surety involves identifying the appropriate levels of confidentiality, integrity, and availability of software and information in an information technology context. The process is one of identifying the information surety requirements, identifying hazards, establishing surety objectives, and recommending, integrating and implementing techniques and approaches to mitigate the hazards.

The control element of surety uses a process similar to that of security, the major difference being the level of implementation. This is especially true when the system involves nuclear weapons. However, for non-nuclear weapon applications the distinctions between control and security may become blurry.

Quality processes use tools to aid in statistical process capabilities and control methodologies. Also available is a Sandia procedure that defines a concurrent process to qualify processes and products.

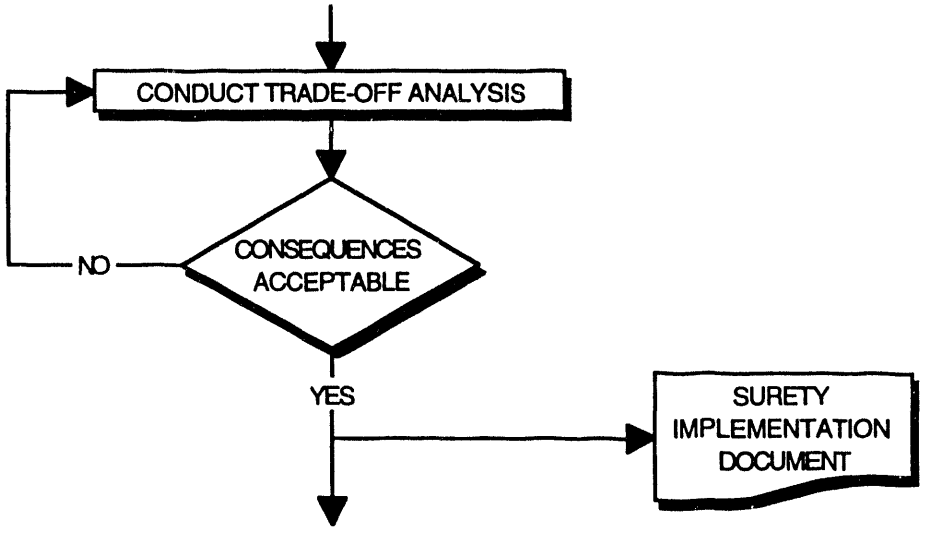
As a part of conducting surety design analyses, how one handles software is still being discussed within the team. What does it mean to have software surety and how does one go about achieving it? The HCS^2 team is currently taking an approach of using tools such as risk assessment and reliability modeling to identify the high consequence items. When software is involved in those models, it is more than likely treated as a "black box" and assigned a probability of failure of one. Refined analysis occurs when the subsystem that includes this software is identified as a high consequence subsystem. The HCS^2 team is exploring various techniques to open up this software "black box" and understand the software design better.



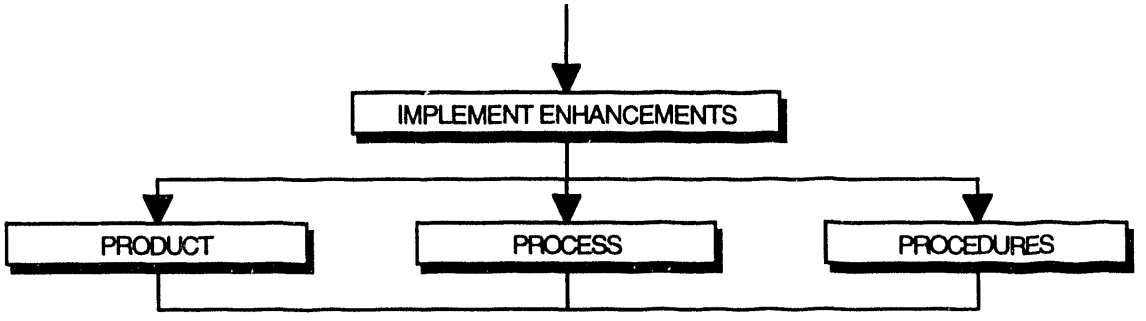
The HCS^2 process shows that individual surety element analyses may very well result in conflicts with some requirements. These conflicts should be resolved between the surety analysts and system customer. Once individual conflicts are resolved, the integration of all the surety elements occurs. The HCS^2 team believes this to be a key step. As mentioned, understanding the interrelationships between the elements of surety is essential. A safety

analysis might point to the need for a safety device to prevent an unwanted event in an abnormal environment scenario unless human intent is present. However, the addition of such a safety device could degrade the reliability of the system with additional hardware that can fail.

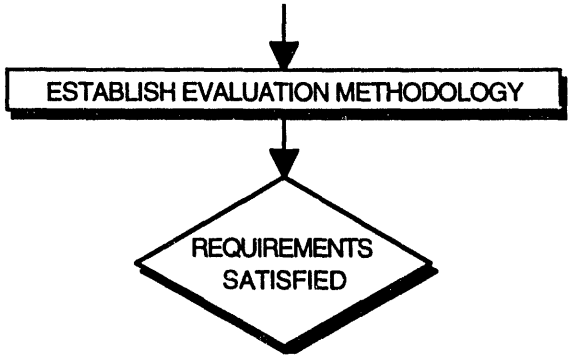
The high consequences of this integrated surety system can now be identified.



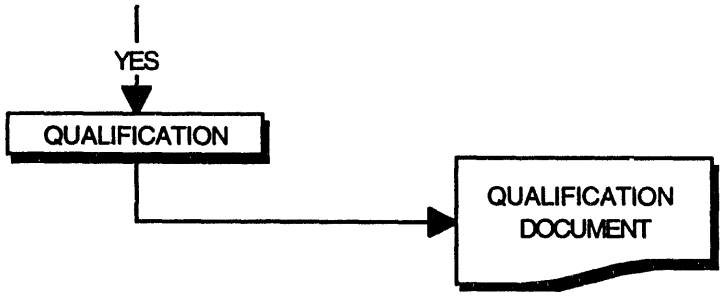
How does one decide whether the addition of a safety device is more important than maintaining a system reliability requirement? What is a proper balance? The HCS^2 process proposes that the team perform trade-off analyses. With the models in place, "what if" exercises can be conducted. Ultimately the system customer must decide what high consequences are acceptable. This decision should be captured in a surety implementation document, a document that details the analyses, the decisions of what is acceptable, and what approaches will be used to mitigate unacceptable consequences. This document should also be traceable back to the requirements to insure they are being satisfied.



The process then flows to realizing those enhancements as included in the implementation document. These enhancements can be categorized in terms of product (e.g., hardware and software devices), process (e.g., using a different manufacturing technique), or procedures (e.g., implementing a two person rule).



Establishing evaluation methodologies such as tracking procedures, verification of processes, and testing of the hardware, is important. This not only allows you to determine if the team has met the system requirements, but the gathering of data allows one to continually enhance the accuracy of the models.



Once the requirements are satisfied, the system is "qualified." Qualification activities are being conducted concurrently throughout the entire process using a team approach. This process is one of assuring that the system and associated processes are capable of meeting customer requirements, design definition, and production readiness. The final result is a formal qualification document.

Since the systems being addressed in this process involve high consequence operations, independent assessment may be desirable. Independent assessors, people who have not been involved with the day-to-day workings of the team, review the process. This review should occur periodically throughout the process, concluding with an assessment when the process is "finished."

Application

The first application of this process will be a remote, automated critical nuclear weapon material handling operation being proposed for the dismantlement and production of nuclear weapons at the Mason & Hanger Pantex plant. In particular, the system is called the Weight And Leak Check System (WALS) and is being designed within Sandia's Intelligent Systems & Robotics Center, 2100. By applying the HCS^2 process to the WALS project, WALS serves as a vehicle to help develop the HCS^2 process and in turn, validates the process.

Objectives

The objectives of the High Consequence System Surety project are threefold: first, to be able to offer a general surety process; second, to offer design verification and design enhancements to the WALS project, emphasizing continuous process improvements with focus on up-front, designed-in surety; and third, to offer a source of surety data that can be used in documentation required by the Department Of Energy prior to granting approval for the WALS project to begin operations.

Example

To illustrate the HCS^2 process, the following is a very brief, non-inclusive, *hypothetical* example. Let's consider a smart credit card, that is, an electronic (contains a microprocessor within the plastic) credit card. Representatives from the smart card designers and surety experts have been called in to form a concurrent team to design in surety in a quality manner. The first step of the process is to determine the system boundaries. In this example, a boundary might just be that of the smart card itself. An increasingly larger boundary would include both the card and its reader. Increasing the boundary again, the system could include not only the card, the reader, but the building or facility that contains the reader. Yet again, the system boundary could include the card, its reader, its building and additionally, the process of mailing the card from a banking institution to a customer. Clearly, depending on the choice of the system boundaries, the requirements and the elements of surety that are important will vary. For

this example, let's take the narrowest view, that of the smart credit card by itself.

The next step is to develop requirements. Requirements often can be categorized into operational, surety, regulatory or other orders. For our example, the following requirements are known at the start of the design.

Operational:
- retain 2,000 bytes of data
- operate from 0°F to 120°F
- survive and remain functional from -32°F to 150°F
- have a two year life

Surety:
- maintain the customer's confidentiality

Regulation:
- meet all applicable ISO standards for credit cards

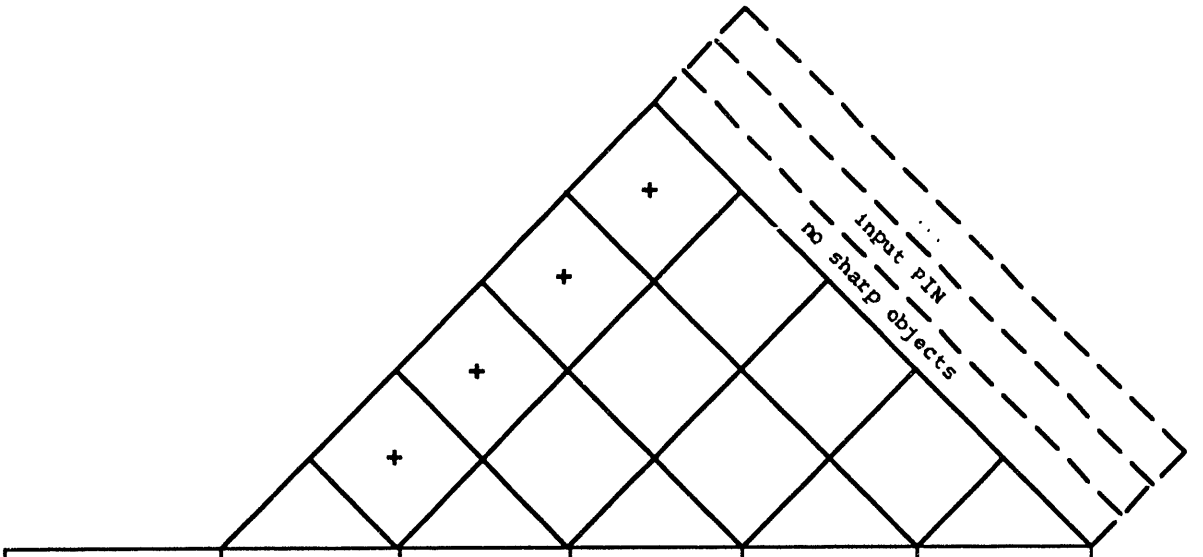
Orders:
- N/A

The team starts to review these requirements and finds them lacking in many areas, especially in surety. After several discussions, it is determined that additional surety requirements are needed, such as:

- there shall be no sharp objects that may harm a person (e.g., the card is used as a windshield ice scraper and cracks in half)
- before performing any operations, the card must process and accept a customer's Personnel Identification Number (PIN)
- the card should only allow ten attempts of the PIN
- once ten attempts have been made, the card shall become inoperable

The team reviews and accepts these requirements. As owners of the system, the designers take responsibility, with the aid of the team, of writing the Smart Credit Card Requirement Document, Issue 1.

To identify the surety element concepts that will be analyzed, the following QFD-type matrix is used.



REQUIREMENT	SAFETY	SECURITY	CONTROL	RELIABILITY	QUALITY
no sharp objects	force probe				
input PIN		PIN compromised			
ten attempts		algorithm defeated			
inoperable after ten			destroy stitch bonds		

The extension of this technique to all of the system requirements leads to a thorough system examination, one that will in all likelihood require changes to the requirements. The resulting surety theme document records what elements of surety will address what requirements.

Several issues arise for the team during the "Conducting Surety Design Analysis" phase of the process. For example, risk analysis shows that the risk of guessing a card's PIN is rather high since historically, people use simple PINs. The team refines the requirement by taking a conservative approach that it is a given, if the card is stolen, that useful customer information is available. Such would be the case if the entire contents of a purse or wallet are stolen and the customer's birth date, addresses, telephone numbers, whatever, are available.

Integrating the elements together is another enlightening task for the team. The analysis for keeping track of the attempts shows a strong correlation with how reliable the software algorithm is. After understanding the interactions, the high consequences are identified. For the smart card, analysis shows that the highest ranked consequences are the reliability of keeping track of the PIN attempts and the probability of a successful attempt within ten attempts. The

team decides that neither of these consequences are acceptable and must be mitigated.

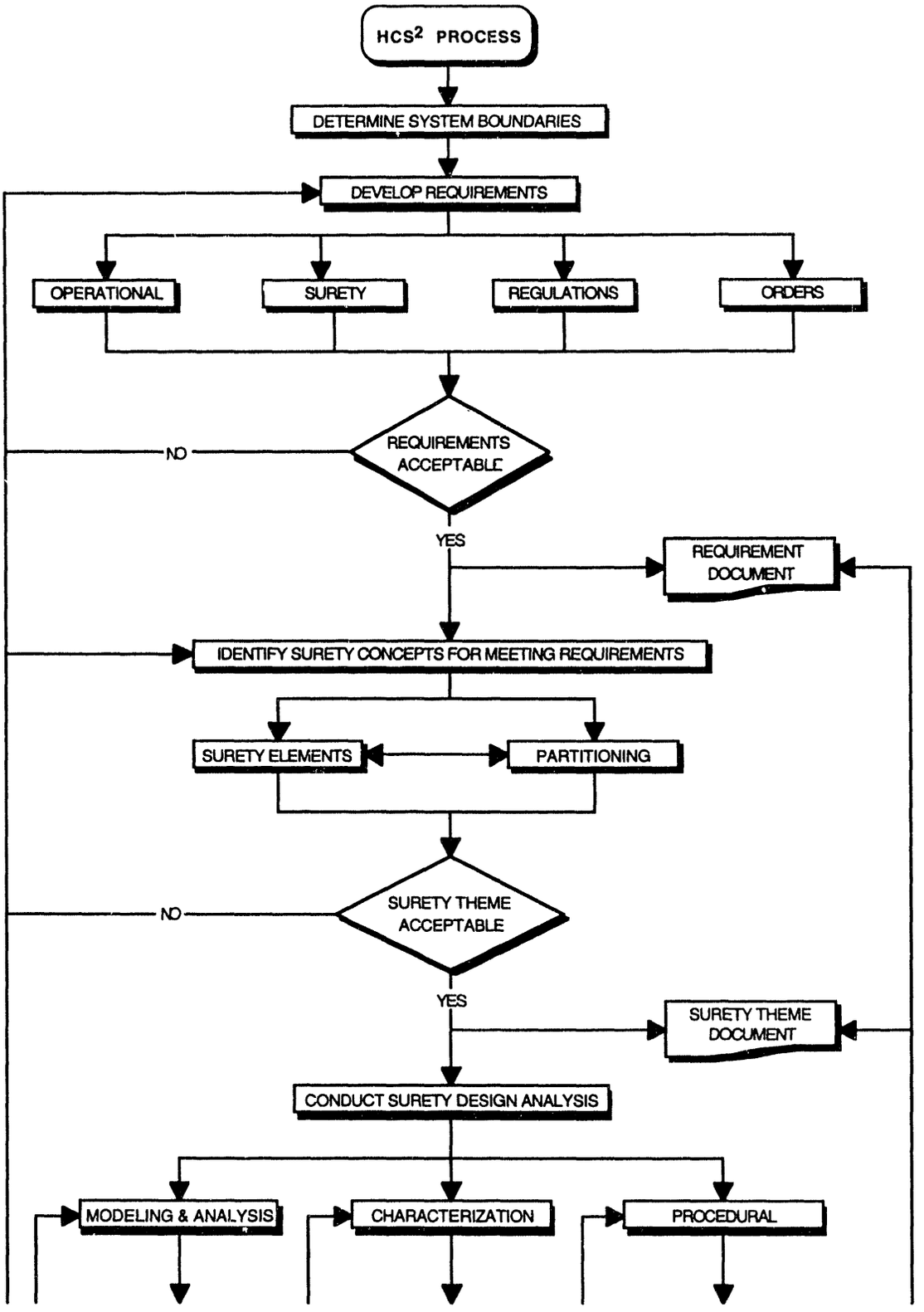
After conducting several trade-off analyses, the designers decide that the consequences would best be mitigated by reducing the attempts to three. Also, the team decides to include redundant hardware and software for the attempt algorithm, at the expense of reliability. All of this is documented in the Smart Card Surety Implementation Document, Issue 1.

While the necessary design changes are being made as agreed to in the implementation document, the team decides on evaluation methodologies. Since the risk model lacks accurate information on how often the limit of attempts is reached with the card then becoming inoperable, a procedure is put in place to track customer complaints and theft reports. Newer data as it becomes available is fed back into the model and the analyses are continuously updated.

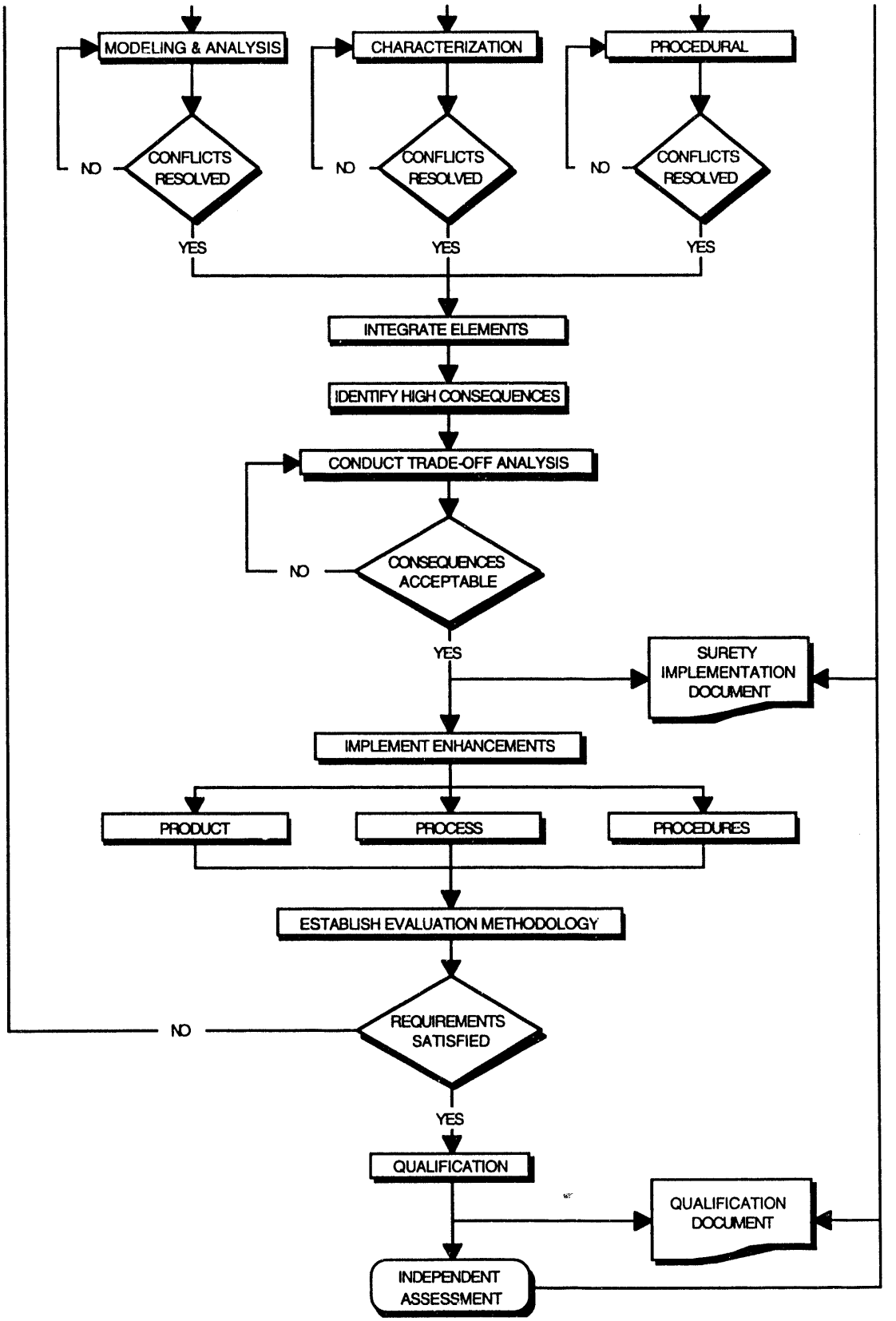
The team verifies having met all the requirements and wraps the project up with a qualification document. A team, composed of members from different parts of the company (people not involved in the day-to-day decisions), performs a successful, independent assessment of the card.

APPENDIX

High Consequence System Surety Process Flow Chart



High Consequence System Surety Process



High Consequence System Surety Process (continued)

DATE
FILMED
11/01/94
END