SAND91-0325C
TTC-1061

SAND--91-0325C

DE91 008576

VULNERABILITY ANALYSIS OF MANUFACTURING SYSTEMS: A Systematic Method for Protecting Industrial Production from Disruption*

Edwin A. Kjeldgaard and Michael G. Vannoni
Risk Assessment and Transportation Systems Analysis Division
Sandia National Laboratories**
P.O. Box 5800
Albuquerque, NM 87185
(505) 845-8361, (505) 845-8011
FAX: (505) 844-0244

and

G. Bruce Varnado and John W. Hockert
ERC Environmental and Energy Services Co.
7301-A Indian School Rd. NE
Albuquerque, NM 87110
(505) 881-9228
FAX: (505) 881-9357

Presented at the Environmentally Conscious Manufacturing
Technology Applications Workshop
Albuquerque, NM, February 20-22, 1991

* This work performed at Sandia National Laboratories, Albuquerque, New Mexico, supported by the United States Department of Energy under Contract DE-AC04-76DP00789

** A United States Department of Energy Facility

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 in electronic image products. Images are produced from the best available original document.

ABSTRACT

The U.S. DOE initiated the Production Risk Evaluation Program (PREP) at Sandia National Laboratories (SNL) to assess quantitatively the potential for serious production disruption as the result of random failures, accidents, natural disasters, or sabotage at its facilities. SNL developed a procedure incorporating both network and fault tree models that identifies production vulnerabilities. For each production step, a steady-state flow model computes the "critical time," which is the maximum period a step can be shut down without preventing the system from achieving production goals. The critical time is then used in fault tree analysis to determine the failure modes that can stop the process for longer than this period. Modular logic modeling is used for constructing the fault trees. Equipment restorable within its critical time need not be considered critical even though it may perform significant work. This paper focuses on sabotage, but the methodology is applicable to analyzing the other production system vulnerabilities mentioned above. The PREP models can be used to identify those plant areas to which a saboteur would need to gain access. A security strategy using graded protection based on a PREP analysis potentially could reduce security costs. PREP methods also provide quantitative insights to develop protection measures that do not infringe upon the liberties of personnel or complicate work practices.

INTRODUCTION

Identifying industrial sabotage targets in an integrated manufacturing system is most effectively performed by looking at the entire system. The U.S. Department of Energy's (DOE) nuclear weapons complex (NWC), uranium enrichment, and naval fuels facilities are examples of such systems. The isolated analysis of a disruption's consequences at a single site ignores the relationships between facilities. It is sometimes possible to use redundant equipment at other facilities to prevent a production disruption from stopping output. A manufacturing system may also increase production rates at all facilities to make up for output lost during an outage. The analytical methodology developed by the Sandia National Laboratories' Production Risk Evaluation Program (PREP) provides a logical method for identifying industrial sabotage targets from a system perspective. In addition, the PREP approach provides quantitative insights that can be used to develop and demonstrate the effectiveness of industrial sabotage protection measures that are based on consequence mitigation.

ANALYTICAL PROCEDURE

PREP was initiated to identify events that could, with significant probability of occurrence, cause an unacceptable outage in nuclear weapons production. The PREP study investigated the disruption of weapons manufacturing operations by accidents, natural phenomena, and random failures as well as industrial sabotage. An "unacceptable production outage" is the failure to produce a package of products consisting of a DOE-defined number of particular nuclear weapon types within a specified period. This period begins after the effects of an event cause the NWC to fail to make delivery from the final assembly plant.

The PREP analytical approach, summarized in Figure 1, embodies much of the underlying philosophy of probabilistic risk assessment

(PRA), but the tools and technical approach are quite different. PRA uses an event tree logic model to represent the combination of subsystem failures that will cause system failure. Possible causes of these subsystem failures are then identified and quantified using fault tree models. In contrast, the PREP approach employs a network model representing production process flows, and fault tree models that represent individual process failures. The PREP network model, unlike a PRA event tree, is not a logic model. Rather it is a detailed representation of a manufacturing system that can be used to determine the overall effects of a production failure.

A detailed survey of the manufacturing operations necessary to produce the PREP product package at each facility is used to develop a network model of the entire manufacturing system. The network consists of a set of vertices referred to as "nodes" and a set of directed arcs together with data associated with the arcs. The arcs represent the production steps and are the key elements of the model. Flow through an arc should be thought of as a quantity of a material or a part being processed within that arc. The incoming arcs to a node bring the ingredients needed by the outgoing production arc, which processes the ingredients into a new product. Each production arc is associated with a certain product and set of equipment and resources necessary to manufacture the product. Arc data (normal and expedited process times, sprint capacity, inventory, yield, bill of material, production schedule), along with several optimization algorithms, are used to compute the "critical time" for each arc. The critical time is defined as the longest period the production step could be shut down without causing an unacceptable production outage of the output package of products.

Fault tree analysis is then used to identify systematically events that could cause any production step to be out of service for longer than its critical time, thus resulting in system failure. Data, describing the number, location, and replacement time of equipment items used in each arc and support system requirements and failure mechanisms, is used to determine the combinations of events necessary to cause unacceptable production outages and to estimate their probabilities. Modular logic modeling, which relies on the fact that items of like function fail in similar ways, is used to assemble the fault trees. The resultant fault trees account for likely recovery actions the plant could implement to mitigate the impact of the failure. If the probability of an event is estimated to be significant, then the event is classified as a "critical link" in production. The probability of an act of sabotage is unknown and is often assumed to be 1.0 for security planning purposes. Relevant industrial sabotage targets are thus those items of equipment which, if destroyed, could not be replaced within the critical time of the associated production activity. An additional type of target that has become more attractive involves releasing hazardous materials into the environment since the recovery time, including political factors, can be significant.

Industrial sabotage targets have different relative importance. In most DOE activities there is no analogy to economic loss; the actual measure of consequence is the adverse impact on national security from a production failure. One measure of consequence is the length of time the production system would be behind its minimally acceptable schedule. "Time behind schedule" may thus be used as a surrogate value for the national security consequence. Because the probability of a sabotage attempt is unknown, time behind schedule is an appropriate measure for relative risk ranking of targets.

APPLICATION TO SECURITY PLANNING

Industrial sabotage is unique among production failure mechanisms because unlike other failure mechanisms, the probability of a sabotage attempt that initiates failure depends on a variety of factors that are largely independent of the production process. These factors include the deterrent effects of sabotage protection measures, the state of labor relations at the plant, and world political conditions. All these factors can vary widely in a short period of time. It is therefore impossible to use historical data to make quantitative risk estimates.

The traditional measures used to protect against sabotage are oriented toward the act itself. Protection against industrial sabotage by outside adversaries is generally provided by a combination of physical barriers, access controls, intrusion detection systems, and security force response. Protection against sabotage by facility employees ("insiders") is much more complex. Programs traditionally rely upon access controls, personnel screening, and searches for contraband. Personnel reliability measures include behavioral observation, drug testing, and work rules such as a two-person surveillance program. The effectiveness of such measures is much more difficult to determine than that for outsider protection.

Historical evidence indicates that the majority of saboteurs act on impulse and generally select targets of opportunity without in-depth consideration of the production or national security consequences of their actions (1). All the sabotage incidents for which the number of perpetrators was known were committed by a single individual, usually motivated by disgruntlement (2). Thus, the likelihood that a saboteur would select as a target a critical piece of equipment, in the PREP context, can be estimated by the ratio of critical targets to potential targets.

The PREP methodology can provide a systematic way to identify critical targets. Besides identifying industrial sabotage targets, the PREP analysis can also provide valuable insights into industrial sabotage protection strategy. Traditional measures used to protect against industrial sabotage emphasize prevention. The PREP analytical tools permit consequence mitigation to become part of a valid sabotage protection strategy as well.

Consequence mitigation strategies recognize the extreme difficulty in anticipating and preventing destructive acts and concentrate upon ensuring that such acts do not have lasting effects. There may be a considerable time lag between the destruction of equipment and the resulting production system outage. This time lag offers the system an opportunity to mitigate the consequence. Industrial sabotage protection measures of this type include: (1) stockpiling products in secured areas; (2) increasing the capacity of subsequent operations so they are capable of making up for lost production after repairs are made; (3) stockpiling critical spare parts or production equipment in secured areas; and (4) developing alternate production capabilities at another site. The first two strategies provide additional time to repair or replace damaged equipment without an unacceptable production outage. The third strategy reduces the time required to repair or replace the equipment, and the fourth limits an adversary's capability to cause sufficient damage to completely interrupt a vital production process. Each has cost benefit trade-offs that govern optimum choice in a given situation.

Such consequence mitigation programs have several potential advantages. First, it is relatively straightforward to demonstrate their effectiveness by means of the network and fault tree models. Second, these programs are not perceived to be as intrusive upon individual liberties as personnel reliability assurance measures such as behavioral observation and drug testing. Third, although consequence mitigation programs require an initial investment, they do not adversely affect productivity as do access controls and restrictive work rules. Fourth, with proper planning, these programs can serve not only to protect against industrial sabotage but also to reduce the overall risk caused by random equipment failures, industrial accidents, and natural phenomena.

The PREP methods can be used to establish the quantitative requirements for each of these measures including: (1) the type and number of products that would need to be stockpiled; (2) the amount by which the production capacity of subsequent processing operations would need to be increased; (3) the amount by which the equipment repair or replacement time would need to be reduced; and (4) the production capability and capacity that would be required for redundant facilities.

CONCLUSIONS

PREP analytical methods provide a structured, systematic approach to the identification of industrial sabotage targets in a manufacturing system. Under the current program, they were successfully applied in 1987 to the manufacture of nuclear weapons and appear to be generally applicable to any manufacturing complex. Based upon the critical times derived from the network model, we have constructed and solved fault trees for the individual production operations and identified potential industrial sabotage targets as well as other vulnerabilities. Our analysis demonstrates that, with proper planning, both security and system reliability can be improved through the use of appropriate consequence mitigation measures.

Development work is required to deal with creating integrated software to increase the ease and efficiency with which a risk assessment or target identification study can be performed. The PREP analysis process was only partly automated during its 1987 application to the NWC; extensive data collection and the creation of the network and fault tree models were done manually. Development is needed to automate both the collection of the network characteristic data and the structuring of the network. A longer-term goal would be to develop an expert system that would fully automate the assembly of the fault tree model given the input of key data.

REFERENCES

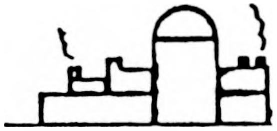
1. Mullen, S., Potential Threat to Licensed Nuclear Activities From Insiders, U.S. Nuclear Regulatory Commission, NUREG-0703, August 1980.

2. Sutton, R., Insider Adversary Study for the Office of the Inspector General, performed for the U. S. Department of Energy by International Energy Associated Limited, Report IEAL-295, August 1983.

DISCLAIMER

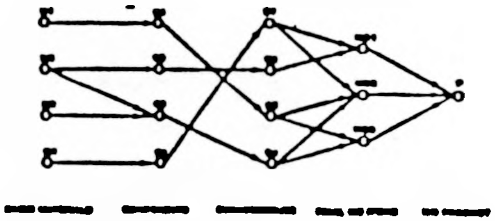
This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, 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.

Flow of PREP Analysis



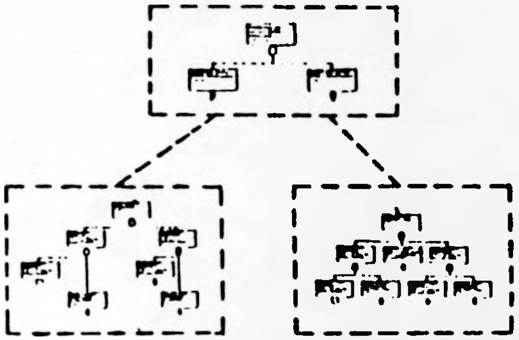
Plant
data

Scheduled production
Ratio & Yield
Sprint capacity
Flow times

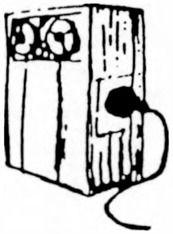


Network flow analysis

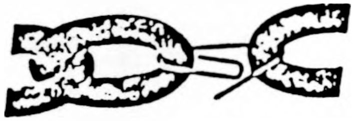
Critical times



Fault tree analysis



Fault tree evaluation
(SETS)



Potential critical links

Figure 1