System Safety Based on a Coordinated Principle-Based Theme

J. Arlin Cooper, Ph. D.; Sandia National Laboratories, Albuquerque, NM

Abstract

In this paper, we demonstrate a logical progression for the identification of assets, threats, vulnerabilities, and protective measures, based on a structured approach that incorporates the results of the previous paper. We utilize a logical structure for identifying the constituents of the problem, derive appropriate applicable principles, and demonstrate a technique for incorporating the principles into a coordinated safety theme. We also show how to qualitatively assess such generally non-quantifiable items such as safety-component and safety-system response to severe abnormal environments. An illustrative example is followed step-by-step through to a safety system design approach and a safety assessment approach.

Introduction

The general approach is illustrated here through an example, generally representing a test rocket launch scenario, where the concern is the potential for loss of life. This specific objective is done in a very general sense, and the treatment is intended only for consideration of the possible design and assessment strategies involved. No implication of completeness or even familiarity with the details of the launch operation process should be inferred. It is expected that someone who was more familiar with the scenario described might find this approach useful while treating the details as only experts in the field could do. One would ordinarily utilize a system diagram to aid in the processes described below. We will omit that here, since the example is only illustrative.

In our example, we will cite only one asset for simplicity: loss of life. However, the lives at potential risk are the workers in the launch area, people on the ground along the flight path and near the impact area, and people in the air along the flight path, which will be treated here as three separate situations, each with its own idiosyncrasies.

Implementation of Safety Theme

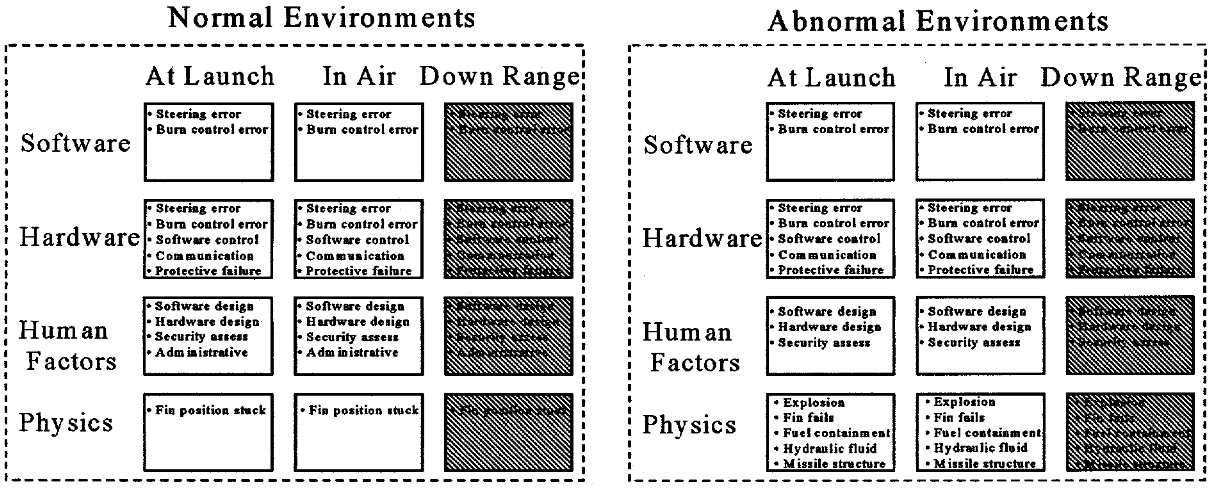
In the previous paper, an overall strategy was delineated and a menu of protective measures was described. Next, implementation (and assessment of the implementation) involves matching vulnerabilities against protective measures in order to check whether or not all vulnerabilities have been satisfactorily considered. For the example scenario, we have indicated a few protective measures in Figures 3-6. They are organized according to a rough qualitative order of effectiveness and cost-effectiveness, ranging from most effective first to least effective last. The "effectiveness" is judged by whether or not a passive first principle can be responsible, to what degree the protective measure reduces some vulnerability or (more preferably) vulnerabilities, and how cost-effective it is. In each figure, the threats addressed are indicated by shading over the appropriate matrix entries. Note that in an actual application, vulnerabilities would be addressed individually, but in this illustration, we are treating them by categories. We would also be more specific about ranking protective measures, since neither the shading nor the number of boxes shaded directly indicates effectiveness.

DISCLAIMER

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, 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 or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

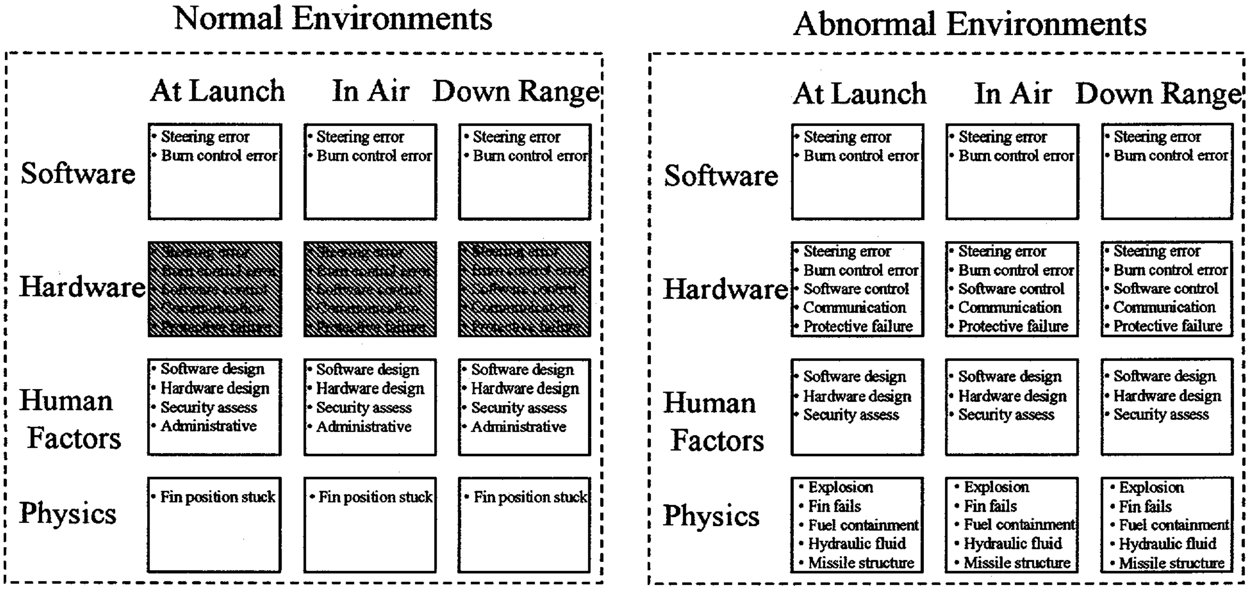
DISCLAIMER

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



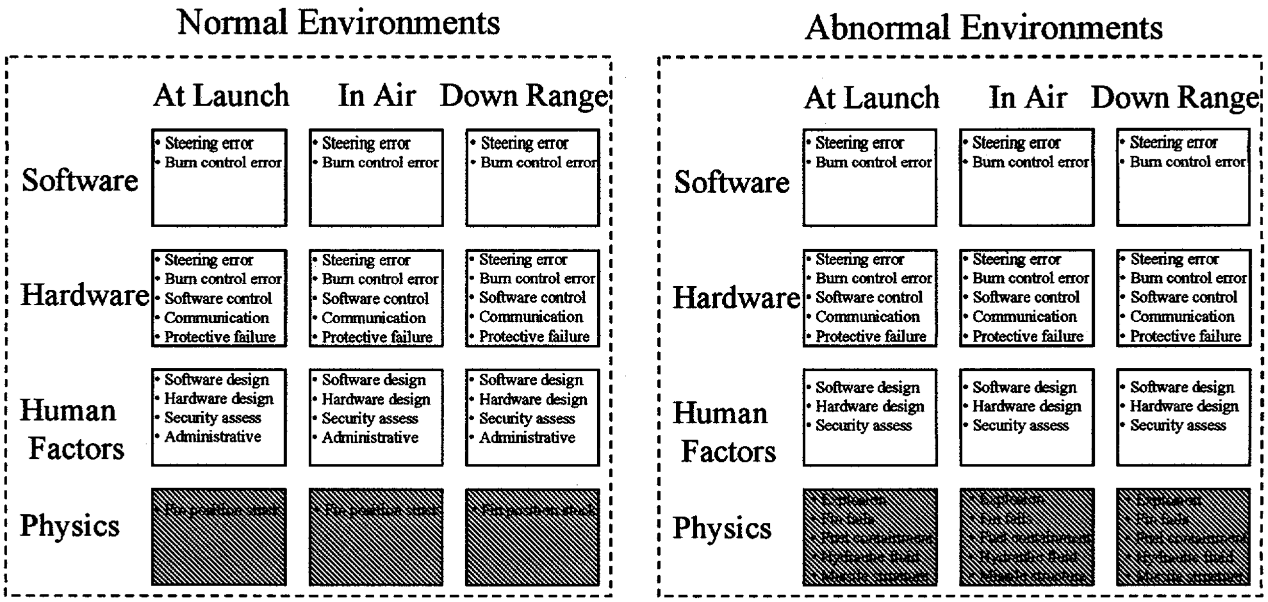
	Normal Environments			Abnormal Environments		
	At Launch	In Air	Down Range	At Launch	In Air	Down Range
Software	• Steering error • Burn control error	• Steering error • Burn control error	▨ • Steering error • Burn control error	• Steering error • Burn control error	• Steering error • Burn control error	▨ • Steering error • Burn control error
Hardware	• Steering error • Burn control error • Software control • Communication • Protective failure	• Steering error • Burn control error • Software control • Communication • Protective failure	▨ • Steering error • Burn control error • Software control • Communication • Protective failure	• Steering error • Burn control error • Software control • Communication • Protective failure	• Steering error • Burn control error • Software control • Communication • Protective failure	▨ • Steering error • Burn control error • Software control • Communication • Protective failure
Human Factors	• Software design • Hardware design • Security assess • Administrative	• Software design • Hardware design • Security assess • Administrative	▨ • Software design • Hardware design • Security assess • Administrative	• Software design • Hardware design • Security assess	• Software design • Hardware design • Security assess	▨ • Software design • Hardware design • Security assess
Physics	• Fin position stuck	• Fin position stuck	▨ • Fin position stuck	• Explosion • Fin fails • Fuel containment • Hydraulic fluid • Missile structure	• Explosion • Fin fails • Fuel containment • Hydraulic fluid • Missile structure	▨ • Explosion • Fin fails • Fuel containment • Hydraulic fluid • Missile structure

Figure 3. Passive Positive Measure
Separation: Insufficient fuel to reach population center



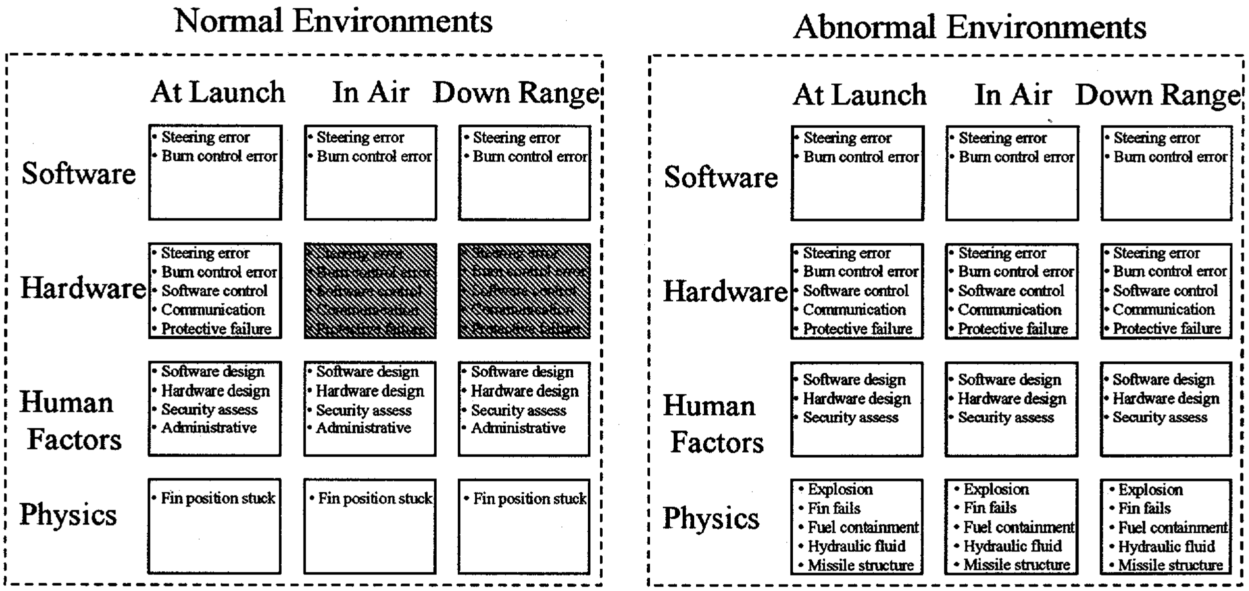
	Normal Environments			Abnormal Environments		
	At Launch	In Air	Down Range	At Launch	In Air	Down Range
Software	• Steering error • Burn control error	• Steering error • Burn control error	• Steering error • Burn control error	• Steering error • Burn control error	• Steering error • Burn control error	• Steering error • Burn control error
Hardware	▨ • Steering error • Burn control error • Software control • Communication • Protective failure	▨ • Steering error • Burn control error • Software control • Communication • Protective failure	▨ • Steering error • Burn control error • Software control • Communication • Protective failure	• Steering error • Burn control error • Software control • Communication • Protective failure	• Steering error • Burn control error • Software control • Communication • Protective failure	• Steering error • Burn control error • Software control • Communication • Protective failure
Human Factors	• Software design • Hardware design • Security assess • Administrative	• Software design • Hardware design • Security assess • Administrative	• Software design • Hardware design • Security assess • Administrative	• Software design • Hardware design • Security assess	• Software design • Hardware design • Security assess	• Software design • Hardware design • Security assess
Physics	• Fin position stuck	• Fin position stuck	• Fin position stuck	• Explosion • Fin fails • Fuel containment • Hydraulic fluid • Missile structure	• Explosion • Fin fails • Fuel containment • Hydraulic fluid • Missile structure	• Explosion • Fin fails • Fuel containment • Hydraulic fluid • Missile structure

Figure 4. Passive Positive Measure
Barrierization: Electrical shielding



	Normal Environments			Abnormal Environments		
	At Launch	In Air	Down Range	At Launch	In Air	Down Range
Software	• Steering error • Burn control error	• Steering error • Burn control error	• Steering error • Burn control error	• Steering error • Burn control error	• Steering error • Burn control error	• Steering error • Burn control error
Hardware	• Steering error • Burn control error • Software control • Communication • Protective failure	• Steering error • Burn control error • Software control • Communication • Protective failure	• Steering error • Burn control error • Software control • Communication • Protective failure	• Steering error • Burn control error • Software control • Communication • Protective failure	• Steering error • Burn control error • Software control • Communication • Protective failure	• Steering error • Burn control error • Software control • Communication • Protective failure
Human Factors	• Software design • Hardware design • Security assess • Administrative	• Software design • Hardware design • Security assess • Administrative	• Software design • Hardware design • Security assess • Administrative	• Software design • Hardware design • Security assess	• Software design • Hardware design • Security assess	• Software design • Hardware design • Security assess
Physics	▨ • Fin position stuck	▨ • Fin position stuck	▨ • Fin position stuck	▨ • Explosion • Fin fails • Fuel containment • Hydraulic fluid • Missile structure	▨ • Explosion • Fin fails • Fuel containment • Hydraulic fluid • Missile structure	▨ • Explosion • Fin fails • Fuel containment • Hydraulic fluid • Missile structure

Figure 5. Passive Positive Measure
Support: Robust structure



	Normal Environments			Abnormal Environments		
	At Launch	In Air	Down Range	At Launch	In Air	Down Range
Software	• Steering error • Burn control error	• Steering error • Burn control error	• Steering error • Burn control error	• Steering error • Burn control error	• Steering error • Burn control error	• Steering error • Burn control error
Hardware	• Steering error • Burn control error • Software control • Communication • Protective failure	▨ • Steering error • Burn control error • Software control • Communication • Protective failure	▨ • Steering error • Burn control error • Software control • Communication • Protective failure	• Steering error • Burn control error • Software control • Communication • Protective failure	• Steering error • Burn control error • Software control • Communication • Protective failure	• Steering error • Burn control error • Software control • Communication • Protective failure
Human Factors	• Software design • Hardware design • Security assess • Administrative	• Software design • Hardware design • Security assess • Administrative	• Software design • Hardware design • Security assess • Administrative	• Software design • Hardware design • Security assess	• Software design • Hardware design • Security assess	• Software design • Hardware design • Security assess
Physics	• Fin position stuck	• Fin position stuck	• Fin position stuck	• Explosion • Fin fails • Fuel containment • Hydraulic fluid • Missile structure	• Explosion • Fin fails • Fuel containment • Hydraulic fluid • Missile structure	• Explosion • Fin fails • Fuel containment • Hydraulic fluid • Missile structure

Figure 6. Passive Positive Measure
Entropization: Cooling fins, flight-air cooling

	Launch SW normal	Air SW normal	Range SW normal	launch SWabnorm	Air SWabnorm	Range SWabnorm	Launch HW normal	Air HW normal	Range HW normal	Launch HWabnorm	Air HWabnorm	Range HWabnorm	Launch HE normal	Air HE normal	Range HE normal	Launch HEabnorm	Air HEabnorm	Range HEabnorm	Launch physics norm	Air physics normal	Range physics norm:	Launch physicsabnorm	Air physicsabnorm	Range physicsabnorm
Separation/fuel			X			X			X			X			X			X			X			X
Barrier/shield								X	X	X														
Support/msl. structure																			X	X	X	X	X	X
Entropy/cooling								X	X															
Info Incomp/anti-jam								X	X															
Separation/traffic																				X			X	
Separation/weather																				X	X		X	X
Incapacitate/cmd destr	X	X	X		X	X	X	X	X		X	X	X	X	X		X	X	X	X	X	X	X	X
Incapacitate/cmd disab	X	X	X				X	X	X				X	X	X				X	X	X		X	X
Support/launch bldgs	X			X			X			X			X			X			X			X		

Figure 7. Matrix of Vulnerabilities vs. Protective Measures

One way to illustrate by groups the potential coverage of vulnerabilities is to portray a matrix such as that shown in Figure 7, where rows indicate protective measures, and columns indicate vulnerabilities. Columns with no checkmarks would represent unaddressed vulnerabilities; columns with single check marks represent vulnerabilities for which a particular protective measure is "essential" (necessary if the vulnerability is to be addressed), and columns with multiple check marks indicated vulnerabilities that can be addressed in multiple ways. Note that this is a binary indication, whereas real situations are generally somewhere between "addressed satisfactorily" and "not addressed." A more comprehensive approach than that indicated would judge the degree to which vulnerabilities are addressed. In some cases, they might be satisfactorily addressed; in others, multiple or coordinated controls might be necessary.

	Launch SW normal	Air SW normal	Range SW normal	launch SWabnorm	Air SWabnorm	Range SWabnorm	Launch HW normal	Air HW normal	Range HW normal	Launch HWabnorm	Air HWabnorm	Range HWabnorm	Launch HE normal	Air HE normal	Range HE normal	Launch HEabnorm	Air HEabnorm	Range HEabnorm	Launch physics normal	Air physics normal	Range physics normal	Launch physicsabnorm	Air physicsabnorm	Range physicsabnorm
Barrier/shield								X	X	X														
Support/msl. structure																			X	X	X	X	X	X
Separation/traffic																				X			X	
Incapacitate/cmd destr	X	X	X		X	X	X	X	X		X	X	X	X	X		X	X	X	X	X	X	X	X
Support/launch bldgs	X			X			X			X			X			X			X			X		

Figure 8. Matrix of Selected Protective Measures

Implementation of a Coordinated Safety Theme

The basic idea behind a "safety theme implementation" is to make a coordinated selection of principle-based protective measures (see preceding discussion) that assure the desired level of safety without under-estimating threats, without over-complicating the approach, and without over-spending available resources. Ideally, there would be one highly effective protective measure addressing each vulnerability, and preferably each protective measure would address multiple vulnerabilities[3]. ("Cost-effectiveness" is generally enhanced by having a minimum number of rows to provide at least one check mark in each column.) The level of risk desired is typically weighed against the monetary and operational cost of incorporating the protective measure. This can in concept be treated quantitatively, semi-quantitatively, or qualitatively. For our scenario, we will use a qualitative treatment, but again with the caveat that more information generally enables more quantitative treatment. The implementation of principle-based positive protective measures becomes "safety-critical," meaning that its effectiveness is essential for safety and therefore it is subject to special scrutiny initially and over the lifetime of the project. In the non-ideal real world, where there are known and/or unknown failure modes, manufacturing anomalies, human errors, etc., the selection is complicated by less-than-perfect protective measures, meaning that layering or defense in depth makes additional rows necessary. For minimizing loss of life, the general theme is to incorporate protective measures that protect life by separating the normal-environment and abnormal-environment energy potential of the rocket to a high level of assurance from any population, even in the presence of reasonably expected system failures.

The focus of the selection is to seek first-principle passive solutions first. For example, in the rocket launch scenario, fuel limitation meets these criteria and is highly effective if the rocket range limits do not reach any population. However, since this protective measure is impractical for most rocket ranges, it was not selected for the example. The next selection can be generally described as observing that command destruct was essential to address many of the vulnerabilities, and also helped address many others. Similarly, robust launch facilities were necessary to address safety of launch personnel, and robust missile structure addressed a number of physical vulnerabilities. Shielding and traffic separation were necessary for more complete protection and are considered "good practice." The other protective measures excluded from this example treatment were entropy cooling, anti-terrorist command disable, and anti-jamming communication (probably unnecessary); and launch delay in the face of bad weather (possibly unnecessary).

As a result of this process, a possible protective selection suite is shown in Figure 8 for the example scenario.

Determination of and Evaluation of Residual Risk

Risk typically combines degree of vulnerability with the consequences of losses in order to measure the priority for incorporating protective measures (controls) in a basic design concept. These types of judgments are almost always necessary because of budget or technological limitations and operational considerations (mission goals in terms of what is to be accomplished and on what time scale). For the example scenario, loss of life (which is the only consequence considered here more simplicity of the example) is a very high consequence, but some risk is accepted. The risk to the general population is usually considered less acceptable than the risk to the operational personnel.

Since there are always some potential residual vulnerabilities, the challenge is to determine level of risk. This can be done in various ways, depending on the amount and type of information available. One common quantitative method is probabilistic determination (probability of an asset being lost or damaged). Since there is usually uncertainty about probabilistic determinations, the uncertainty is sometimes represented by probability density functions. Another semi-quantitative method is possibilistic estimation, which relies on both data and expert judgment to give possibilistic ranges. Purely qualitative rankings are another approach. For our scenario, we will use qualitative illustrations, but in general, the more knowledge available, the more one moves from qualitative

[3] A real world concern is that a single protective measure is subject to "first-order" potentially catastrophic failure. For this reason alone, it is generally considered desirable, if feasible, to use multiple protective measure coverage.

to quantitative approaches. The tools discussion below shows how systematic logic construction can be a valuable adjunct to this process.

Configuration Control of Safety-Critical Components

Since many opportunities for safety compromise can occur in production, repair, and maintenance, safety-critical components must have configuration control. Basically this means that any proposed changes are subject to a comprehensive safety review before their implementation. This control continues for the system lifetime.

Independent Review and Assessment

Note also that the approach outlined above in a design context would ideally be accompanied by a similar continuous review process and independent assessment. In other words, the assessors examine assets, threats, environments, vulnerabilities, principles behind protective measures, and residual risk. They give particular emphasis to principle-based positive measures implemented with what become safety-critical components coordinated to achieve a safety goal through the use of a safety theme, and they assess the safety theme. This assessment process is "cradle to grave" over the system lifetime.

Logic Model Guidance and Physical Response Modeling

Physical response modeling can specifically address the ways components fail under known stresses. Beyond this, a logic structure, for example comprising event trees and fault trees, is a useful tool for understanding the interaction of various ways system failures can take place and be prevented. Where enough information is available, these can be used to estimate probabilities or possibilities of affecting assets. They are also useful in identifying catastrophic failure potential and "order" (number of failures necessary) for a particular outcome. As an illustration, Figure 9 shows a high level fault tree reflecting the threat categorization in a manner similar to the organization of Figure 1. Figure 10 shows a more detailed view of one portion of the fault tree, illustrating the effect of protective measures and the failures that must occur for the particular fault. Also indicated in Figure 10 is the role of event trees in providing fault tree inputs.

Accident and Occurrence Emergency and Non-Emergency Response

At times designs and products will fail, people will make mistakes, sequences will be out of control, and unexpected environments will occur. With these considerations in mind, products can be better designed to prevent catastrophic failures, mitigate the effects of a failure, and incorporate appropriate damage control to recover the lost safety as quickly as possible—all in a proactive designed-in approach. In order to accomplish this goal, a special team of pre-trained personnel is essential. These personnel must periodically train, both in the classroom and in the field, on how to handle emergency conditions, and on how to restore any lost safety to the system as quickly as possible. Drills and practice may bring out needed changes that will enhance recovery of lost system safety.

Conclusions

The potential payoffs of the outlined approach are that it helps establish a high level of assurance in system safety design and assessment, provides an auditable and reviewable process, and enables cost-effectiveness of design, review, and upgrades. There is an exemplary track record for the approach in the nuclear weapons program, and we have every reason to believe that the methodology could benefit many other areas of system safety.

Biography

Arlin Cooper has worked at Sandia National Laboratories for 35 years, specializing in electronic component design, safety and security systems development and analysis, and algorithm development and assessment. He is a Distinguished Member of Technical Staff and has a Ph. D. from Stanford University.

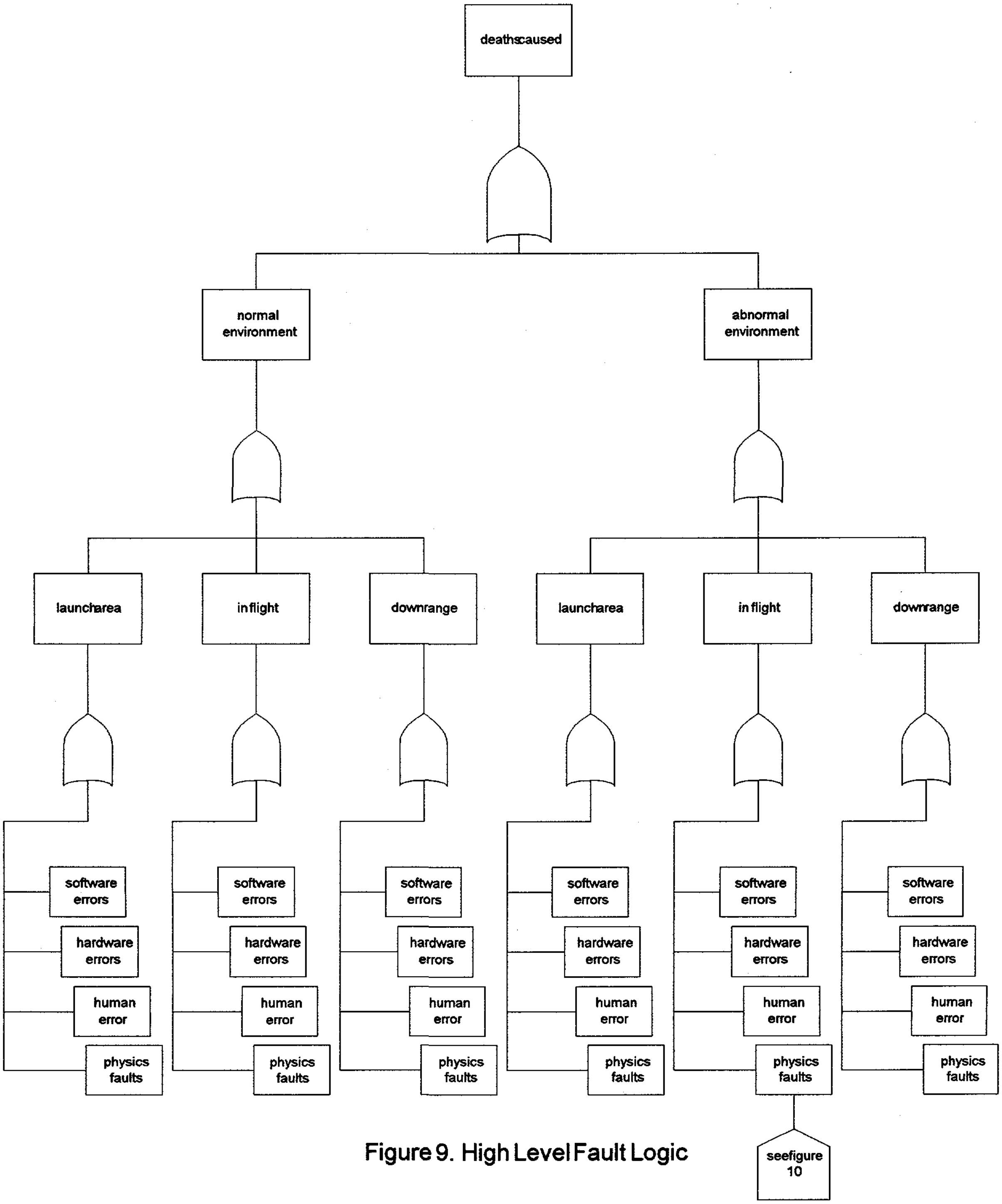


Figure 9. High Level Fault Logic

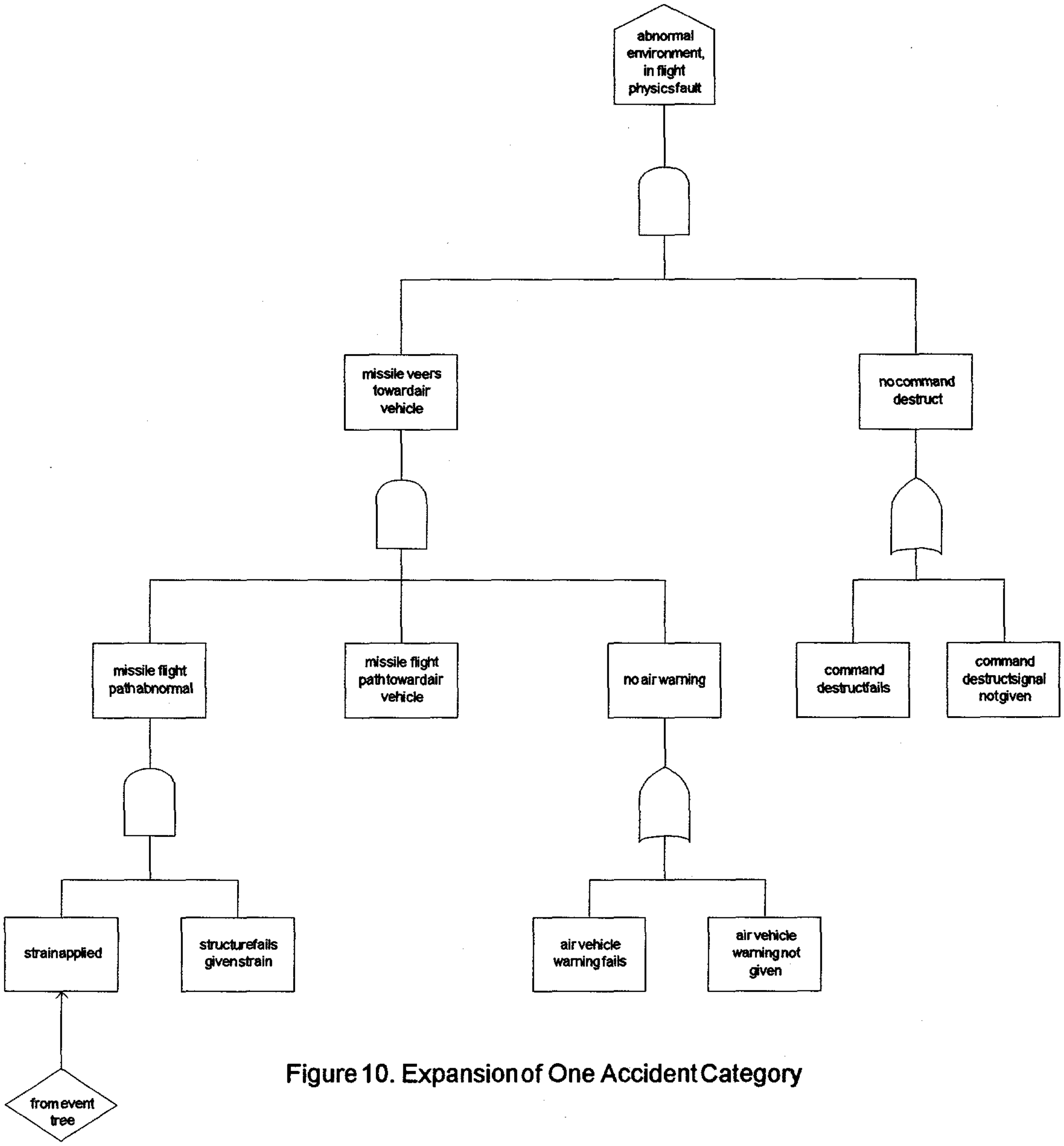

abnormal environment, in flight physics fault
missile veers toward air vehicle
no command destruct
missile flight path abnormal
missile flight path toward air vehicle
no air warning
command destruct fails
command destruct signal not given
strain applied
structure fails given strain
air vehicle warning fails
air vehicle warning not given
from event tree

Figure 10. Expansion of One Accident Category