A major purpose of the Technical Information Center is to provide the broadest dissemination possible of information contained in DOE's Research and Development Reports to business, industry, the academic community, and federal, state and local governments.

Although a small portion of this report is not reproducible, it is being made available to expedite the availability of information on the research discussed herein.

LA-UR -86-119

CONF

CONF-8604111--1

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

LA-UR--86-119

DE86 006012

TITLE: APPLICATION OF SYSTEMS ANALYSIS TECHNIQUES TO
VULNERABILITY STUDIES OF COMPLEX INSTALLATIONS

AUTHOR(S): T. F. Bott

MASTER

SUBMITTED TO: 9th Advances In Reliability Technology Symposium - 1986
London, England, April 1986.

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.

By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes.

The Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy.

Los Alamos Los Alamos National Laboratory
Los Alamos, New Mexico 87545

APPLICATION OF SYSTEMS ANALYSIS TECHNIQUES TO VULNERABILITY STUDIES OF COMPLEX INSTALLATIONS

T. F. Bott
Los Alamos National Laboratory, Los Alamos, New Mexico 87545, USA

Application of reliability and risk analysis methods (particularly fault trees) to failure analysis of systems in hostile manmade environments is discussed. Methods for constructing, analyzing, and interpreting the fault trees, graphs, and diagrams are described. The application of fault-trees, directed graphs, and functional diagrams to problems in sabotage, survivability, and information protection is discussed in general terms. Special problems encountered in this type of analysis are discussed, and future research directions are considered.

INTRODUCTION

Engineering analysis has long been concerned with reducing failures in complex systems. Often this analysis has focused on failures with randomly occurring causes, but recent analyses at the Los Alamos National Laboratory have included failure induced by malvolent or hostile actions of human adversaries. Los Alamos has worked since 1977 on applying reliability and safety analysis techniques to system vulnerability studies involving sabotage, security compromise, and combat damage.(1,2) In this paper, I will describe our experiences in this field, compare them with more traditional assessments, and discuss the special problems encountered in vulnerability assessments.

The details of most vulnerability analyses are classified because of their potential usefulness to an adversary. For this reason, the specific results of the analyses cannot be presented in an open forum. However, techniques used and general examples of the results obtained from these studies are not classified.

METHODOLOGY

The purpose of vulnerability analysis is to provide an assessment of the likelihood of system failure in a manmade hostile environment. This environment may include stresses that are far beyond the system design capabilities and that are applied purposefully to the system by an adversary intent on causing system failure. Thus, the analysis includes elements of secondary cause, common cause, and human performance but from a unique viewpoint. Secondary causes that lead to failures of many components are the rule rather than the exception. Human actions may include acts of commission as a matter of course. The likelihood of the occurrence of a system failure cut set is a function of its attractiveness as a sabotage scenario, not a function of the basic reliability of the components in the cut set. In contrast to most reliability analyses, multiple initiating events and multiple mitigating system failures are likely, which makes the problem very complex from a systems standpoint. A major problem is just organizing the multidisciplinary information in a usable form. To approach this problem in a logical manner, Los Alamos has turned to the tools of reliability and risk analysis.

Deductive analysis methods are well suited to many of the vulnerability analyses. Undesired events are easier to determine than possible undesired sequences. For example, the unwanted results of sabotage at a nuclear reactor are limited: (1) radionuclide release and (2) economic loss to the plant. From these top undesired events, detailed sabotage scenarios may be deduced using fault trees.

The fault-tree approach has proven very useful in enforcing the discipline of systematic reasoning on the analysis. Many obscure, but significant, failure modes have surfaced as a result of the step-by-step logic involved in fault tree construction. System interfaces and interrelationships

are illuminated and unanalyzed sequences of events often are discovered. The fault-tree development procedure guides the analyst in obtaining and correlating diverse system knowledge. Fault trees are graphic representations of abstract ideas and easily understood by technical people, so a good review of the analysis by specialists on the system is possible without losing the independence of thinking of the vulnerability analysts. For these reasons, fault trees typically are chosen as the logic framework for the system modeling.

FAILURE MODELS

The failure of a system to perform a required mission is the undesired event in vulnerability analysis. This undesired event may be the result of a saboteur's carefully laid plans or the outcome of the more indiscriminate destructive capability of a hostile weapon. In either case, the first problem confronting the analyst is establishing the failure criteria for his system. This is not always easy because systems may degrade gradually in many environments. The point where system performance is no longer acceptable is often a matter of judgment. Multimission systems provide particular difficulties. Our experience has indicated the necessity for developing the top events of the tree carefully to insure a bounded problem and results that address the truly critical issues. This is accomplished by having detailed discussions with the systems experts for the facility or equipment under study.

After the failure criteria are established, a fault tree is constructed whose cut sets represent the sets of components whose failure will lead to mission failure. We have found that the vulnerability trees fall naturally into three principal sections. The top of the tree includes the undesired events (the goals of the adversary). Beneath the top of the tree are gates that describe system-level events. These gates typically have as inputs initiating events (adversary actions to stress the system) and mitigating system failures. Mitigating systems are designed to stop the progression of an undesired event (for example, a fire suppression system or a security alarm system). The adversary must either overwhelm or fail the mitigating systems to achieve his goals. Unambiguous system success criteria are critical to constructing this middle section of the tree, and a lack of understanding is very noticeable. In fact, sabotage analysis uncovered gaps in nuclear reactor safety knowledge before these issues were recognized generally as reactor safety issues (3,4).

The final level of the tree is the subsystem and component level. This level is often the most straightforward part of the model to construct. In some cases, detailed failure analysis at the subsystem level already has been performed for safety or reliability purposes. However, emphasis on single-failure assumptions often reduces the usefulness of this work when adversary actions are considered.

The fault-tree cut sets are determined using the SETS computer code.(5) The fault tree is entered into the computer using a symbolic language that is converted automatically to Boolean equations for the various gates. The cut sets are solved by successive substitution from the top event to basic events, with simplification occurring along the way. The cut sets of the fault tree (in symbolic form) are then available as terms in a disjunctive normal form of the fault-tree Boolean equation,

$$F_T = \bigvee_{j=1}^K \bigwedge_{i=1}^{N_j} B_{ij} \quad (1)$$

where

F_T = a repeated cut set disjunction,
 $\bigwedge$ = is a repeated event conjunction,
 F_T = the top event,
 j = the j^{th} cut set,
 B_{ij} = the i^{th} event of the j^{th} cut set,
 N_j = the number of events in the j^{th} in the cut set, and
 K = the number of cut sets.

The SETS code is currently operable on the Cray-XMP computers at Los Alamos, and very large trees ($\sim 10^3$ gates) may be reduced to cut sets in relatively short run times (~ 10 min).

BOOLEAN EQUATION TRANSFORMATIONS

The event cut sets generated from the system failure model fault tree are useful, but much additional information can be gained by transforming these equations into new Boolean equations representing other attributes of the system. For example, the locations from which a saboteur may induce a failure are of interest in sabotage analysis. This can be a major bookkeeping problem for

a large facility with many remotely operated components. Nevertheless, the problem is made manageable by transforming variables.

Sets of components that a saboteur could attack to gain his objective are already available from the system failure model cut sets. For each failure, a Boolean equation is constructed that symbolically represents the locations from which that component may be affected. For example, failure F_A could be caused by visiting location B or both locations C and F in sequence. This is represented by the Boolean location equation

$$F_A = B + (C \times F) \quad , \quad (2)$$

where + and $\times$ represent Boolean disjunction and conjunction operations. To convert a Boolean equation with event variables into its location equivalent, the Boolean equations for each failure event (such as F_A above) are substituted into the event equation and the equation is simplified. The resulting equation has locations as variables, with the terms of the equation representing sets of locations that allow the saboteur access to enough equipment to achieve his goals.

The transformation of variables is used frequently in vulnerability analysis. Transformations to locations, hazards, and threats are all useful for analysis of survivability in combat. For security, susceptibility to a surveillance method is a useful transformation. In these analyses, a large amount of information is sorted automatically into new forms for different perspectives on the problem.

NUCLEAR REACTOR SABOTAGE

The United States Nuclear Regulatory Commission (NRC) is charged with protecting the public from exposure to radiological hazards from nuclear power plants. This charter includes protecting nuclear power plants from sabotage that could cause the release of radionuclides to the environment. The NRC assesses the adequacy of security at nuclear plants, in part by ensuring that areas containing vital equipment are protected by physical and administrative safeguards. Los Alamos has provided technical assistance to the NRC by performing vulnerability analyses on commercial nuclear power plants to determine what equipment is vital to preventing radionuclide releases from the plant and the locations of this equipment.

This problem is addressed by constructing a fault tree with radiological release as a top event. To develop the fault-tree logic and to identify locations of equipment, the plant is visited by Los Alamos analysts because site-specific information is essential. A senior operator or engineer at the plant is involved in detailed discussions to determine system requirements and procedures. The physical layout of the plant is examined, and separable areas are designated as locations. A location is basically any area that can reasonably be enclosed to provide physical separation from the rest of the plant. The fault tree is developed based on reactor safety analysis and system performance specifications. The fault-tree model is realistic, but a conservative assumption is made when uncertainty exists. The fault-tree events are of two general classes: (1) initiating events that cause a potentially dangerous situation (for example, a pipe break) and (2) events that cause loss of components designed to mitigate the results of the initiators. The completed fault tree is transformed to location space by the methods described earlier and then solved for its cut sets, with the cut sets being in terms of locations a saboteur must visit to cause radionuclide release. The nuclear reactor fault trees are transformed to locations before solving for cut sets because of the great reduction in the number of location cut sets compared with event cut sets. This is because there are far fewer locations than component failure basic events. The cut sets typically consist of a number of single location sets and other sets which contain two or more locations. The Boolean equation for the cutsets becomes

$$\text{TOP-EVENT} = \text{LOC1} + \text{LOC2} + \dots + (\text{LOCN} \times \text{LOCM}) + \dots \quad , \quad (3)$$

where TOP-EVENT is the sabotage goal, and LOCX is a plant location. LOC1 and LOC2 are single locations where enough equipment is accessible for the saboteur to cause a radiological release without visiting another area, and multiple location cutsets like LOCN $\times$ LOCM represent sets of areas that must all be visited to perform successful sabotage. The areas identified in the analysis are compared with the areas protected at the plant to insure that protection is given to vital equipment. To date, this analysis has been performed for over 80 nuclear power reactors in the US.

An outgrowth of nuclear plant vital area analysis is communicated threat credibility assessment. When a threat is made against a nuclear plant in the US, the NRC mobilizes a team of experts to assess its credibility. Los Alamos draws on its extensive accumulation of technical material to determine if the threatened act is a credible method for achieving the saboteur's objectives.

SPACE TRANSPORTATION SYSTEM VULNERABILITY

Security personnel for the Space Transportation System (STS) (commonly known as the Space Shuttle) at Kennedy Space Center (KSC) requested help from Los Alamos in determining the most likely STS sabotage targets and potential countermeasures. Los Alamos was chosen because of our experience with nuclear power plants and because we offered an independent, unprejudiced view of the problem.

This project was approached in a systematic manner by constructing a fault tree to describe the STS failure. The first problem encountered in the analysis was determining failure criteria for the STS failure. Thus, the systematic approach indicated areas of incomplete understanding for the STS security system from the beginning. To gather the information needed for constructing the fault tree, detailed discussions were held with technical experts in specialized areas at KSC. The fault tree was developed by identifying hazards, components vulnerable to the hazards, and actions defeating safeguards. The cut sets of the fault tree were calculated and represented sabotage scenarios (sets of actions leading to saboteur objectives). These scenarios then were evaluated in matrix form to determine their attractiveness as potential routes to achieving sabotage. The criteria for evaluation included accessibility, danger to the saboteur, likelihood of detection, likelihood of success, specialized knowledge required, and the time required to complete the actions. The scenarios fell into three main categories: (1) high-risk scenarios that were very destructive and achievable; (2) scenarios that were for some reason difficult, dangerous, or uncertain of success; and (3) scenarios that were malicious but not highly destructive. Countermeasures to reduce the risk from the five high-risk scenarios were suggested.

This study confirmed the ability of systems analysts to contribute to an area outside their specific fields of expertise by using systematic techniques to collect and interpret information collected from experts on diverse subjects. The results of the analysis helped focus the attention of security personnel in areas of the greatest security concern. In addition, the enumeration of possible scenarios gave security personnel considerable insight into what evaluations or equipment should be regarded with suspicion or challenged.

COMBAT SYSTEM VULNERABILITY

Survivability may be defined as the likelihood of a military system performing a mission successfully in a manmade hostile environment. Survivability is often considered in two phases. Susceptibility, the first phase, is the probability that a system interacts with the threats. Susceptibility reduction includes measures to avoid being acquired, targeted, tracked, or hit by a threat. Vulnerability, the second phase of survivability, deals with the probability of a system failing given that it interacts with a threat.

At Los Alamos, determining the vulnerability of combat systems to enemy threats is approached in a systematic manner by first constructing a failure model of the system to be analyzed. The failure model is, as in previous examples, a Boolean representation of system fault tree cut sets. The basic events of the cut sets are component failure. Component failures are related to hazards that cause failure by Boolean equations of the form

$$(LDRANT) = (/KE) + (/FIRE) + (/X-RAY) + (/EMP) \quad (4)$$

This equation means that a lookdown radar antenna for an aircraft may fail because of interaction with kinetic energy (/KE), fire (/FIRE), x-ray flux (/X-RAY) or electro-magnetic pulse energy (/EMP) from a nuclear detonation. (The "/" is a tag for convenience in working with the SETS code). Cut sets of events are transformed into cut sets with both events and hazards. The hazards are transformed to threats by equations like

$$\begin{aligned} FIRE &= /HE + /INCENDIARY, \text{ and} \\ EMP &= /JAMMER + /NUDET \end{aligned} \quad (5)$$

which means that fire can result from high explosive (HE) or incendiary devices and electromagnetic pulse (EMP) can result from jamming or nuclear weapons. The transformed equations will have cut sets that indicate both the vulnerable components and the threats to which they are vulnerable. For example the "event loss of fire control radar" consists of loss of both lookdown (LDRADAR) and sidelooking radar (SLRADAR)

$$LOSS-FCRADAR = LDRADAR \times SLRADAR = LDRANT \times SLRANT + \dots \quad (6)$$

Transformed into a three-event equation, it becomes

$$LOSS-FCRADAR = (/HE + /JAMMER) \times (LDRANT \times SLRANT) + \dots \quad (7)$$

which indicates that either a high explosive or a jamming device can cause loss-of-the two-radar-antenna cut set LDRANT x SLRANT, causing loss of fire control radar and mission failure. The

weapon system critical components and threats to them can be identified for a very large system by using the bookkeeping capabilities of the fault-tree Boolean equations and their transformations. This approach gives a logical foundation to vulnerability studies. The approach is being quantified by determining the hardness (for example, failure stress distribution) of each critical component to each hazard. The hardness may be represented by a plot of the expected component degradation as a function of stress. The probability of exceeding a given stress level for a component may be estimated by including spatial stress distributions, shielding, and critical component presented areas. Work is just beginning in this area, but already the fault-tree approach has indicated areas of concern for focusing detailed analysis.

INFORMATION SECURITY

In many situations, a critical item of security is protecting information. An entire security system may be developed to prevent proprietary or classified documents, data, or equipment from being compromised. Protecting information about a military system that may be used by an adversary also can be considered from an information security viewpoint. It is important to assess the effectiveness of such a system. Los Alamos has applied system analysis techniques similar to those used in sabotage analysis to the assessment of information security effectiveness.

Information security attempts to control knowledge of a facility's existence, its mission or design details, or relevant procedures. The controlled information can be compromised by "leakage" of observables through information flow paths to collectors of information. The attributes of the facility then can be inferred by the collector based on his context or "frame." To control this leakage of information, safeguards are set up to interrupt the information flow paths.

The first step in our analysis is to compile a list of observables. This is done by using logic diagrams that first divide the activity into phases, for example, the design, construction, and operation phases. The activities in each phase then are expanded to finer and finer detail until observables can be identified. To bound the problem, some measure of importance must be attached to observables during this process. This is done by expert judgments.

The observables are represented by source nodes in acyclic directed graphs (hereafter referred to as information flow graphs). The graphs consist of nodes that represent steps in a leak path (for example, copying a classified document) and safeguards against information leakage. The sinks of the graph are collectors of information. The graph is represented by Boolean equations for each node. The node equations indicate the adjacent nodes by Boolean equations such as

$$N_1 = e_{12} N_2 + e_{13} N_3 \quad (8)$$

where the N 's are nodes or vertices and the e 's are the edges of the graph. This equation indicates that node N_1 is connected to nodes N_2 and N_3 by edges e_{12} and e_{13} , respectively.

Paths from observable sources to collector sinks are constructed by successive substitution into the graph equations. The nodes of the graph that represent safeguards failures are developed as fault trees, and the Boolean equations are substituted into the information flow graphs equations, giving a sequence of events leading to disclosure of an observable.

This approach has proven very useful for identifying qualitatively areas where information security can be upgraded. For example, steps in a procurement procedure that introduce many new leak paths can be circumvented. Some quantitative analysis is possible by assuming independence of events and using special data bases on human factors, trust violations, and security hardware failures. However, the principal value remains the increased qualitative understanding of the observables and leak paths.

Los Alamos also has applied these techniques to reducing the susceptibility of military systems. In this case, the goal is to reduce the likelihood of an adversary acquiring, identifying, tracking, targeting, or hitting a military asset. For example, the list of observables for a satellite may be developed by working from satellite missions to required functions. The functions necessitate systems, which are made of components. The components generate observable emanations such as infrared radiation or optical emanations. Thus, a signature of the system can be developed with locations, intensities, and time dependencies included for each class of observable emanation. The reduction of observables can be addressed by shielding of large-signature components, by anti-simulation, or by other deceptive techniques.

SUMMARY AND CONCLUSIONS

Analysis tools developed for reliability and risk assessment of complex systems have been applied to the systematic analysis of sabotage, combat, and security vulnerability. The most useful techniques have been fault-tree analysis with variable transformations, functional diagrams, and directed graphs. Some tentative attempts at quantification of the analysis have begun using human

factors and trust violation data, but much more effort is needed. The principal result of the work has been an increased qualitative understanding of system vulnerabilities, the effectiveness of countermeasures, and the ranking of scenarios by their attractiveness to saboteurs or other adversaries. The techniques have been applied to problems in nuclear reactors, the STS, defense, and information security.

REFERENCES

1. Bott, T. F., July 1985, "Sabotage Analysis and Risk Contributors to STS," Proc. of Seventh Annual System Safety Conference.
2. Cameron, D. F., July 1985, "Vital Areas at Nuclear Power Plants," Proc. of Seventh Annual Safety Conference.
3. Bolstad, J. W., and Haarman, R. A., May 1980, "Summary of Thermal-Hydraulic Calculations for a Pressurized Water Reactor," Los Alamos National Laboratory report LA-8361-MS.
4. Barts, E. W., and Bott, T. F., June 1984, "TRAC-PF1 Study of Loss of Pump Seals in a Westinghouse PWR," American Nuclear Society Transactions TANSO 46.
5. Stack, D. W., and Hill, M. S., April 1984, "A SETS User's Manual for Vital Area Analysis," Sandia National Laboratories report NUREG/CR-3134.