INTERNATIONAL JOURNAL OF COMPUTERS
Issue 3, Volume 3, 2009

Analysis of Information Security Problem by Probabilistic Risk Assessment

Naoki Satoh, Hiromitsu Kumamoto

***Abstract*—** The information security risk assessment is investigated from perspectives of most advanced probabilistic risk assessment (PRA) for nuclear power plants. Accident scenario enumeration by initiating events, mitigation systems and event trees are first described and demonstrated. Assets, confidentiality, integrity, availability, threats, vulnerabilities, impacts, likelihoods, and safeguards are reformulated by the PRA. Two illustrative examples are given: network access attacker and physical access attacker. Defenseless time spans and their frequencies are introduced to cope with non-rare initiating events of information security problems. A common event tree structure may apply to variety of security problems, thus facilitating the risk assessment.

Keywords— Information security, Probabilistic risk assessment, Initiating event, Mitigation system, Asset, Threat, Vulnerability, Impact

I. Introduction

At a first glance an information security problem is far different from a nuclear power plant risk assessment, because the former primarily deals with virtual information whereas the latter with physical processes[21,22,23]. This paper demonstrates that, from perspectives of probabilistic risk assessment (PRA), these two problems may have more commonalities than differences.

The first landmark application of the PRA occurred more than 30 years ago. This is known as the WASH-1400 Reactor Safety Study[1]. Sophisticated models and attitudes developed for nuclear PRAs have found their way into other industries including chemical, railroad, aerospace systems[2]. The PRA methodology has advanced and matured to a point where standards become available to guide and evaluate each PRA performed for a particular nuclear plant. The ASME standard, for example, consists of high level requirements and supporting requirements for each major step of PRA[3]. The risk is defined as a pair of impact and likelihood. Both qualitative and quantitative risk assessments can be performed by generating scenarios called accident sequences. Initiating events, mitigation systems and event trees are used to enumerate these scenarios[4,5].

A good survey of information security risk assessment is found in a cyber security article[7]. OCTAVE (Operability Critical Threat, Asset, and Vulnerability Evaluation) classifies threats by event trees[8] to depict relatively simple scenarios. The event tree headings are "asset", "access", "actor", "motive", "outcome", and "impact". The first four headings, however, are unfamiliar to ordinary PRA event trees which model responses of mitigation systems.

Attack trees are versions of fault trees to represent how attackers succeed in achieving their objectives[9,10]. Only a limited scope of scenarios can be generated because of the use of fault trees. For example, emergency responses to a stolen key of a door are not included in the attack trees. The traditional PRA uses event trees to enumerate scenarios; the fault trees are used to search for causes of scenarios.

The RAPSA article[11] includes the term "PSA (Probabilistic Safety Assessment)" in its title. The PSA is a synonym of PRA. It is claimed that event/fault trees will be used where needed to assist with understanding how attacks can be neutralized. Attack scenarios are first given prior to event trees. The event trees are suggested to be used to evaluate these given scenarios. Scenario enumerations by event trees are not performed.

It is now clear that few have applied a genuine PRA to the information security problem. This paper depicts a potential scheme for such application through correct understanding of PRA concepts and methodologies. This PRA methodology consists of below two steps:

ETA(Event Tree Analysis) for describing accident sequences. The root node is an initiating event of the scenarios. A branch

point is called “Node” correspond to function or action This sample is indicated in Fig1.

FTA(Fault Tree Analysis) for analyzing the reason of abnormal situation. Fault Tree(FT)

is an and/or tree. It is used for the analysis of the reasons why each function correspond to

the event tree node failures/falls down. This sample is indicated in Fig2.

F. A. Author is with Kyoto University, Graduate School of Informatics e-mail: Sato@sys.i.kyoto-u.ac.jp.

S. B. Author, Jr., was with Kyoto University, Graduate School of Informatics (e-maial: kumamoto@i.kyoto-u.ac.jp).

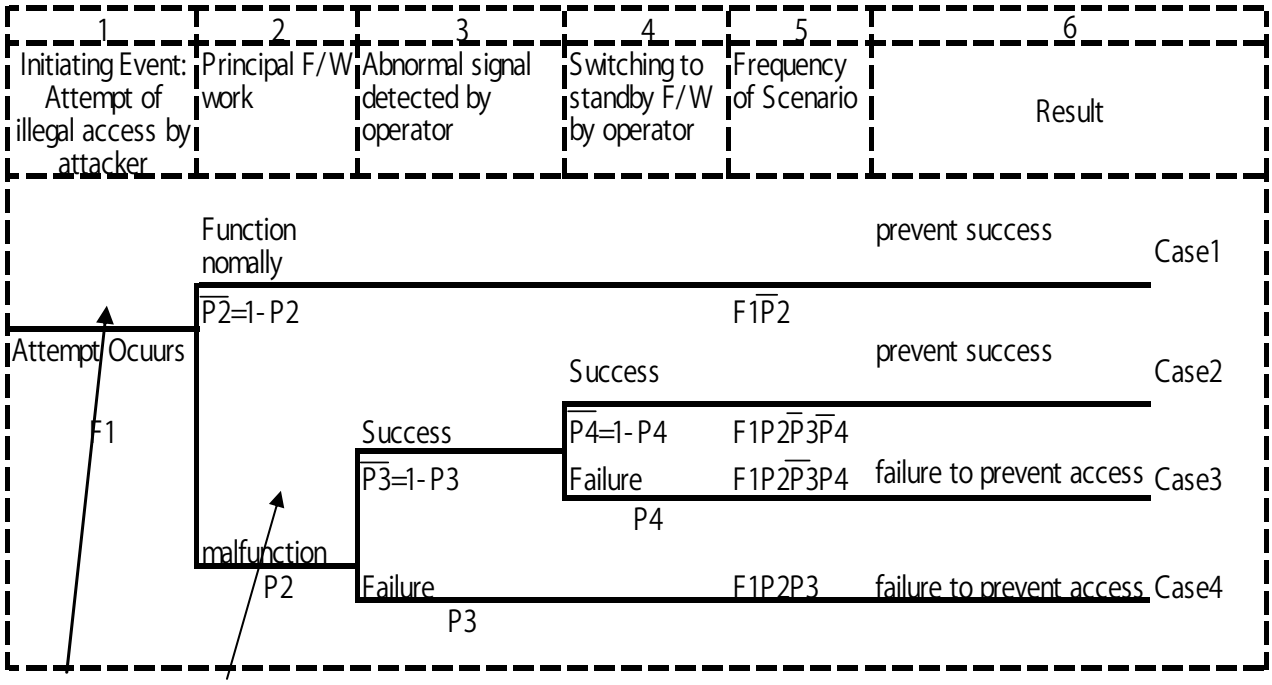

Fig 1: ETA Sample

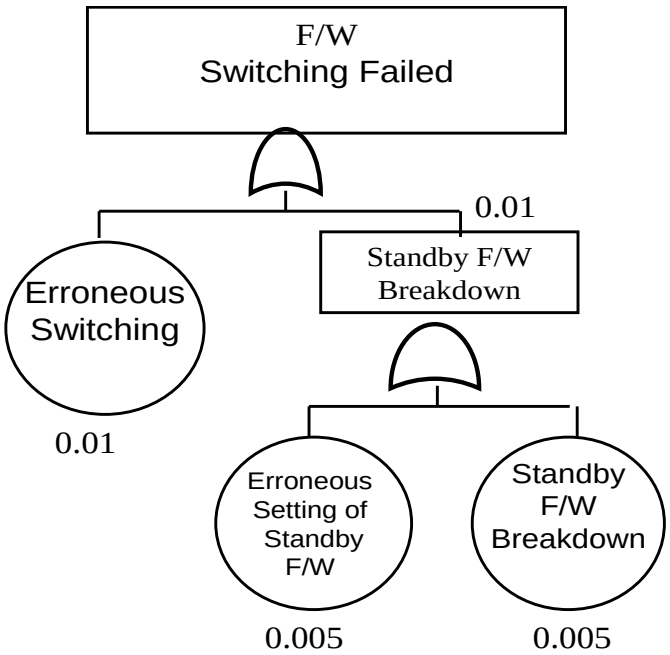

Fig2: FTA Sample

Table1:Comparison of physical(nuclear) and virtual(information security) PRA

	Asset	Accident	Initiator	Mitigation system	Impacts	Likelihoods
Nuclear PRA	Core material	Core damage	Internal and external initiating events	Failure modes	Quantitative or qualitative	Annual frequencies or qualitative
information security PRA	Valuable information and information systems	Loss of confidentiality, integrity, or availability	Portion of threats	Portion of vulnerabilities	Low, medium, high	Low, medium, high

II. PRA Concepts and Methodologies

In this section, a sample case is discussed; therefore, in regard to the details of PRA, please refer to the literature and our previous study[11,12].

A. Initiating Events and Event Trees

The definition of initiating event in the ASME PRA standard [3] can be rephrased as follows. An initiating event is any event either internal or external to the plant that perturbs the normal operation of the plant, thereby initiating responses of plant mitigation systems whose failure could lead to an accident. For the nuclear power plant the accident is core damage.

The initiating event is the most important concept of the nuclear PRA. The event has a potential to initiate a series of events eventually leading to core damage of a nuclear power plant. There are a variety of initiating events. All the scenarios leading to core damage can be found if all the initiators and the succeeding events are enumerated.

An event tree is a key methodology to enumerate accident scenarios. The event tree is a logic diagram that begins with an initiating event and progresses through a series of branches that represent expected system or operator performance that either succeeds or fails and arrives at either successful or failed end state[3]. Accident scenarios from each initiating event are enumerated by the event tree starting with the event.

B. Risk Reduction Measures

Four major steps of risk reduction can be considered as shown in Figure 1) inherently safer design, 2) initiating-event prevention, 3) initiating-event mitigation, and 4) accident mitigation. A level one PRA primarily deals with the initiating event mitigation phase with a secondary consideration of initiating event prevention. Accident mitigations are dealt with by level two and three PRAs[4,5]. This paper focuses on the level one.

The inherently safer design is based on elimination of hazards. Accidents can not occur when hazards are removed by the inherently safer design. An overhead crossing is an elimination of an intersection, a typical hazard in transport. In many cases only portions of hazards can be removed by the inherently safer design. For the hazards not eliminated, initiating events are identified.

An accident can not occur when each initiating event is prevented or mitigated successfully.

The mitigation prevents the initiating event from propagating to an accident. The operator shutdown of the pressure-tank system acts as an initiating-event mitigation.

Accident mitigations come into play after an accident occurs by failures of the initiating-event prevention and mitigation. A typical accident mitigation is a radioactive material containment to prevent a harmful release into the environment. The containment as an accident mitigation aims at preventing release of harmful materials. Thus, the core-damage accident is mitigated by preventing the release. Washing facilities for removal of contamination and first aid[13] can be regarded as a consequence mitigation. The accident mitigation includes the containment and the consequence mitigation.

III. Information Security Concepts

A. Assets

The radioactive material at the core of a nuclear power plant is the asset to be protected for the nuclear PRA. In information security the asset is defined as various types of information and related information systems that are valuable to an organization.

B. Accident

The Federal Information Security Management Act of 2002 (FISMA) defines "information security" to mean protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide "confidentiality", "integrity" and "availability"[14,15]:

1) Confidentiality: The information is protected from unauthorized or accidental disclosure.

2) Integrity: The information is as intended without inappropriate modification or corruption.

3) Availability: Authorized users can access applications and systems when required to perform their jobs.

These three requirements are security objectives for information and information systems. Therefore, as shown in

Table \ref{NPRA-ISPRA}, an accident for information security can be defined as a loss of confidentiality, integrity, or availability[16], while the accident of nuclear PRA is the core damage.

Compared to the nuclear PRA, there exit far more varieties of information types as assets targeted by the risk assessment. The information types include privacy, medical, propriety, financial, investigative, contractor sensitive, and security management[16]. A particular asset has to be specified clearly for the risk assessment. The lack of this specification forms a source of confusion.

Consider, for instance, password information. An information security accident occurs when a password is stolen if the password information itself is an asset targeted by the risk assessment. Suppose on the other hand that financial information is protected by the password. As described shortly, the stolen password is an initiating event. The stolen password does not necessarily yield an accident for the financial information when the password is promptly invalidated by security management.

C. Threats and Initiating Events.

For the information security problem, a threat is defined as a cause of potential impact to the organization (ISO 17799). The threat is also defined as an event or entity with potential to harm the system (NIST). The threat is any circumstance or event that could harm a critical asset through unauthorized access, compromise of data integrity, denial or disruption of service, or physical destruction or impairment.

The threats are classified as follows[15].

1) Natural threats: Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.

2) Human threats: Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent information entry) or deliberate actions (network-based attacks, malicious software, unauthorized access to confidential information).

3) Environmental threats: Long-term power failure, pollution, chemicals, liquid leakage.

Most of the natural threats and environmental threats are called external initiating events by the nuclear PRA. These external events are dealt with separately from internal initiating events. The human threats can be regarded as internal initiating events even if attackers reside outside of the information system.

According to the nuclear PRA, initiating events are delineated by mitigation systems to respond to the event. Consider for instance a stolen password. The asset is financial information protected by the password. Suppose that a password invalidation process as a mitigation system is activated against the stolen password. In this case, the stolen password becomes an initiating event for an information security PRA for the financial information.

The OCTAVE approach distinguishes a physical access attacker from a network access attacker[8]. This is reasonable because different mitigation systems are used for the two types of attackers.

D. Vague Concept of Vulnerabilities

The information security discipline defines vulnerabilities a condition or weakness or absence of security procedures, technical controls, physical controls, or other controls that could be exploited by a threat. Vulnerability classes and examples are[17]:

1) Physical: Unlocked doors. Unguarded access to computing facilities.

2) Natural: Facility located on a fault line.

3) Hardware: Systems not physically secured.

4) Software: Missing patches. Deliberately placed weaknesses such as keyloggers.

5) Communications: Unencrypted network protocols.

6) Human: Poorly defined procedures yielding insufficient incident response preparedness. Stolen credentials.

These vulnerabilities reflect different aspects. The unlocked door is a failure mode of an physical access control as a mitigation system. The facility on a fault line contributes to an increase of an external initiating event of earthquake. This is a contributing factor. The physically unsecured systems are also contributing factors to increasing likelihoods of system failures. The missing patches increase failure modes of the software. The keylogger existence in a software is nothing but an information disclosure and an occurrence of an information accident. The unencrypted network protocol means a lack of a mitigation system. Poorly defined procedures either increase human error types or their occurrence likelihoods. The stolen credential is similar to a stolen password and can be viewed as an accident or an initiating event.

E. Qualitative and Quantitative Impacts and Likelihoods

The impact is defined as the overall business loss expected when a threat exploits a vulnerability against an information asset[17]. There are three qualitative levels of potential impact[16].

1) Low: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. An example is a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced.

2) Moderate: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. An example is a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced.

3) High: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or

individuals. An example is a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions.

As shown in Table1, the nuclear PRA yields quantitative or qualitative rankings of core damage severities. Qualitative likelihoods (low, medium, high) are considered in the information security [15]. The risk is defined as a combination of the likelihood of an accident and its impact. A likelihood-impact matrix is used to depict various levels of risks.

F. Safeguards and Mitigation Systems

A safeguard is defined as a risk-reducing measure that acts to detect, prevent, or minimize loss associated with the occurrence of a specified threat or category of threats. Synonyms include control, countermeasure, protection strategy and mitigation plan[18].

1) Administrative workforce controls.

2) Operational and technical controls. This includes a) identity and access management such as authorization and authentification, b) access control, c) systems and application security such as backup and retention, d) network security such as firewalls, e) change management, f) audit logs, and g) encryption.

3)] Physical and environmental controls. This includes a) risk mitigation measures for the earthquake, fire or water leakage, b) physical access control, c) device tracking, d) equipment disposition, and e) portable devices and media.

4) Incident response planning and notification procedures.

5) Education and security awareness training.

6) Third-party agreements.

The operational and technical controls and physical and environmental controls have close resemblance to the mitigation systems for the nuclear PRA. The administrative workforce controls form background factors for the performance of mitigation systems. Incident response planning and notification procedures correspond to accident mitigation shown in Figure3. The education and training and third-party agreements yields background factors.

IV. PRA ANALYSIS SAMPLE

In this section, a sample case is discussed; therefore, in regard to the details of PRA, please refer to the literature and our previous study [19,20].

A. A sample case: Firewall

As indicated in Fig 3, Firewall(F/W) is set in order to protect information asset from illegal access. This is a dual system composed of the main F/W, which usually runs, and the standby F/W, which runs when the main F/W is out of order. The break down of the main F/W triggers an alarm, and the operator, who has caught the alarm, switches to the standby F/W.

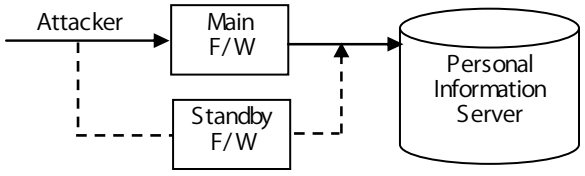

Fig3:Illegal Access and F/W as a mitigation System

B. Generation of an accident scenario with event trees

As illustrated in Fig 4, in PRA, the scenario of accident occurrence is described with a binary tree called Event Tree, and the point where the two branches diverge each other is called Node. The initiating event is written on the left of the scenario. In this case, the initiating event is "the attempt of an illegal access by the attacker," and the F/W responses to this initiating event as a mitigation system. In other words, an initiating event can be defined as the event that requires the response of the mitigation system.

To begin with, while the main F/W is working normally, the illegal access can be prevented, which means the mitigation system is working effectively. This is the Scenario 1 in Fig 4.

Next, let us suppose that the main F/W does not work, i.e., it has broken down. In this case, as has been stated in Section 3.1, an alarm is usually triggered, and the operator detects the abnormality of the main F/W. If the operator is successful in detecting the abnormality, he/she switches to the standby system. The case that the operator succeeded both in detecting the abnormality and in switching to the standby system is Scenario 2 that corresponds to Node 2.

Scenario 2 further diverges into another two branches. In the physical system like a nuclear reactor and a chemical plant, the operator has enough time-allowance for switching to the standby system. Therefore, if the operator has successfully detected the breakdown of the main system and switched to the standby system, the accident can be prevented.

However, in the case of information security, it is possible for the attacker to access during the time slot between the break down of the main system and the time when the standby system begins to work. Thus, Scenario 2 further diverges. In Scenario 2.1, illegal access is prevented because both the detection of the abnormality of the main system and the switching to the standby system are successful. In Scenario 2.2, illegal access is not prevented during the time slot between the breakdown and switching, even though both the detection of the abnormality and switching were successful.

As for the length of the blank time slot in the numerical example that will be stated later in Section 3.4, for the sake of simplicity, it is assumed that it takes 5 minutes to detect the abnormality of the main system and 5 minutes to switch to the standby system; that is, the total length of the blank time slot is 10 minutes. In this example, this time slot length is long enough for the attacker to illegally access because our aim is to explain PRA. Therefore, it goes without saying that depending on the way of access, it can be impossible for the

attacker to access.

Now let us suppose for the sake of simplicity that the inspection cycle of the dual F/W is one month, that the two F/Ws come back to the mint condition after the inspection, and that the initiating event of "the attempt of illegal access by the attacker presents during the half of the one-month inspection cycle.

If the initiating event exists during the blank time slot, illegal access is possible. For example, the occurrence frequency of illegal access per month is 1 % in Scenario 2, the possible access frequency per month in Scenario 2.2 is 0.5 %. Needless to say, in Scenario 2.1, because the standby F/W is normally working, illegal access is prevented despite the presence of the initiating event.

In Scenario 3, the detection of the breakdown of the main system was successful but switching to the standby system failed. In this case, the standby F/W does not work and, as a result, illegal access cannot be prevented. From the viewpoint of maintenance, the situation that illegal access cannot be prevented continues until the next routine inspection. Likewise, in Scenario 4, since the detection of the abnormality of the main F/W has failed, illegal access cannot be prevented until the next routine inspection. In Section 3.4, we will discuss the occurrence frequencies of these scenarios.

C. Analysis of the cause of branching with Fault Tree

The diagram in the lower part of Fig 4 is called Fault Tree that is used for the analysis of the reasons why each Event Tree diverges downwards.

As an example of Fault Tree of the dysfunction of the main F/W, the breakdown of the main F/W itself is a Fault tree on the one hand, which stems from the breakdown of either the hardware or the soft ware, and on the other hand, the mistake in setting the main F/W is also a Fault Tree.

Likewise, as for the cause of the failure of the detection of the breakdown of the main system, the dysfunction of the alarm and the misleading by the operator are the Fault Trees. In addition, as for the cause of the failure of switching to the standby system, erroneous operation and the breakdown of the standby system F/W are the Fault Trees. The latter can be divided into the breakdown of the main F/W itself and the error in setting the main F/W.

The events that are located at the bottom of the Fault Tree are called Basic Events, and in PRA, it is assumed that occurrence frequency and/or occurrence probability can be assigned.

Here, if we assign the numerical values to Basic Events in Fig 4, and if we assume that these events are independent each other, we can approximate the Top Event. For example, let us suppose that the occurrence frequency of the breakdown of the main F/W is 0.0005 times, and that the occurrence frequency of the breakdown of the main F/W that is caused by other reasons than erroneous setting is 0.005 times. Then, it can be approximated that the occurrence frequency of the breakdown of the main F/W is 0.01. Likewise, if it is assumed that the probability of the dysfunction of the alarm under the condition that the main F/W is broken down is 0.01, and that the probability of the erroneous recognition of the alarm by the operator is 0.01, then, it can be approximated that the probability of detection error (so-called Demand Breakdown Probability) is 0.02. Moreover, if it is assumed that the probability of switching failure under the condition that the detection is successful is 0.01, that the probability of the breakdown of the standby F/W caused by the erroneous setting is 0.005, and that the probability of the breakdown of the standby F/W caused by other reasons is 0.005, then it can be approximated that the probability of switching failure after the success of detection is 0.02.

In addition, when the same person set both the main system and the standby system by copying, the dysfunction of the main system means the dysfunction of the standby system, and thereby illegal access cannot be prevented. In this case, the independence of the Basic Events cannot be assumed; therefore, it is necessary to quantify based on the Minimal Cut Set, a failure mode. For example, the pair of the two Basic Events, i.e., the erroneous setting of the main F/W and the dysfunction of the alarm, is a Minimal Cut Set, and is also one of the failure modes of the dual F/W. Therefore, its occurrence frequency can be attained by multiplying the probability or the frequency of the Basic Events. In general, since there exist several Minimal Cut Sets, the scenario is quantified as the total of the occurrence frequency of each Cut Set.

Finally, the probability varies according to the different cases such as when the same person set the main F/W and the standby F/W individually without copying or when different persons set the main system and the standby system; therefore, it is possible to quantify the safety measures even though it is a relative estimation. Likewise, in the case of alarm detection, the scenario can be assumed that either the operator or the automatic switching worked or not.

D. Analysis with concrete numerical numbers

As is indicated in Fig 4, if it is supposed that the breakdown frequency of the main F/W is 0.01 times per month, the probability of the detection failure is 0.02, and the probability of the switching failure after the successful detection is 0.02, the occurrence frequency under the presence of the initiating event is 0.0096, because $0.01\times0.98\times0.98=0.0096$. If this scenario occurs, since it is assumed that it takes 10 minutes to finish switching, the expected value of the time slot is 0.096 minutes, because$0.0096\times10=0.096$.

Here, in order to exemplify, let us suppose that the real initiating event of the illegal access by the attacker occurs during half of the time slot, then by multiplying 0.096 (the expected value) by 0.5 (the probability of the presence of the initiating event), we can gain 0.048 minutes, which is the time length of illegal access per month in scenario 2.2. In other words, it can be estimated that during 0.048 minutes in a given month, illegal access of scenario 2.2 occurs. In order to reduce this time length, reduction of the time necessary for detection and switching can be considered. Likewise, in scenario 3, the occurrence

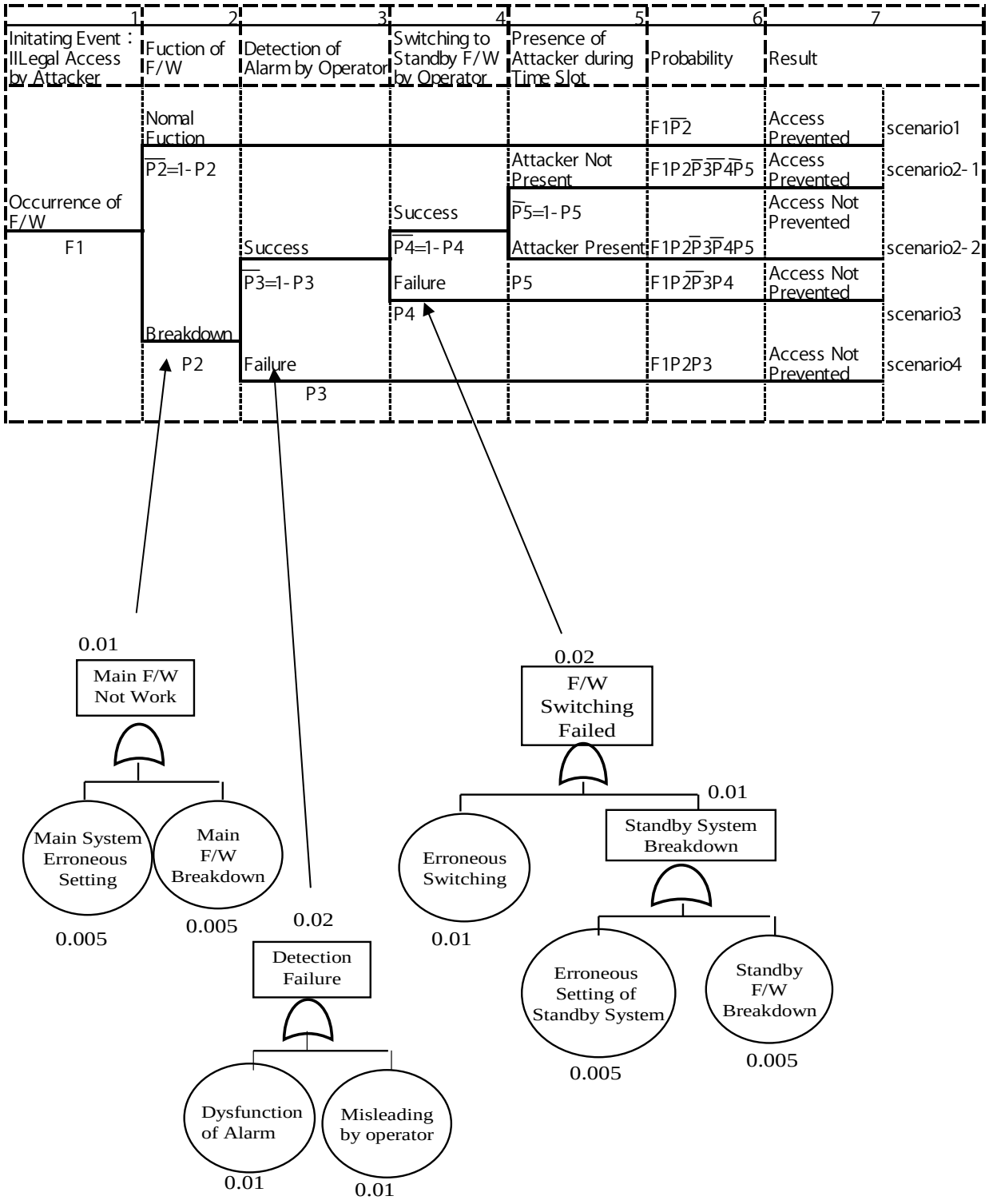

Fig4: Event Tree and Fault Tree of Illegal Access as Initiating Event, F/W example

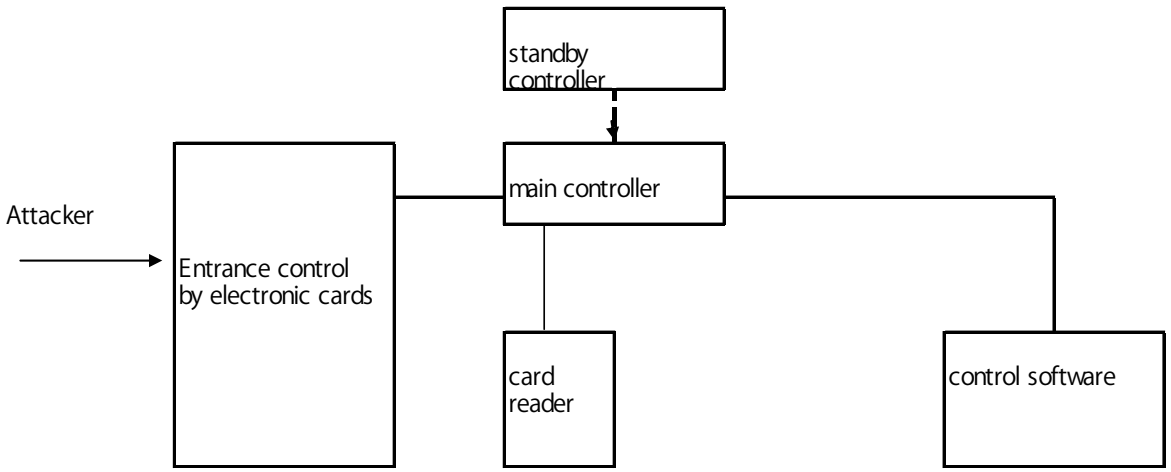

Fig5: Illegal Access and Entrance Control System by Electronic Cards as a Mitigation system

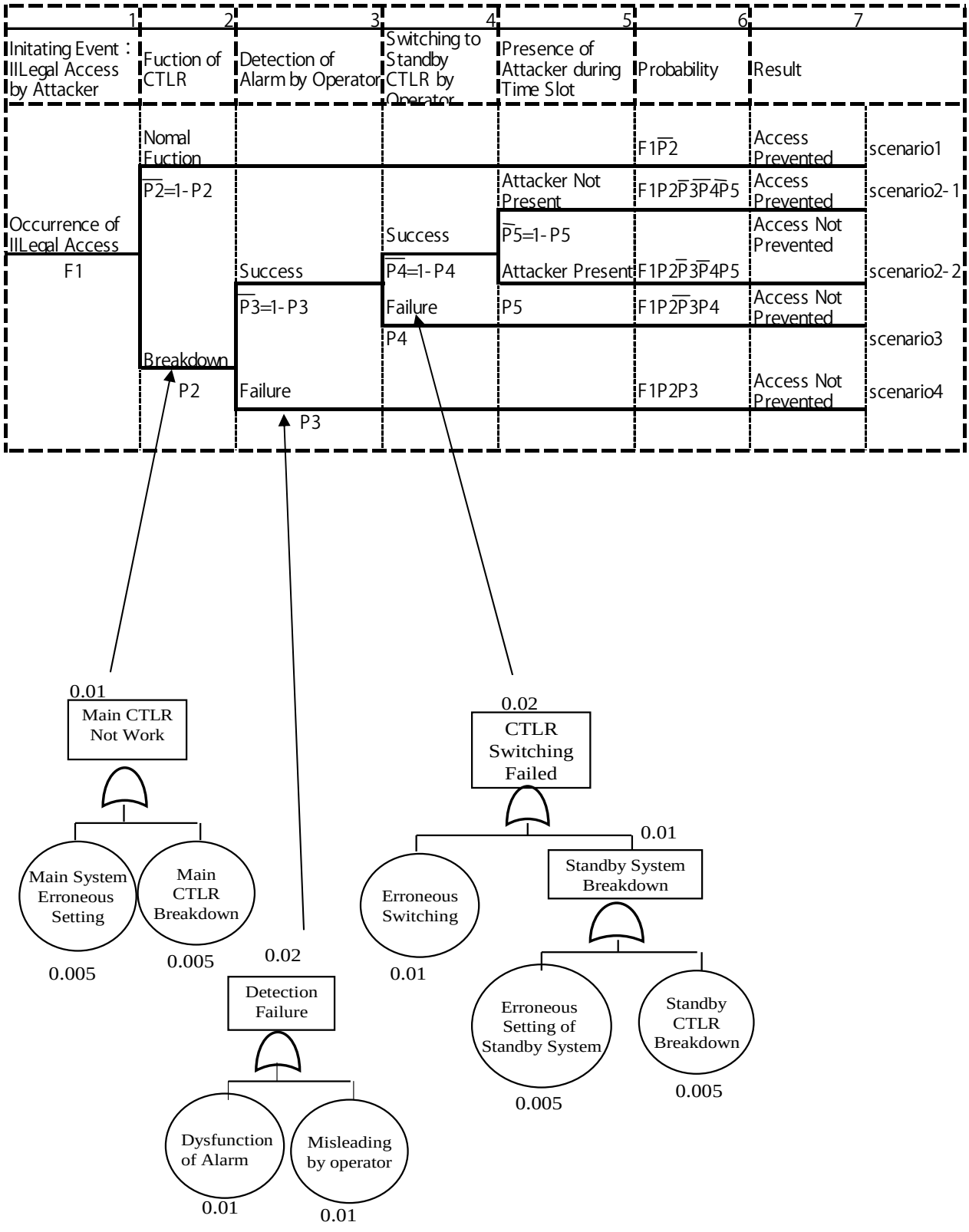

Fig 6 Event Tree and Fault Tree of Illegal Access as Initiating Event, Entrance control

Frequency is 0.000196, because0.01×0.98×0.02=0.000196. Here, for the sake of simplicity, it is assumed that this scenario occurs at the middle point of the inspection period. Then, because during the 15 days or 21600 minutes, which is the time after the inspection, the dual F/W system is open to illegal access, the expected value is 4.23 minutes, because0.000196×21600=4.23. This is example around 44 times longer than that of scenario 2.2. If the real illegal access is done during half of the times when the dual F/W is open to illegal access, the time length of the illegal access can be estimated as 2.11 minutes per month. In order to reduce this time length, the contraction of the routine inspection cycle and the reduction of the probability of switching failure can be considered.

Likewise, n scenario 4, the occurrence frequency is 0.0002, probability can be assigned.

Here, if we assign the numerical values to Basic Events in Fig 4, and if we assume that these events are independent each other, we can approximate the Top Event. For example, let us suppose that the occurrence frequency of the breakdown of the main F/W is 0.0005 times, and that the occurrence frequency of the breakdown of the main F/W that is caused by other reasons than erroneous setting is 0.005 times. Then, it can be approximated that the occurrence frequency of the breakdown of the main F/W is 0.01. Likewise, if it is assumed that the probability of the dysfunction of the alarm under the condition that the main F/W is broken down is 0.01, and that the probability of the erroneous recognition of the alarm by the operator is 0.01, then, it can be approximated that the probability of detection error (so-called Demand Breakdown Probability) is 0.02. Moreover, if it is assumed that the probability of switching failure under the condition that the detection is successful is 0.01, that the probability of the breakdown of the standby F/W caused by the erroneous setting is 0.005, and that the probability of the breakdown of the standby F/W caused by other reasons is 0.005, then it can be approximated that the probability of switching failure after the success of detection is 0.02. *In addition, when the same person set both the main system and the standby system by copying, the dysfunction of the main system means the dysfunction of the standby system, and thereby illegal access cannot be prevented. In this case, the independence of the Basic Events cannot be assumed; therefore, it is necessary to quantify based on the Minimal Cut Set, a failure mode. For example, the pair of the two Basic Events, i.e., the erroneous setting of the main F/W and the dysfunction of the alarm, is a Minimal Cut Set, and is also one of the failure modes of the dual F/W. Therefore, its occurrence frequency can be attained by multiplying the probability or the frequency of the Basic Events. In general, since there exist several Minimal Cut Sets, the scenario is quantified as the total of the occurrence frequency of each Cut Set.*

Finally, the probability varies according to the different cases such as when the same person set the main F/W and the standby F/W individually without copying or when different because 0.01×0.02=0.0002. Here, for the sake of simplicity, it is assumed that this scenario occurs at the middle point of the inspection period. Then, because during the 15 days or 21600 minutes, which is the time after the inspection, the dual F/W system is open to illegal access, the expected value is 4.32 minutes,

Because 0.0002×21600 = 4.32. This is around 45times longer than that of scenario 2.2. If the real illegal access is done during half of the times when the dual F/W is open to illegal access, the time length of the illegal access can be estimated as 2.16 minutes per month. In order to reduce this time length, the contraction of the routine inspection cycle and the reduction of the probability of detection failure can be considered.

V. Physical Access Attacker

Consider an entrance control by electronic cards as indicated in Figure5. A duplicated entrance controller permits entrance for personnel with an authorized card. A main controller, an operator, and a standby controller constitute a mitigation system. The event tree is shown in Figure 6. Note that this tree has the same structure as Figure 4 in spite of the fact that the former deals with physical access, while the latter with network access. This indicates that, once an event tree is constructed, a similar version can be applied to other problems of information security.

VI. Conclusion

In this paper, we have attempted to apply probabilistic risk assessment (PRA), which has been traditionally employed in assessing the risk of physical systems such as a nuclear reactor and a chemical plant, to the area of virtual information security.

In this paper, following the method of PRA, we have attempted to quantify the risk of information asset by describing a scenario based on the responses of the mitigation systems to the initiating event of each Event Tree and Fault Tree. To be concrete, we supposed a case that an illegal access to the dual F/W, described its scenarios, calculated the occurrence probability of each scenario, and calculated the expected value of the time length of the illegal access.

As a result, it has been quantitatively revealed that to what extent the reduction of the time lengths of switching to the standby system, of the inspection, and of the probability of the failure in detecting dysfunctions and switching exerts influence on the expected value.

Acknowledgement

This paper could not have been completed without various useful advices from my project members and party involved. I would like to express my sincere gratitude to these people.

REFERENCES

[1] USNRC: Reactor safety study: An assessment of accident risk in U.S. commercial nuclear power plants. USNRC, WASH-1400, NUREG-75/014 (1975).
[2] G.E. Apostolakis, J.H. Bickel, S. Kaplan: Editorial: Probabilistic risk assessment in the nuclear power utility industry, Reliability Engineering and System Safety, vol. 24, no. 2, 91-94 (1989)
[3] ASME: Standard for probabilistic risk assessment for nuclear power plant applications, ASME RA-S-2002 (2002).
[4] H. Kumamoto, E.J. Henley: Probabilistic risk assessment and management for engineers and scientists, IEEE Press (1996)
[5] H. Kumamoto: Satisfying safety goals by probabilistic risk assessment, Springer (2007).
[6] ISO/IEC TR 13335 (2001).
[7] P.A.S. Ralston, J.H. Graham, J.L. Hieb: Cyber security risk assessment for SCADA and DCS networks, ISA Transactions, vol. 46, 583-594 (2007).
[8] C.J. Alberts, A.J. Dorofee: OCTAVE method implementation guide version 2.0, vol. 17: Appendix C - Complete example results (2001).
[9] B.Schneider: Attack trees, Dr. Dobb's Journal, December (1999)
[10] E.J. Byres, M. Franz, D. Miller: The use of attack trees in assessing vulnerabilities in SCADA systems, International Infrastructure Survivability Workshop, Lisbon, IEEE (2004)
[11] C. Taylor, A. Krings, J. Alves-Foss: Risk analysis and probabilistic survivability assessment (RAPSA): An assessment approach for power substation hardening, Proc. ACM Workshop on Sientific Aspects of Cyber Terrorism, pp.1-9 (2002).
[12] H E Lambert (1991)Case study on the use of PSA methods: Determining safety importance of systems and components at nuclear power plants. IAEA IAEA-TECHDOC-590.
[13] HSE: Five steps to risk assessment.
[14] IS-2 Inventory, Classification, and release of university electronic information, IS Series Information Systems, Business and Finance Bulletin, University of California (2007).
[15] T.R. Peltier: Information security risk analysis, Second Edition, Auerack Publications (2005).
[16] Standards for security categorization of federal information and information systems, National Institute of Standards and Technology, U.S. Department of Commerce (2004).
[17] Microsoft: The security risk management guide (2006).
[18] IS-3 Electronic information security, IS Series Information Systems, Business and Finance Bulletin, University of California (2007).
[19] N. Satoh & H. Kumamoto, Enumeration of initiating events of information security accidents, 2007 International Conference Innovation & Management, pp. 119-124(2007)
[20] N. Satoh & H. Kumamoto, Comparison of ISO GMITS and Probabilistic Risk Assessment in Information Security, 2008 International Conference Innovation & Management, pp. 351-355(2008)
[21] Naoki Satoh and Norihisa Komoda; An Analysis of Influential Factors for the Information Security Audit Labor Time and Regressive Estimation of the Labor Times, WSEAS Trans. on Information Science and Applications, Issue 1, Vol.3, pp.154-161 (2006)
[22] Matsuki Yoshino, Norihisa Komoda, and Michiko Oba: An Analysis of Patterns for Automating Information System Operations,WSEAS Trans. on information science and Application, Issue 11, Vol 5, pp.1618-1627 (2008)
[23] N. Satoh & H. Kumamoto,Viewpoint of ISO GMITS and Probabilistic Risk Assessment in information Security, WSEAS Trans on information science and Application, issue 4 , Vol.2, pp237-244(2008)

First A. Author (M'76–SM'81–F'87) and the other authors may include biographies at the end of regular papers. Biographies are often not included in conference-related papers. This author became a Member (M) of **NAUN** in 1976, a Senior Member (SM) in 1981, and a Fellow (F) in 1987. The first paragraph may contain a place and/or date of birth (list place, then date). Next, the author's educational background is listed. The degrees should be listed with type of degree in what field, which institution, city, state or country, and year degree was earned. The author's major field of study should be lower-cased.

The second paragraph uses the pronoun of the person (he or she) and not the author's last name. It lists military and work experience, including summer and fellowship jobs. Job titles are capitalized. The current job must have a location; previous positions may be listed without one. Information concerning previous publications may be included. Try not to list more than three books or published articles. The format for listing publishers of a book within the biography is: title of book (city, state: publisher name, year) similar to a reference. Current and previous research interests ends the paragraph.

The third paragraph begins with the author's title and last name (e.g., Dr. Smith, Prof. Jones, Mr. Kajor, Ms. Hunter). List any memberships in professional societies other than the **NAUN**. Finally, list any awards and work for **NAUN** committees and publications. If a photograph is provided, the biography will be indented around it. The photograph is placed at the top left of the biography. Personal hobbies will be deleted from the biography.