9/13/95

SANDIA REPORT

SAND94-3223 • UC-700

Unlimited Release

Printed September 1995

High Consequence System Surety Process Description

Gary T. Randall

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-94AL85000

Approved for public release; distribution is unlimited.

SF2900Q(8-81)

MASTER

RECEIVED

SEP 26 1995

OSTI

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

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
PO Box 62
Oak Ridge, TN 37831

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

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

NTIS price codes
Printed copy: A03
Microfiche copy: A01

DISCLAIMER

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

SAND94-3223
Unlimited Release
Printed September 1995

Distribution
Category UC-700

High Consequence System Surety

Process Description

prepared by the

High Consequence System Surety Project Team
Sandia National Laboratories
Albuquerque, New Mexico 87185

compiled by

Gary T. Randall

Abstract

This report documents work-in-progress accomplished prior to programmatic changes that negated bringing this effort to conclusion as originally intended. The High Consequence System Surety (HCS²) project pulls together a multi-disciplinary team to integrate the elements of surety - safety, security, control, reliability and quality - into a new, encompassing process. The benefit of using this process is enhanced surety in the design of a high consequence system through an up-front, designed-in approach. This report describes our integrated, high consequence surety process and includes a hypothetical example to illustrate the process.

MASTER

High Consequence System Surety

Process Description

TABLE OF CONTENTS

INTRODUCTION.....	1
TEAM MEMBERS	1
VISION.....	2
GOAL	2
DEFINITIONS.....	3
PROCESS DESCRIPTION.....	4
Determine System Boundaries.....	7
Develop Requirements.....	7
Identify Surety Concepts For Meeting Requirements.....	11
Conduct Surety Theme Analysis.....	14
Integrate and Establish Quantified Consequences.....	17
Conduct Trade-Offs.....	18
Implement Design Enhancements.....	19
Establish Evaluation Methodology.....	20
System Qualification	21
Independent Assessment.....	21
ILLUSTRATIVE EXAMPLE.....	22

High Consequence System Surety

Process Description

Introduction

High Consequence System Surety (HCS²) is the name of a project at Sandia National Laboratories, formed in February 1994. This project pulls together a multi-disciplinary team to integrate the elements of surety - safety, security, control, reliability and quality - into a new, encompassing process. The original plans for this surety process was to augment and validate the process by applying it to a remote, automated nuclear weapon component handling operation being proposed for use at the Mason & Hanger Pantex Plant. The perceived benefit of applying our surety process to this operation is up-front, designed-in system surety and an enhanced Department Of Energy approval process. Programmatic changes during the development of the HCS² process resulted in not fully applying it to the handling operation. Thus, the process has not been augmented or validated. The project team believes that our surety process accomplished to date is worth documenting. This report describes our integrated, high consequence surety process and includes a hypothetical example to aid in illustrating the process.

Team Members

The High Consequence System Surety Process is the result of a collaborative team effort. Members of the HCS² team changed with time -- some retiring, some moving on to other projects and some occasionally called upon as consultants. The following list captures (and thanks) those people who have contributed to this process.

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, 12333
Sabina Jordan, 5861

Stan Kawka, 5122
Tom Kerschen, 12335
Bill McCulloch, 12333
Scott Nicolaysen, 2645
Bill Paulus, 5845
Gary Randall, 2645
Stu Rogers, 12326
Heather Schrinier, 6412
Mark Snell, 5845
Pat Tempel, 13311
Sharon Trauth, 13311
Ken Varga, 2643

Vision

The vision of the HCS² project is:

VISION

To Provide Seamless System Surety For High Consequence Operations

This vision statement purposely does not mention a particular customer or application. Part of the vision is not only to solve a Department Of Energy (DOE) need, but to offer industry insights into a surety process. There are numerous high consequence operations conducted by a variety of industries (for example, medical, chemical, explosive, military, airline, and insurance) that face consequences involving loss of large investments or loss of life. We believe surety is an area in which Sandia can excel, based on our history in designing and developing high consequence nuclear weapons.

Goal

The HCS² team developed the following goal statement in support of our DOE role and internal Sandia customer.

GOAL

To Develop A High Consequence System Surety (HCS²) Process, Augmenting And Validating It By Applying It To The Weight And Leak Check System (WALS)

Sandia has many recognized experts in the areas of surety. We believe that an integration of these surety areas into one surety process is lacking. The goal statement therefore explicitly mentions developing a surety process. Note that the WALS application is not only a vehicle to validate the process, but will augment the process. That is, as we apply the process and learn more, the team expects to make enhancements to the process.

Definitions

Assessment	An independent review by people not directly associated with the day-to-day activities of the project.
Assurance	The day-to-day, concurrent team interactions that occur in accomplishing the project objectives.
Consequence	The outcome of a hazard; it is, to a large extent, in the "eye of the beholder." Realizing a hazard is not necessary for it to be a consequence; consequences can be perceived or expected.
Control	To provide positive measures to both assure authorized use and assure against unauthorized use.
Hazard	A potential consequence.
High Consequence	Varies with the operation and the customer, but is a consequence judged to be severe, for example, resulting in significant loss of investment or loss of life. Not all consequences are necessarily high consequences. Analysis of a component within 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.
Product Realization Team (PRT)	As defined by EP401100 ¹ , it is a multi-disciplinary team that is responsible for the definition, development, delivery, and support of a product through concurrent engineering methods.
Quality	Is the conformance to customer requirements and expectations.
Reliability	The probability that a system will perform a required function under stated conditions for a stated period of time.
Risk	A measure of a hazard's probability of occurrence times the magnitude of the consequence.

¹ Interagency Engineering Procedure, "EP401100/C - Qualification Process For The Nuclear Weapons Complex," Draft, October 1, 1994.

Safety	Is the assurance against unintended adverse consequences. To mitigate safety one uses safety theme concepts such as isolation, incompatibility, inoperability, and independence.
Seamless	Seamless means 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 reliability.
Security	Is the denial of unauthorized access.
Surety	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. We drop the word "use" in "use control" to make the term more general in nature when addressing non-nuclear weapon audiences. The HCS ² process also addresses reliability and quality as essential components of a system. This paper refers to these five areas -- safety, security, control, reliability, and quality -- as the elements of surety.
Surety Team	A team comprised of representatives from safety, security, control, reliability, and quality that support the PRT.
System	Here, "system" emphasizes 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.

Process Description

The following two pages present our entire High Consequence System Surety Process in flowchart form. Following sections then further describe the process in more detail.

Determine System Boundaries

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

Develop Requirements

Next is to start developing the requirements. This is an essential step and, as with many other endeavors, is the foundation of a quality process. It is suggested that many of the errors or poor performance of a system can be traced back to a lack of clear, accurate, traceable, meaningful, and measurable requirements. Developing these requirements can be a difficult and time consuming process. Our team's

rationale for such a commitment to this up-front investment in time is that the project will realize a greater return on this time investment by experiencing and dealing with far fewer surety issues. We strongly encourage negotiating the requirements up front. The following diagram further clarifies developing the requirements.

We recommend using a concurrent team approach by having representatives from both the system designers and surety experts to help develop requirements. A suggested organizational relationship would be for this "surety team" to be lead by a member of the system Product Realization Team. The first purpose of this surety team is to identify clear, accurate, traceable, meaningful, and measurable requirements. Traceability is important in demonstrating a quality process, a process where the work being done is clearly attributable to a customer's requirement and is measurable.

At this time it is useful to understand what the perceived consequences of the system are. Why does this effort (with a

focus on surety) seem to be necessary? What are the customer's concerns? With the aid of the surety team members, what additional concerns may be identified that the customer may not even be aware of yet? These are indeed "perceived" consequences since no analysis has yet been conducted to quantify their risks. It is also useful to sort the consequences. A system may have so many perceived consequences that to rigorously analyze all of them is not practical. The act of sorting also aids in the identification of additional perceived high consequences, a brainstorming effect.

How does one elicit requirements? Brainstorming, Quality Function Deployment (QFD), and other informal and formal methods of requirement elicitation are being discussed within the HCS² team.

There are several types of requirements and in the context of the HCS² process, categorizing them into operational, surety, and regulatory helps focus on the surety requirements. An example of operational requirements may be the temperature extremes the product will see; a surety requirement being the trade-off between safety and security; and for regulatory, Occupational Safety and Health Administration (OSHA) rules. The HCS² process focuses on surety requirements in the belief that they do not normally receive the attention other requirements do. Regulatory requirements for a system will vary depending on the owner of the system. For the nature of the work performed by Sandia National Laboratories, 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. An important question to ask is who accepts the requirements? The following diagram addresses this question.

First, the requirements should be acceptable to the team that has responsibility for the system. Here the "team" refers to the surety team and as appropriate, the Product Realization Team. This is also an appropriate point in the process for independent assessors to review the requirements. We recommend that the results of the assessors' review be documented (referred to as a Surety Assessment Report). This report is a living document, recording assessment reviews throughout the entire process. Management should have the opportunity to understand and comment on the requirements as well as the customer. The Product Realization Team should choose the appropriate independent assessors, managers and customers for these reviews. The above diagram shows that any one of the reviewers could cause an iteration or refinement of the requirements. Also, the serial appearance of the diagram does not mean actions are occurring sequentially in time.

What happens if there is not agreement on the requirements? For example, the independent assessors are recommending something and the team disagrees. If this happens, we believe the Product Realization Team has the responsibility for deciding. Additionally, we recommend that the dissenting opinion, and the reason why the PRT decided to proceed as they did, be documented.

An outcome of determining if the requirements are acceptable, and what they are, is a requirement document, written by the system owners with the aid of team members.

Identify Surety Concepts For Meeting Requirements

Once the team members define the system requirements to the best extent possible, they identify surety concepts for meeting these requirements. We use the surety elements to help identify issues as early as possible and to develop conceptual principles and approaches for meeting the requirements. At this phase of the process, these surety assertions of how the system must behave have no backing with analysis; that follows later. It is important for the team to understand these assertions and, as work proceeds, to continually assess themselves against them, changing them as needed.

This activity begins to show how the surety elements interact. It also shows that, given the system and its requirements, possibly not all of the surety elements will be part of the surety theme. This portion of the process is heavily methodology oriented, needing techniques useful in developing surety concepts into a theme. One might be a QFD-type tool where the top portion of the "house" is of particular value. By listing the requirements against the various surety elements, the interactions are systematically explored (see Figure 1).

Figure 1. QFD-Type Tool

Requirement #1	concept	concept	concept	concept	N/A		
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 #5	concept	concept	N/A	concept	N/A		
Requirement...	concept	concept	concept	concept	concept		
	SAFETY	SECURITY	CONTROL	RELIABILITY	QUALITY	STAGE 1	STAGE 2

Our adaptation of this technique includes listing the requirements against all of the surety elements rather than just use control. By using stages, it differs from the QFD-type tool. Stages could possibly represent differing states of the system in time.

Our 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 same process as diagrammed in determining if the requirements are acceptable is applicable for determining if the surety concepts are acceptable. That is, they must be acceptable to the team, independent assessors, management and the customer.

2 Security and Use Control Assessment Department, 12334, "Use Control Theme Development," January 13, 1994.

Conduct Surety Theme Analysis

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 by starting to quantify the risks. This fundamental analysis helps to identify potential problems, design errors, process capability limitations, components that dominate risk or reliability and other issues. Separating the analysis into three areas - modeling and analysis, characterization, and evaluation - helps conceptualize the process.

Here, modeling and analysis implies a rigorous, mathematically based analysis of the system.

Characterization of processes helps to quantify and understand their limitations. Evaluation recognizes that it is possible to base surety theme analyses on intangibles such as judgment or expert opinion. The HCS² process shows that individual surety element analyses may very well result in conflicts with the requirements. For example, instead of a system reliability of 0.95, the model may show a reliability of 0.90. The surety analysts and system customer should resolve these conflicts before proceeding. There are several tools and techniques available to aid in quantifying a system, each one in essence representing a process of its own. A few examples of what may be used for the WALs project follow.

Quantitative Risk Assessment (QRA) or Probabilistic Risk Assessment (PRA) uses tools and techniques to evaluate the safety of a system. This process begins by gathering data and becoming familiar with the system. Reviews of the design, process flow, documents, procedures, requirements, and standards occur. An operations analysis identifies potential failure modes, sources of energy, and preliminary abnormal environments. One then develops preliminary hazard matrices, followed by accident scenarios and system modeling. The process uses event trees and fault trees throughout. The integration of the event tree frequencies with fault tree probabilities aids in determining the dominant risk contributors and rank ordering of those risks. Risk assessment provides information on which components really matter, which have a higher vulnerability, and which will potentially provide a greater safety enhancement to the system. An additional benefit of this modeling is that it provides a validation of intuition; one can now discuss initial intuition and assertions with quantified risks.

Reliability modeling is a technique used to understand and characterize a product's design by using mathematical expressions for quantifying its reliability. A couple of organizations within Sandia have the capability for producing reliability models. Our process uses the Manufacturing Systems Reliability Department, 6613, reliability modeling software. This software, named RAMP (Reliability Analysis & Modeling Program), uses many analyses. This includes common cause analysis, failure analysis, fault trees, and failure mode effects and criticality analysis (FMECA). These help in identifying those factors that dominate the system reliability and offer predictive uncertainty and sensitivity analyses. RAMP performs both repairable and non-repairable analyses. This design-for-reliability tool integrates data management, model development, and model analysis (including uncertainties) with graphical output.

Security uses a Protection System Development Process. Determining what the objectives are, by defining the adversarial threat and target, is the first step in this

process. This is answering the question of what is to be protected. The next step is to evaluate the design by performing vulnerability analyses which may involve the use of computer tools, for example, a facility protection system vulnerability analysis. Finally, based on the results of the analyses, the design is improved and then re-evaluated. 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.

Information surety is another process, one that encompasses many of the surety elements. 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 and it may be more productive to just consider control as security.

The quality surety element uses many tools to aid in statistical process capability and control methodologies. Well documented quality improvement techniques such as Pareto Charts, Fishbone Diagrams, and Control Charts are available. Sandia has developed a Process Characterization Methodology³ (PCM) that is a systematic approach for transitioning from design to production. PCM is useful in anticipating and thus preventing processing problems. Also available are procedures that define a concurrent process to qualify processes and products (EP401100¹ and EP401099⁴).

As a part of conducting surety design analyses, the team is discussing how one handles software. What does it mean to have software surety and how does one go about achieving it? Questions such as these become more and more important with the continually increasing amount of software in systems. The HCS² team is currently taking an approach of using tools such as risk assessment and reliability modeling to identify the high consequences. When software is part of these

³ Process Characterization Methodology, Sandia National Laboratories, Greg Neff, organization 2643, and Naomi Christensen, organization 2645.

⁴ Interagency Engineering Procedure, "EP401099/A - Product Realization Process," Draft, September 1, 1994.

models, it will more than likely be treated as a "black box" and assigned a probability of failure of one. Refined analysis occurs when the subsystem that includes this software becomes a high consequence subsystem. The HCS² team is exploring various techniques to "open up" this software black box and understand the software design within better. This includes using linked state machines and Software Safety Fault Tree analyses.

Integrate and Establish Quantified Consequences

The HCS² team believes that the integration of all the surety elements is a key step. As mentioned, understanding the interrelationships between the elements of surety is essential. A safety analysis might point to the need for the addition of a safety device, thus increasing overall system safety. However, the addition of such a device could degrade the overall reliability of the system with the addition of new hardware. At this point in the process one begins to see the surety interrelationships.

Quantifying some of the risks and consequences of this integrated surety system is now possible. Some of the perceived consequences as postulated in the requirements phase now have quantified risks associated with them. The relative importance of the consequences start to emerge with an understanding of what is a "high" consequence.

Inherent in this portion of the process of integrating the elements is a "baseline" configuration. 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? What measure is used? Answers to questions such as these will establish a baseline design with associated risks.

Conduct Trade-Offs

Now with an understanding of the risks, one must first answer the question if they are acceptable. If they are, we recommend that the reasons for accepting these risks be included in a surety implementation document. If they are not, is further analysis needed? Do different configurations need exploring? If so, the team can perform trade-off analyses or cost benefit studies.

Conducting "what if" exercises is possible now that models are in place and there is an understanding of the

consequences. After conducting the trade-offs and establishing new risks, one can again determine if the risks are acceptable. Ultimately some of the risks will not be acceptable and will require mitigation. Although this is a team process involving independent assessors, managers and the customer, the system customer must decide what is, and is not, acceptable if conflicts arise.

One can also start to prioritize the high consequences and associated risks requiring mitigation. One should capture all of these decisions in the surety implementation document; detailing the analyses, the decisions of what is acceptable, and the approaches to mitigate unacceptable consequences. This document should also be traceable to the requirements for ensuring they are being satisfied.

Implement Design Enhancements

The process then flows to implementing those enhancements. The enhancements mitigate the unacceptable risks that are in the implementation document. It may be useful to point out that solutions are not necessarily hardware based. The following diagram further clarifies this.

Categorizing enhancements into 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) is helpful for distinction. It may be more cost effective to implement a procedure than to design hardware preventing something from occurring.

Establish Evaluation Methodology

Establishing evaluation methodologies such as tracking procedures, verification of processes, and testing of the hardware, is important. This not only allows one 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. If the requirements are not satisfied (according to the team, independent assessors, management, and the customer), the process can feed back to whatever point in the process that is appropriate to resolve the issue.

System Qualification

"Qualifying" the system occurs after satisfying all of the requirements. Note that qualification activities are being conducted concurrently throughout the entire process. This qualification process is one of assuring that the system and associated processes are capable of meeting customer requirements, design definition, and production readiness. The outcome is a formal qualification document.

Independent Assessment

Since the HCS² process proposes to address systems involving high consequence operations, it may be desirable to have an independent assessment. Independent assessors, people not involved in the day-to-day working of the team, review the process and documentation. This review should occur

periodically throughout the process, concluding with an assessment when the process is "finished."

Note that independent assessment does not replace any concurrent, self assessing the team is doing. The team should be making assertions throughout the process, self evaluating against those assertions, and making corrections as needed.

Illustrative Example

To help illustrate the HCS² process the following is a brief, non-inclusive, *hypothetical* example. Let's consider a smart credit card; that is, an electronic, microprocessor based credit card. First, the Smart Card Product Realization Team forms. The product realization team in turn forms a concurrent surety team comprised of representative card designers and surety experts.

The first step of the process is to determine the system boundaries. In this example, a boundary might just be 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 and 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. As part of this, an understanding of what the perceived consequences are is useful in establishing a surety perspective. The Smart Card PRT feels that the following consequences are of concern:

- loss of funds due to unauthorized account access
- inaccurate transactions resulting in account errors
- customers unhappy with the card due to unreliability

If there were many consequences, a sorting exercise would be useful to help identify what consequences are of most concern.

Continuing in the process, categorizing requirements (into operational, surety, or regulatory) helps in distinguishing the surety requirements. At the start of the design there are the following requirements.

Operational:

- retain 2,000 bytes of data

- operate within 0°F to 120°F
- survive and afterwards remain functional within -32°F to 150°F
- have a two year life

Surety:

- maintain the customer's confidentiality

Regulatory:

- meet all applicable ISO standards for credit cards

The team starts to review these requirements and finds them lacking in many areas, especially in surety. After much discussion, the team includes the following surety requirements.

- 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 exposing silicon wafers or circuit traces)
- before performing any operations, the card shall process and accept a customer's Personnel Identification Number (PIN)
- the card shall only allow ten attempts of the PIN
- once ten attempts have been made, the card shall become inoperable

The last three of these additional requirements are traceable to the perceived consequence of "loss of funds because of unauthorized account access." Here, the identification of perceived consequences led to detailed requirements that will in turn be quantified as to their risk.

The team, managers and independent assessors (as selected by the PRT), and the customers, review and accept these requirements. The product realization team takes responsibility, with the aid of the surety team, of writing the Smart Credit Card Surety Requirement Document, Issue 1.

Using the following QFD-type matrix, the team identifies surety concepts for meeting the requirements.

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 while conducting surety theme analyses. For example, risk analysis shows the risk of guessing a card's PIN is rather high since historically people use a simple PIN. 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 team quantifies the consequences and has a feel for which are high consequences. The consequence of losing funds due to unauthorized access is very high. Analysis shows that the risks associated with the reliability of keeping track of the PIN attempts and the probability of a successful attempt within ten attempts is high.

After conducting several trade-off analyses, looking at various interaction options, the team chooses which risks are and are not acceptable. For example, the risk associated with losing funds due to unauthorized access is not acceptable. The team prioritizes the not acceptable consequences and for budget reasons, agrees on a phased approach for mitigating them. The first to mitigate is the loss of funds' consequence. Trade-off analysis shows the consequence is best mitigated by reducing the access attempts to three and to include redundant hardware and software for the attempt algorithm (notably at the expense of reliability). The Smart Card Surety Implementation Document, Issue 1, documents these decisions.

While the necessary design changes are being made as agreed to in the implementation document, the team chooses 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. The team updates the models as new data becomes available and continuously updates the analyses.

The team verifies having met all the requirements and completes the project with a qualification document. A team, composed of members from different parts of the company does a successful, independent assessment of the card.

DISTRIBUTION:

1	MS0319	Ray Leuenberger, 2645
1	MS0319	Scott Nicolaysen, 2645
5	MS0319	Gary Randall, 2645
1	MS0329	Ruben Urenda, 2643
1	MS0329	Ken Varga, 2643
1	MS0405	Todd Jones, 12333
1	MS0405	Bill McCulloch, 12333
1	MS0458	Laura Gilliom, 5603
1	MS0484	Roxie Jansma, 9415
1	MS0486	Stan Kawka, 5122
1	MS0492	Mark Ekman, 12324
1	MS0535	Larry Dalton, 2615
1	MS0535	Steve Giles, 2615
1	MS0560	Paul Longmire, 5407
1	MS0627	Ed Fronczak, 12334
1	MS0637	Joe Chiu, 12336
1	MS0638	Stu Rogers, 12326
1	MS0639	Sharon Trauth, 13311
1	MS0639	Pat Tempel, 13311
1	MS0746	Jim Campbell, 6613
1	MS0746	Maria Armendariz, 6613
1	MS0747	Heather Schriener, 6412
1	MS0759	Bill Paulus, 5845
1	MS0759	Mark Snell, 5845
1	MS0762	Sabina Jordan, 5861
1	MS0830	Elmer Collins, 12335
1	MS0830	Tom Kerschen, 12335
1	MS1006	Bill Drotning, 2171
2	MS0100	Document Processing, 76132-2
		For DOE/OSTI
1	MS0619	Print Media, 12615
5	MS0899	Technical Library, 13414
1	MS9018	Central Technical Files, 8523-2