CONF-781108--3

MASTER

DYNAMIC ANALYSIS OF NUCLEAR SAFEGUARDS SYSTEMS

NOTICE
This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Department of Energy, 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.

by

J. R. Wilson
D. M. Rasmuson
F. H. Tingey

EG&G Idaho, Incorporated
Idaho Falls, Idaho 83401

ABSTRACT

The assessment of the safeguards/adversary system poses a unique challenge as evolving technology affects the capabilities of both. The method discussed herein meets this challenge using a flexible analysis which can be updated by system personnel. The automatically constructed event tree provides a rapid overview analysis for initial assessment, evaluation of changes, cost/benefit study, and inspection and audit.

To be presented at the Fourth DOE Statistical Symposium, Albuquerque, NM, November 3, 1978

DYNAMIC ANALYSIS OF NUCLEAR SAFEGUARDS SYSTEMS

I. INTRODUCTION

In recent years a number of techniques have been developed for the analyses of the performance of complex systems involving both men and machines. These techniques are designed to assess the risks to society from unwanted events. Essentially all of the techniques utilize large networks and/or flow diagrams which show the sequencing and interrelationships between activities which lead to the unwanted event.

In the area of water reactor safety, The Reactor Safety Study[1], commonly known as the Rasmussen Report, used fault and event trees extensively, with a considerable body of technology being developed for the analyses of such trees.

Management Oversight and Risk Tree[2] (MORT) technology is being used throughout DOE and its contractors in occupational safety analysis. MORT is a comprehensive analytical procedure that provides a disciplined method for determining the cause and contributing factors of major accidents. Alternatively, it serves as a tool to evaluate the quality of an existing safety system. While similar in many respects to fault tree analysis, MORT is more generalized, works in success space and presents over 1500 specific elements of an ideal "universal" management program for optimizing occupational safety.

Diversion Path Analysis[3,4,5] (DPA) has been developed for application to nuclear materials safeguards. This technique systematically analyzes existing or proposed internal controls of a facility in order to identify potential vulnerabilities to successful diversion of material by an adversary. The technique makes extensive use of flow diagrams and a system of weights. Consideration of diversion paths is ordered in terms of material attractiveness and path complexity.

Each diversion path is evaluated by assessing the mass, time and space sensitivities of attempted diversion using that path. The techniques developed for DPA have proved to be extremely useful for assessing the contribution of internal control to the reduction of risk.

The usual approach in the evaluation of physical security systems is to assume the diverter is successful in obtaining the SNM. The analysis then consists of constructing computer simulation models of physical security systems, devising scenarios of system assaults, and evaluating the system against the assault. This analysis usually results in quantifying success paths and draws upon fault tree analysis technology.

A major problem in such analysis is that of accommodating change. Two major areas of change are the potential characteristics of the adversary and of the system. New technology influences both of these and should be accommodated in the analysis.

System characteristics evolve due to design improvements, experience, or temporary system changes. Experience may show that the design adequacy must be reassessed. Impairment of the system may result from temporary system changes such as unexpected maintenance, accidents, insufficient personnel, or subversion of the operating crew or guard force.

The solution to the dynamic safeguards problem is to make the analysis dynamic; that is, to make the analysis adaptable to real time situations and revisable by persons operating or inspecting the system. This paper presents such a methodology.

The methodology results in an analysis that can easily be updated as system and adversary characteristics change. The basic techniques applied to safeguards are extensions of those developed in support of the Reactor Safety Study, particularly event trees and associated analysis to identify system design interdependencies, redundancies, diversities, and vulnerabilities. The main

extension involves computer constructed event trees which are easily updated as the system changes. The loss mechanism is evaluated through application of probability methodology to these event trees.

An example is presented in detail to illustrate the power and flexibility of the technique.

II. THE GENERIC AUTOMATED EVENT TREE

Since the Reactor Safety Study, event trees have been recognized as a powerful tool for a broad system overview and enumeration of system failure sequences. While the fault tree is used to develop subsystem faults down to the component level, the event tree interrelates these subsystem fault trees. If detailed fault trees do not exist, interdependencies can still be diagnosed at the subsystem level. Thus, interdependencies between subsystems are displayed straightforwardly in the event tree. As each sequence is developed into success and failure branches for each subsystem, complete enumeration of all subsystem state combinations results.

This ability to compactly represent the full system analysis and to account for subsystem interdependencies has application to assessing the vulnerability of a nuclear facility to safeguards assaults. This is especially so with the generic subsystem, a collection of all subsystems which have a common nature or share susceptibilities to adversary attack.

For example, physical security analysts in the course of evaluating a system often calculate the probability that the adversary will successfully disable alarm A, then alarm B, and then alarm C. The theoretical probability is usually so small that an adversary would not dare the attempt if he knew the "odds." However, if the adversary attempts the crime, more than likely he is confident of bypassing all three alarms using the same skills. The alarms should be analyzed as one subsystem because the common nature of the alarms causes shared weaknesses. This illustrates the grouping of physical security subsystems into generic sybsystems.

The usefulness of event trees for systems analysis is significantly increased through automation. Using the computer code, AUTOET III[6], developed at INEL, the

event tree is automatically constructed, with unnecessary branches eliminated, and resulting tree and relevant calculations printed as output.

Advantages resulting from automation include:

(1) The event tree is rapidly constructed, relieving the analyst of drafting and calculation concerns, and

(2) Changes can be incorporated and results quickly produced, making the analysis flexible. In the area of safeguards where constant system improvements are expected, along with evolving adversary capabilities, such flexibility is essential.

1. INPUTS

The application of AUTOET III to evaluate facility assaults requires:

(1) Characterization of the physical security system by generic subsystems.

(2) Obtaining the generic subsystem cut sets in terms of subsystem interdependencies and adversary characteristics. (A cut set is the collection of necessary and sufficient events that would result in a failed system.)

(3) Estimation of maximum path time.

(4) Subsystem failure mode consequences.

1.1 Generic Subsystem

The generic subsystems which can affect the success of the adversary must be specified. In the usual case these include power systems, physical barriers, alarms, communication devices and networks, guards, and offsite response teams. The independent failure probabilities of each of these subsystems is also an input to the code.

The order in which the subsystems are input is dictated by time or dependency sequencing. Subsystems which the adversary will encounter first, or whose failure will influence other subsystems, must come first.

1.2 Maximum Path Time

The primary purpose of the onsite physical security system is to delay the adversary until sufficient offsite reinforcements arrive. Therefore, if this offsite response force does not arrive, an adversary of sufficient size and skill should be capable of obtaining its objective. The maximum path time is the time required for the adversary to reach his objective, given that all onsite security systems function as designed, and the offsite response force does not arrive.

1.3 Generic Subsystem Cut Sets

Each subsystem may fail independently or due to previous subsystem failures and/or employed adversary characteristics. Additional situations, called conditional events, also contribute to subsystem failure. Each of these can belong to a generic subsystem cut set; its affect upon the system is discussed below.

1.3.1 Previous Subsystem Failures

The treatment of these failures is standard to event tree analysis. If a subsystem has a sequence in which all subsystems of a cut set are failed, that subsystem is failed. A cut set composed of only previous subsystems is a "total failure" cut set.

1.3.2 Adversary Characteristics

An adversary characteristic is a weapon or individual skill used to defeat the system. Each adversary characteristic is assigned a probability

$$P(\text{Characteristic}) = P\begin{pmatrix}\text{the subsystem fails,}\\ \text{given the characteristic}\\ \text{is present}\end{pmatrix} * P\begin{pmatrix}\text{adversary possesses}\\ \text{sufficient quantity}\\ \text{of skill in that}\\ \text{characteristic}\end{pmatrix}$$

Any cut set containing an adversary characteristic is a "partial failure" cut set.

1.3.3 Conditional Events

A conditional event allows for more accurate system modeling. For example, in a system without emergency power, failure of offsite power fails

the alarm system, and is a "total failure" cut set. In another system, failure of offsite power and onsite emergency power, conditioned with failure of response force emergency power, fails the alarm system. This conditional event produces a "partial failure" cut set.

1.3.4 Path Time Reduction Factors

Associated with each cut set is a number that represents the path time reduction resulting from the subsystem failure in that mode. Thus, with a reduction factor of .5 for a given cut set, the adversary can cut his path time in half.

1.4 Subsystem Failure Mode Consequences

Whenever a physical security subsystem fails, the adversary's path time is decreased, and his probability of success is increased. The probability of success is estimated by the subsystem cut set probability. The path time decrease is represented by a fraction assigned to each cut set. This is the consequence of that failure mode of the subsystem. Each failure mode has a distinct consequence depending upon how badly the subsystem is disabled.

At each branch in the event tree, the weighted average of the relevant failure mode consequences is calculated, and multiplies the previous consequences in that sequence. The total consequences of a sequence multiply the maximum path time, yeilding the sequence path time.

If a particular branch point has both "total failure" and "partial failure" cut sets, no weighted average is calculated since all "total failure" cut sets have failure probability of one. Instead, the maximum path decrease of the "total failure" cut sets is selected for further calculations.

III. APPLICATIONS

The advantages of AUTOET III are rapid, automatic event tree construction, broad system overview, and flexibility to input changes. These advantages encourage the following applications:

(1) Initial System Assessment

(2) Cost/Benefit Analysis

(3) Online Evaluation by Plant Manager

(4) Inspection and Audit

1. INITIAL SYSTEM ASSESSMENT

In the design stage, a system has frequent design changes and little component resolution. As each design change evolves, rapid, complete analysis is advantageous; such an analysis is very time consuming if conducted by hand.

In the early design stage, many decisions yet remain about component design; hence, component analysis is incomplete. However, interdependency analysis on the subsystem level is just as feasible, and valid, as at later stages.

2. COST/BENEFIT ANALYSIS

In a cost/benefit analysis, many combinations of benefit packages exist. Rapid, thorough analysis of each option is crucial; again, this is difficult to accomplish by hand. An automatic analysis can be set up to evaluate these many options, if benefits and costs are assumed independent. Techniques for evaluating cost/benefit study results are given in the Joint Results Section.

3. ONLINE EVALUATION BY PLANT MANAGER

After the system has been analyzed and built, the analysts go to other tasks. The analysis is finished and fixed. To incorporate any changes, another analysis

staff must be assembled, unless a flexible analysis tool exists.

Using AUTOET III, the plant manager can make changes to the input of the initial analysis to reflect system upgrades, maintenance activities, and unavoidable system degradations. Suspected increases in adversary characteristics can be accounted for. Failures can be evaluated to determine pattern, and reveal insider preparations for an adversary attack.

4. INSPECTION AND AUDIT

AUTOET III would also be useful to the inspection and audit function in assessing the vulnerability of particular physical security systems. Tables can be developed for assisting the inspector in the determination of input data. Also relevant inspector experience can be factored in to provide independent assessment.

IV. SPECIFIC EXAMPLE

The technique is illustrated by application to a hypothetical reactor complex containing SNM primarily in the form of fuel elements. Input was formulated by knowledgeable safeguards and security personnel familiar with such facilities. Two cases, a reference and an upgrade, were considered in order to demonstrate the cost-benefit potential of the technique.

1. REFERENCE FACILITY

1.1 System Description

The reference system consists of a single exterior fence with hourly security checks. The post guard checks all entering traffic and is stationed in a non-hardened cublicle. The roving guard maintains radio contact with the post guard, except in certain areas where transmission is impossible; his rounds take two hours. All alarms annunciate locally, with inadequate location information. Loss of offsite power disables all alarms.

1.2 Adversary Characteristics

The adversary is assumed to conduct an overt/covert attack with six men and an insider. Covert attack can be analyzed with appropriate input changes. Several skills are assigned the adversary, with probability values listed in Tables II and VI. The characteristics differ with the system because only the minimum skills required for subsystem defeat are listed. The level of skill is assumed to be equal to that found in the military or prisons.

1.3 Input Description

The input for the existing facility is summarized in Tables I through IV. In Table I the generic subsystems are listed across the top. The next row is the independent failure probability of each subsystem. The subsystem cut sets are listed next. The number under each cut set is the path time reduction factor.

1.4 Results

The event tree for the reference system analysis is shown in Figure 1. A high probability path combined with a low path time is of concern. Therefore the path probability is divided by the path time to give the significance which is a relative weighting of the importance of a path to adversary success. High significance paths should be given additional analyst attention.

The probability that a particular path describes the outcome of an attack is listed in the probability column. If the path ends in capture, no path time is printed out, nor is any further calculation done.

The most significant path (7.87×10^{-2}) is the ninth from the top. Although the path time is large, the high path probability more than makes up for it. The system weaknesses pointed out by this path are the dependence of the guards on a secure alarm system, and the vulnerability of the guards. The analyst would therefore recommend immediate attention in these two areas. More complex recommendations would follow similarly.

2. PROPOSED FACILITY

2.1 System Description

The proposed system has a lighted double fence with closed circuit TV (CCTV) and microwave intrusion monitoring. All alarms are upgraded, annunciate locally with detailed location information, and signal the offsite response force. Onsite emergency power picks up crucial security system loads upon loss of offsite power.

The post guard has a hardened station, which is monitored with CCTV by the offside response force, and the SNM storage areas have permanent guards. Whenever the roving guard must break radio contact, an additional guard must be stationed nearby. The two-man rule applies any time the guards enter a target area

(SNM storage), and more guards are hired.

2.2 Input Description

The input for the proposed system is given in Tables V through IX:

Table V - Proposed System Cut Sets

Table VI - Assumed Adversary Characteristics

Table VII - Conditional Events Inputs

Table VIII - Analysis Assumptions

Table IX - Benefit Costs

The cut sets are essentially the same as for the reference system. Due to system upgrades, the adversary success probabilities have been reduced where appropriate. The adversary appears more formidable in this analysis because the system upgrades require additional use of adversary skills.

2.3 Results

The most significant path (1.53×10^{-4}) is the second from the top. The system weakness portrayed is the vulnerability of the offsite response force. Analyst suggestions may include increased manpower, firepower, and protection, or a diverse offsite response force.

3. JOINT ANALYSIS OF RESULTS

Obviously, the proposed system is better than the old system, but any time money is involved, the degree of improvement is important. Before the improvement is assessed, path times exceeding the average offsite response force time are eliminated. The adversary is assumed captured on these paths. No paths can be eliminated from the existing system results; six paths are eliminated from the results of the proposed system.

The remaining paths are summed to obtain probability of adversary success. The adversary success probability is .936 for the existing system and .0016 for the proposed system.

The total cost of system upgrades relevant to overt attack is $4.76 million. The cost for a one percent increase in reliability is $50,000. This cost/(reliability unit) may be useful in the future for setting a minimum cost/benefit standard.

Alternatively, the number of paths greater than a set significance level may be compared. The existing system has 12 paths with significance greater than 10^{-4}. The proposed system has only one path at that significance level. It is difficult to set a quantitative criterion based on this; however, viewed qualitatively, a system with one "substandard" path is stronger and easier to protect than a system with 12 "substandard" paths.

V. CONCLUSIONS

AUTOET III is a valuable tool for a rapid, flexible overview of the design stage, onsite real-time operation, cost/benefit, and international safeguards network. A checkout and verification of the methodology should be conducted with a multi-facility analysis.

Benefits of this multi-facility analysis are as follows:

(1) Checkout and fine tuning of code and procedures.

(2) Evaluation of these existing plants and proposed upgrades.

(3) Condensation of experience into standard procedures, tables of data and guidelines for future inspections (i.e. IAEA inspection and audit, etc.).

VI. ACKNOWLEDGMENTS

The authors are grateful to F. J. Balkovetz, J. J. Britschgi, and D. E. Six of EG&G Idaho for their helpful comments and suggestions.

VII. REFERENCES

1. U.S. Nuclear Regulatory Commission, Reactor Safety Study, WASH-1400, NUREG 75/014 (October 1975).
2. U.S. Department of Energy, MORT User's Manual ERDA-76/45-4, SSDC-4 (Rev. 1) (November 1976).
3. W. M. Murphey, J. C. Schleter, and M.D.K. Maltese, "Internal Control Vis-a-Vis Diversion Path Analysis," Nuclear Materials Management, 2, 1973, p. 232.
4. W. M. Murphey, and J. C. Schleter, "Practicality of Diversion Path Analysis," Nuclear Materials Management, 3, 1974, p. 236.
5. M.D.K. Maltese, K. E. Goodwin, and J. C. Schleter, Diversion Path Analysis Handbook, ERDA (October 1976).
6. J. R. Wilson, Automatic Event Tree Analysis: AUTOET III User's Guide, in preparation.

TABLE I

REFERENCE SYSTEM CUT SETS

Generic Subsystem	Power (Offsite)	Barriers (Fence, Vault)	Alarms (Contact, Motion)	Communications (Radio, Telephone)	Guards (Post, Roving)	Offsite Response Force
Independent Failure Probability	10^{-5}	10^{-8}	10^{-6}	10^{-6}	10^{-4}	10^{-5}
Subsystem Cutsets/ Path Time Decrease	EXPLO1 .7	EXPLO2 .5 COLLUSION .5	LOCKPICK .9 BARRIERS, B .7 POWER .6 ENVIRONMENT .7	RADIO JAM .7	COMMUNICATIONS, D .2 ALARMS, A .2 BIOLOGICAL1 .2 COLLUSION .6	GUARDS .2 COMMUNICATIONS, C .2 BIOLOGICAL2 .2 CAPTURE 1.

TABLE II

ASSUMED ADVERSARY CHARACTERISTICS

FOR THE REFERENCE SYSTEM ANALYSIS

Adversary Characteristic	Explanation	Probability
EXPLO1	Sufficient explosives to destroy offsite power.	.1
EXPLO2	Sufficient explosives to destroy vault.	.05
LOCKPICK	Capability to bypass vault door, and door contact alarm.	.5
COLLUSION	Insider aids adversary in bypassing guards and barriers.	.01
ENVIRONMENT	In the general sense, represents degradation in guard vigilance due to a history of false alarms, or alarm oversaturation at time of attack, caused by storm conditions, stray animals, or adversary action.	.05
RADIO JAM	Successful jamming of radio without tipping off location of attack.	.1
BIOLOGICAL1	Personal attack on onsite guards which removes them from action.	.9
CAPTURE	Represents the ability of the adversary to deal with the offsite response force. If probability = 1.0, capture is assured, given timely response.	1.0
BIOLOGICAL2	Personal attack on offsite response force which removes them from action.	.01

TABLE III

CONDITIONAL EVENT INPUTS FOR

REFERENCE SYSTEM ANALYSIS

Conditional Event	Explanation	Probability
A	Given that alarms fail, guards don't detect intruders.	.95
B	Given that barriers and contact switch fails, motion detector doesn't detect intruders.	.1
C	Given that communications fail, suspicion of offsite response force isn't aroused in time.	.5
D	Given that roving guard communication fails, post guard doesn't sound alarm.	.7

TABLE IV

ASSUMPTIONS FOR THE REFERENCE SYSTEM ANALYSIS

1. The adversary has a maximum of six men and one insider.

2. The offsite response force has a bullet-proof communications center and an armored personnel carrier.

3. The adversaries outnumber the onsite guards, so the offsite response force must arrive in time to capture the adversary. Timely arrival implies capture.

4. The offsite response force time is 70 minutes, which allows a one hour delay in detecting and reporting initiation of adversary activity.

5. Onsite explosions and gunfire cannot be detected from the offsite response force communciations center.

6. Maximum path time is 90 minutes.

7. Prior to attack, a drill was conducted, which should make the security force temporarily more alert, increasing maximum path time by 50%.

TABLE V

PROPOSED SYSTEM CUTSETS

Generic Subsystem	Power (Onsite)	Barriers (Lighted Double Fence, Vault)	Alarms (Contact, Motion, CCTV, Microwave)	Communications (Radio, Telephone)	Guards (Post, Roving, Station, Backup)	Offsite Response Force
Independent Failure Probability	10^{-5}	10^{-9}	10^{-7}	10^{-6}	10^{-6}	10^{-5}
Subsystem Cutsets/ Path Time Decrease	EXPLO1 .7	EXPLO2 .5 COLLUSION1 .5	LOCKPICK .9 BARRIERS, EXPLO3 .7 POWER, C .6 ENVIRONMENT .7	JAM, ALARMS .7	COMMUNICATIONS, E .2 ALARMS, A .2 BIOLOGICAL1 .2 COLLUSION .6	GUARDS 6 .2 CAPTURE 1. COMMUNICATIONS, ALARMS, F .2 BIOLOGICAL2 .2

TABLE VI

ASSUMED ADVERSARY CHARACTERISTICS

FOR THE PROPOSED SYSTEM

Adversary Characteristic	Explanation	Probability
EXPLO1	Sufficient explosives and skill to knock out onsite emergency power. Additional protection of onsite emergency power decreases probability.	.01
EXPLO2	Sufficient explosive and skill to pierce vault without activating door alarms and CCTV. Upgraded vault and alarms decrease probability.	.01
COLLUSION1	Insider aids adversary in defeating barriers. Larger guard force and two-man rule decrease probability.	.005
LOCKPICK	Sufficient security and electronic skill to shortcircuit alarms and vault door.	.1
ENVIRONMENT	In the general sense, represents degradation in guard vigilance due to a history of false alarms, or alarm oversaturation at time of attack, caused by storm conditions, stray animals, or adversary action.	.7
RADIO JAM	Successful jamming of radio without tipping off location of attack.	.01
BIOLOGICAL1	Personal attack on onsite guards which removes them from action. Hardened guard post, more guards and two-man rule decrease this probability.	.05
COLLUSION2	Insider helps neutralize guard force. Increased size of force, improved alarms and two-man rule decrease this probability.	.001
CAPTURE	Represents the ability of the adversary to deal with the offsite response force. If probability = 1.0, capture is assured, given timely response.	1.0
BIOLOGICAL2	Personal attack on offsite response force which removes them from action.	.01

TABLE VII

CONDITIONAL EVENTS INPUTS

FOR THE PROPOSED SYSTEM

Conditional Probability	Explanation	Probability
B	Given that barriers are bypassed, no detection results.	.03
C	Given that onsite power fails, CCTV power source also fails.	.1
E	Given that communications fail, suspicion of offsite response force is not aroused.	.1
A	Given that alarms fail, guards fail to detect intruders.	.5
G	Given that guards are neutralized, remote annunciation alarms and CCTV fail to arouse suspicion.	.005
F	Given that alarms and communication fail, suspicion of offsite response force is not aroused.	

TABLE VIII

ANALYSIS ASSUMPTIONS FOR THE PROPOSED SYSTEM

1. The adversary has a maximum of six men and one insider.

2. The offsite response force has a bullet proof communications center and an armored personnel carrier.

3. The onsite guard force is assumed comparable in size to the adversary force.

4. The offsite response force time is 40 minutes, which allows a half hour delay in detecting and reporting initiation of adversary activity.

5. Onsite explosions and gunfire cannot be detected from the offsite response force communications center.

6. Maximum path time is 180 minutes.

7. Prior to attack, a drill was conducted, which should make the security force temporarily more alert, increasing maximum path time by 50%.

8. Two-man rule applies in all potential target areas.

TABLE IX

BENEFIT COSTS

Proposed System	Cost (Million $)
Lighted double fence, CCTV, microwave detection system.	1.5
Consolidation of SNM storage sites, additional motion detectors, contact alarms, and CCTV for alarm assessment.	1.2
Hardened onsite guard post.	.062
Alarm upgrade.	1.0
Dedicated computer for real time accountability (impacts covert adversary only).	.050
Two-man rule, increased guard force, require upgrade and/or security clearance.	1.0

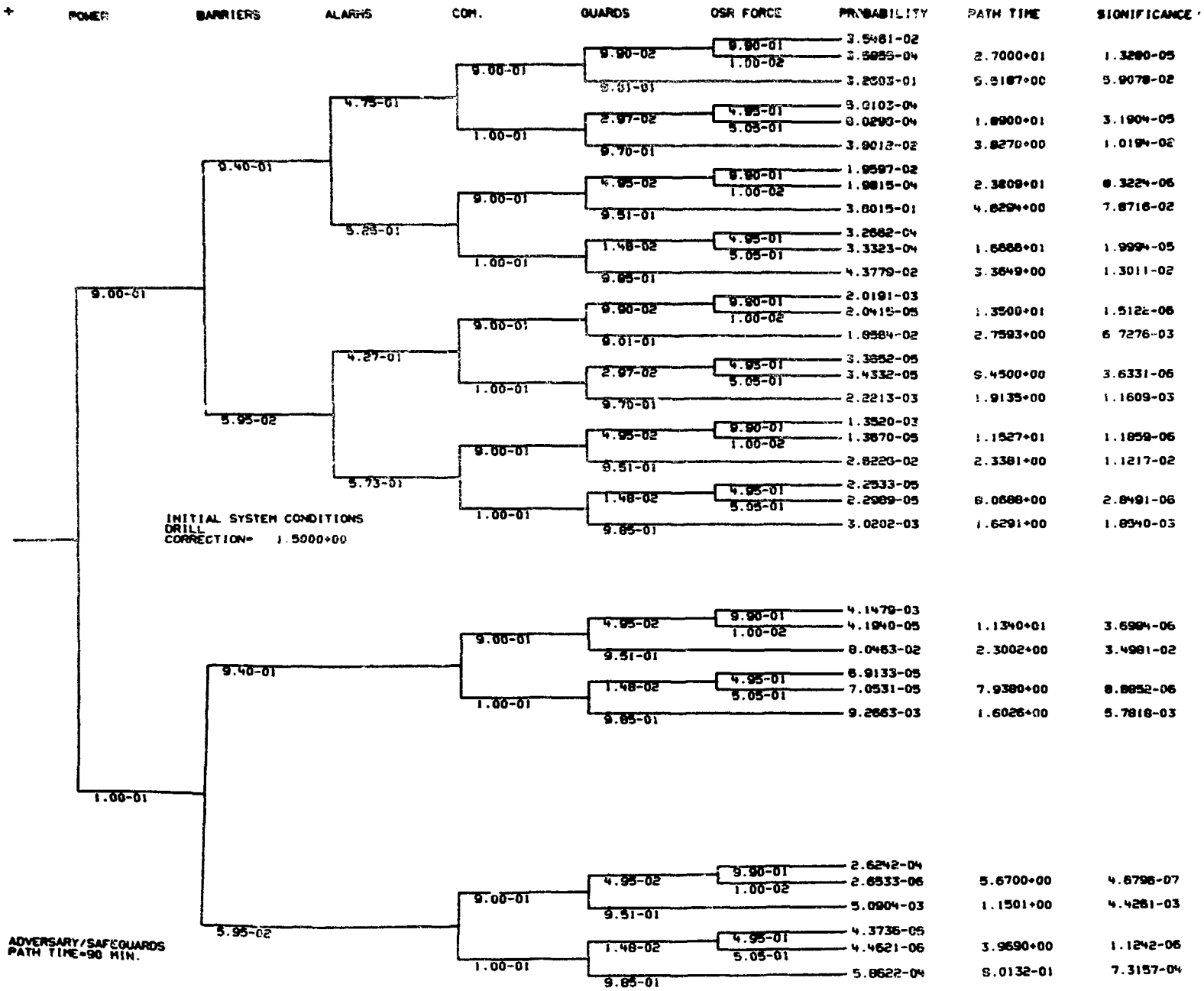

Fig. 1 Printout of reference system.

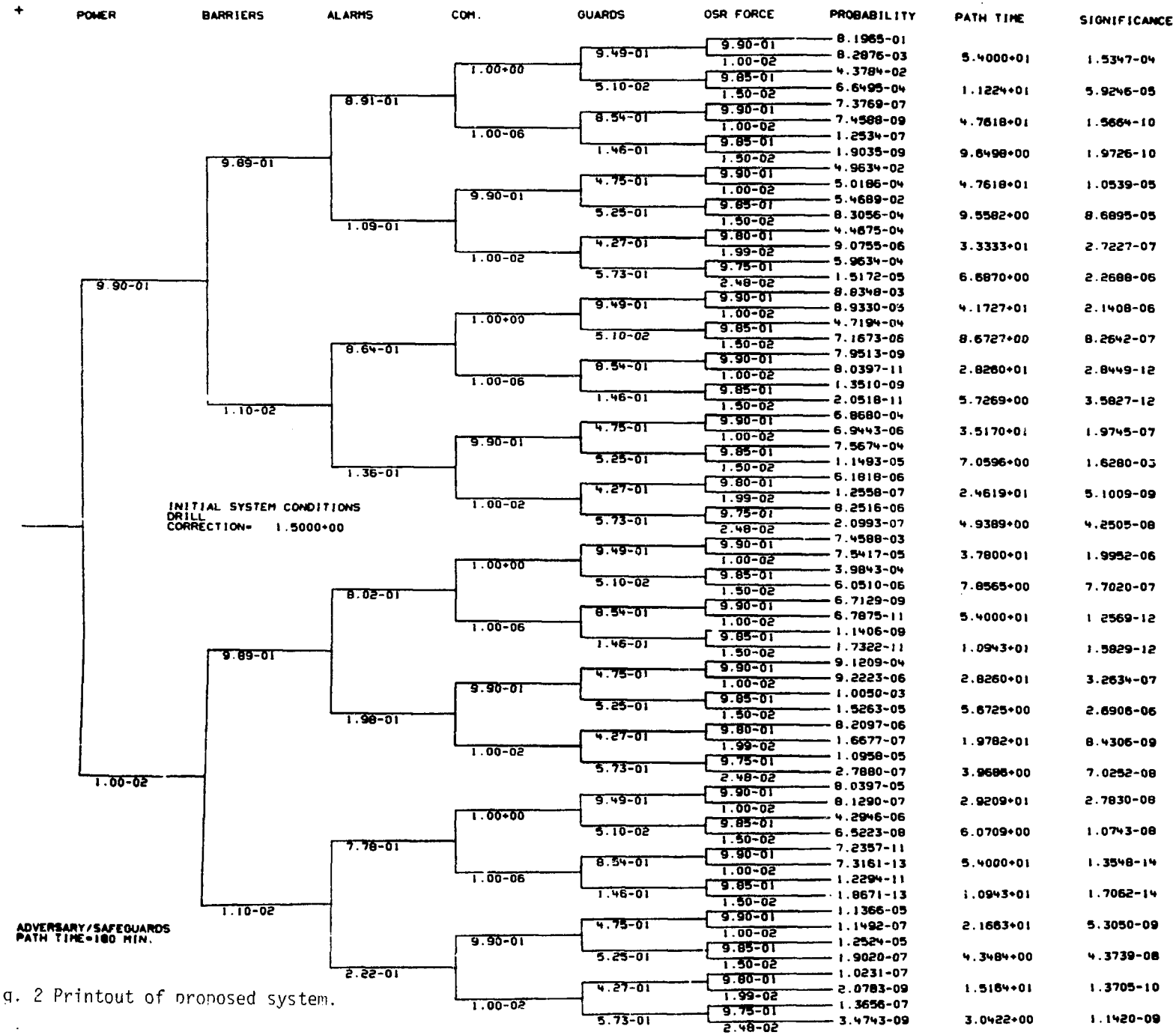

Fig. 2 Printout of proposed system.