The Nucleus, **46** (4) 2009 : 415-428

The Nucleus
A Quarterly Scientific Journal of Pakistan
Atomic Energy Commission

NCLEAM, ISSN 0029-5698

ATTACK TREE BASED CYBER SECURITY ANALYSIS OF NUCLEAR DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

P. A. KHAND

Theoretical Plasma Physics Division, PINSTECH, P.O. Nilore Islamabad, Pakistan.

(Received April 20, 2009 and accepted in revised form October 02, 2009)

To maintain the cyber security, nuclear digital Instrumentation and Control (I&C) systems must be analyzed for security risks because a single security breach due to a cyber attack can cause system failure, which can have catastrophic consequences on the environment and staff of a Nuclear Power Plant (NPP). Attack trees have been widely used to analyze the cyber security of digital systems due to their ability to capture system specific as well as attacker specific details. Therefore, a methodology based on attack trees has been proposed to analyze the cyber security of the systems. The methodology has been applied for the Cyber Security Analysis (CSA) of a Bistable Processor (BP) of a Reactor Protection System (RPS). Threats have been described according to their source. Attack scenarios have been generated using the attack tree and possible counter measures according to the Security Risk Level (SRL) of each scenario have been suggested. Moreover, cyber Security Requirements (SRs) have been elicited, and suitability of the requirements has been checked.

Keywords: Attack tree, Cyber security, Digital instrumentation and control systems, Threat, Vulnerability

1. Introduction

Instrumentation and control (I&C) systems are the heart of most industrial plant operations. I&C systems are used for monitoring, control, and protection of process components in Nuclear Power Plants (NPPs) [1]. In the past, the security of nuclear I&C systems consisted of limiting access to authorized plant staff using administrative procedures, securing physical access to consoles, and by isolating them from other networks. Unfortunately, nuclear I&C systems utilized today still rely on those techniques. Clearly, this approach no longer works, as design trends of nuclear I&C systems have been changed. Analogue technology based systems are being replaced with digital technology as it provides many improved advantages. Systems are highly interconnected to convey the flow of information amongst different components of the plant for economic benefits. In modern plants, plant sensor data is acquired through remote multiplexers and provided to the control and safety systems, which in turn, send the data to monitoring systems through the gateways, where the data is stored, processed and analyzed and displayed. The on-site technical support centres and emergency operations facilities can retrieve and see the trends of the data, for monitoring plant conditions, through data links from the monitoring systems. Moreover, equipment failures can be detected online and diagnostic tests performed to know the cause; consequently, on-line maintenance, and repair is possible. Hence, the interconnectivity can contribute to better plant operation, maintenance, management of resources and future planning. Furthermore, the tendency in the nuclear industry over the past ten years has been in use of technologies by commercial vendors [2,3]. Commercial-off-the-shelf (COTS) products allow end user to choose simply from a myriad of suppliers (or among the best technologies), to minimize complexity of maintenance, and reduce costs. However, those products use open protocols and operating systems. The information about those can be easily available, which makes them vulnerable to a host of cyber attacks. New cyber security problems can arise due to the new trends such as on January 25, 2003, infection of Ohio’s Davis-Besse NPP with a MS SQL 2000 worm [4], named as slammer [5].

CSA means to analyze digital systems for

[*] Corresponding author: parvaiz_123@yahoo.com

unauthorized access, use, disclosure, disruption, modification, or destruction. CSA can help in analyzing and finding the solutions for the security problems and eliciting cyber SRs. CSA of digital I&C systems should be performed to identify the vulnerabilities, threats that can exploit the vulnerabilities, to select suitable technical and managerial controls and to elicit cyber SRs.

Several methodologies for quantitative analysis of cyber security such as probabilistic quantification methodology [6], methodologies for SITAR system [7, 8], Information Security Risk Analysis Method (ISRAM) [9], Cost-of-Risk Analysis (CORA) [10], a cyber security assessment approach for power industry [11] and an attack tree based methodology for distributed systems [12] have been proposed. The quantitative methods can provide numerical values for cyber security risks. However, to use the quantitative methods, qualitative analysis must precede them – cyber security risks and their causal factors must be identified before the numerical values can be assigned to them. Thus, the quality of the quantitative analysis depends on how good the qualitative one was [13].

For qualitative CSA, many methodologies can be found. Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) [14] evaluate the cyber security at organizational level and provide an organizational wide view of cyber security risks and a baseline for improvement. Nuclear digital I&C systems such as protection systems, process control systems, process computing systems and administrative computer systems have different security levels [15]. Evaluation of cyber security at organizational level will be very difficult to perform and may not be suitable. A model-based risk assessment approach for security critical systems (named as CORAS [16]) requires building a profile based on several Unified Modelling Language (UML) diagrams for different aspects of system. That profile is then evaluated by conducting various workshops and discussions with different people. However, to apply CORAS for the CSA of nuclear digital I&C systems a lot of time and effort are required as the available system specification documentation may not contain UML diagrams and the evaluation will not be easy. Control Objective for Information and related Technology (COBIT) [17] and other methodologies [18-20] were built mainly for analyzing and securing the business IT systems. They consider building security in systems without considering the details about the threat sources. Security and performance requirements and operational environment of nuclear I&C systems are different from that of business IT systems [21]; therefore, the use of these methodologies to analyze the cyber security of nuclear digital I&C systems may not be appropriate. Some attempts have also been made to use attack trees for the CSA of critical systems [22,23]. However, those approaches lack the methods for threat analysis, security risk assessment and mitigation.

The remainder of this paper is organized as follows: In section 2, description of the methodology is given. Then, section 3 contains a case study and detailed discussion about the application of methodology. Finally, in section 4, conclusion and further work is presented.

2. The Methodology

Bruce Schneier [24] introduced the attack trees to model the security of a system by considering a security breach as an attack goal, and describing it with a set of events that lead to the goal in a combinatorial way. Attack trees help us to understand the ways in which the attackers can engineer the attack and reach the attack goal. The attack tree based CSA can help to find out the root causes of compromises to systems. The main flow of the methodology is shown in Figure 1. The detailed description of each step is given in the following subsections.

2.1 Preparation

This step involves arrangement of system documentation, security evaluation criteria, and a schedule. The system documentation includes system specifications and plant network diagrams. The security evaluation criterion helps to determine the threat levels of cyber threats and SRL of each cyber security risk. The schedule is a plan to carry out the CSA. It clearly describes when a particular step will start and when it will be completed.

2.2 System identification

System and its operational environment are to be identified using system documentation. System specifications and plant network diagrams helps to identify the following: (i) components of the system and their functions; (ii) interactions between the components of the system; (iii) interactions of the system with other systems; (iv) users and management of the system; (v) interactions of plant Local Area Network (LAN) with other networks; and (vi) security mechanisms placed to secure the system.

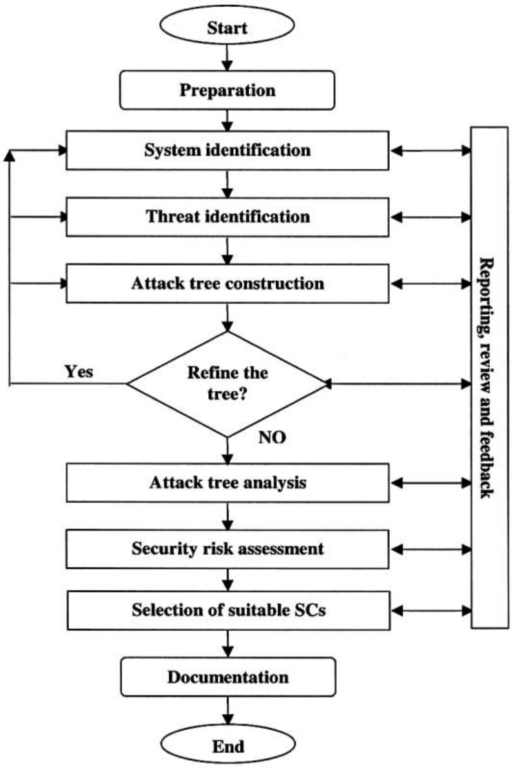


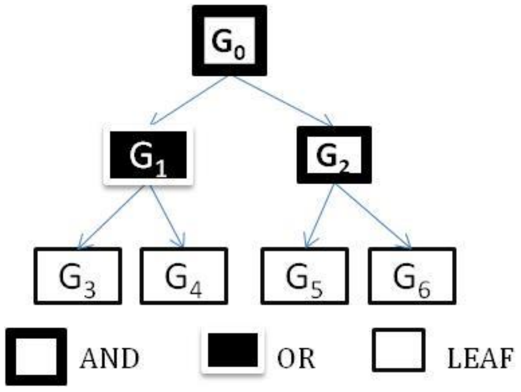
Figure 1. Main flow of the methodology.

2.3 *Threats identification*

The purpose of this step is to identify vulnerabilities and threats. Vulnerabilities present in the system and its entry points (section 2.2) can be identified by using existing information about vulnerabilities of those systems such as vulnerability databases [25-31] and the documentation of the operating experiences [32, 33]. Special attention should be given to determine how access to the entry points is controlled and who have what privileges (user access capabilities) to access the system. Consideration of threats to NPP digital I&C systems include threats from insiders and outsiders [34]. An outsider is a person who is not authorized to use a digital system - i.e., they do not have the assigned privileges. Threat sources (potential attackers) [35] can pose threats to the system by exploiting the vulnerabilities and disrupt the system. Threat sources and types of threats they can pose should be enlisted.

2.4 *Attack tree construction*

The construction of an attack tree starts with the identification of the attack goal. A successful security breach due to a cyber attack is called an attack goal. Successive subordinate security breaches are called attack sub goals. The sub goals can be broken down further to successive events called atomic attacks. The attack goal, sub-goals, and atomic attack are linked together by using logical connective functions and hence a tree structure is created. The synthesis of the tree is described graphically using connective symbols (AND, OR). The node that represents the attack goal is called root node. When an attack sub goal is broken down further, the corresponding node is called a non-leaf node. In case, when an attack sub goal cannot be divided further, or when it is decided to limit the analysis further, the corresponding branch is terminated with a leaf node. A leaf node can cause a root node or it can contribute to occurrence of a non-leaf node. An example of the attack tree, with root node G_0, non-leaf nodes G_1 and G_2, and leaf nodes G_3, G_4, G_5, and G_6, is shown in Figure 2. The basic feature of attack trees is their hierarchical structure: the model is constructed in top-down manner from the higher-level events to the leaf events (Root node → Connective Symbols (non-leaf nodes) → Leaf events). The process of attack tree construction starts from the root node and proceeds to leaf events. Each attack event at the lower level of attack tree is considered in terms of its effects on



G_0 Disrupt System
G_1 Disrupt Software
G_2 Defeat Intrusion detection System
G_3 Disrupt Operating System
G_4 Disrupt Application Software
G_5 Defeat Network Intrusion Detection System
G_6 Defeat Host Intrusion Detection System

Figure 2. An example of attack tree.

the root node or the events at the next level of the attack tree hierarchy. The best attack tree can be constructed by considering how a threat source with infinite capabilities can use atomic attacks to exploit the vulnerabilities for reaching the sub-goals and ultimately the attack goal [36].

Table 1. Classification of possibility levels.

PLs	*Description*
P_1	Highly likely (The highest possibility) of occurrence. The vulnerability can easily be known from literature and the existence of threat is known.
P_2	Likely to occur.
P_3	Unlikely to occur.
P_4	Highly unlikely to occur.
P_5	No possibility of occurrence. The threat or the vulnerability exists only in theory.

Table 2. Classification of consequence levels.

CLs	*Description*
C_1	Catastrophic effect on the environment and plant staff.
C_2	Major effect on the reliability and availability of system.
C_3	Moderate effect on the reliability and availability of system. Severe effect to the integrity of the system.
C_4	Minor effect on the reliability, availability and integrity of the system but confidentiality is severely violated.
C_5	No effect on the reliability, availability and integrity of the system, only confidentiality is violated

Table 3. Classification of security risk levels.

PL/CL	C_1	C_2	C_3	C_4	C_5
P_1	SL_1	SL_1	SL_2	SL_2	SL_3
P_2	SL_1	SL_2	SL_2	SL_3	SL_4
P_3	SL_2	SL_2	SL_3	SL_4	SL_4
P_4	SL_2	SL_3	SL_4	SL_4	SL_5
P_5	SL_3	SL_4	SL_4	SL_5	SL_5

2.5 *Decision for refinement*

The analyst(s) decides whether there is need for further refinement of the tree or not. The basis for this decision should be to check whether all identified threats have been addressed in the tree. If the decision is made to refine the tree further then the analyst(s) can go to any of the system identification, threats identification, or attack tree construction steps depending upon the need of the analysis.

2.6 *Attack tree analysis*

All possible attack scenarios should be generated from the attack tree and SRLs of the root node and attack scenarios should be determined in this step. An attack scenario is a minimum combination of leaf nodes that are necessary to achieve the root node [35]. SRL represents the qualitative value of the risk due to a threat. The SRL of the root node can be obtained by determining SRLs of leaf nodes, and then calculating SRLs for non-leaf nodes upto the root node in bottom-up manner. The SRL of a leaf node is the combination of attack Possibility Level (PL) and Consequence Level (CL). The attack PL for the “AND” node is the minimum of the PLs of its children, where for the “OR” node it is the maximum of the PLs of its children. CL of the attack for a given non-leaf node is taken as the maximum of the CLs of its children. The SRL of a given attack tree node is determined by the combination of its attack PLs and CLs. We have described the PLs, CLs, and SRLs according to guidelines given in [37-39]. The PLs, CLs, and SRLs are shown in Tables 1 to 3 respectively. The combination of attack PLs and CLs is determined by the SRL classification matrix (Table 3). SL_1, SL_2, SL_3, SL_4, and SL_5 represent the SRLs as extreme, very high, high, moderate, and low respectively. The SRL of an attack scenario is the maximum of the SRLs of its contributing leaf nodes. When many experts develop an attack tree, the small trees can be analyzed separately and then results of the analysis for higher-level tree can be obtained by combining the results of analysis of small trees in bottom-up manner [36].

2.7 *Cyber security risk assessment*

The security of a system is assessed according to its SRL. The SRL of the root node of the attack tree represents the SRL of a system. The SRL of a system must not be above the Desired Risk Level (DRL). Typically, the owners of a system describe the DRL. If the SRL is above the DRL then the attack scenarios with SRL above the DRL are selected. All possible Security Controls (SCs) are enlisted for each scenario. Some of the recommended SCs for the digital systems used in various industries can be found in [40-43]. SCs are the management, operational and technical controls (i.e., safeguards or counter measures) prescribed for a digital system to protect its security [40]. The technical controls are primarily implemented and executed by the digital system through mechanisms contained in the hardware, software, or firmware components of system [40]. The management controls for a digital system focus on the management of risk and the management of digital system security [40]. However, the selection of the suitable SCs should be done after evaluating their effectiveness to reduce the SRL of the scenarios to the DRL using the procedure described in the following section. The selected SCs can be used to elicit SRs. The SRs are required for the design and evaluation of different security aspects of computer systems. SRs will help to develop a Cyber Security Policy (CSP) [44]. The CSP includes control of access of software functions, use of system services, data communication links, and a list of personnel who may access or use the system [45]. Typically, the CSP is divided into two parts: the administrative and other non-technical procedures and the technical measures (routines, and procedures) [44]. A procedure described in the next section should be used to check whether the elicited SRs would actually address the identified threats.

2.8 Selection of suitable security controls

A method has been described (Figure 3) to determine the effectiveness of the SCs to reduce the SRL of a scenario to a DRL. The method was described for attack scenarios instead of leaf nodes due to fact that same atomic attacks can be used in a different attack scenario; therefore, SCs required for a leaf node might differ for a particular scenario. Moreover, the method is an improvement of the method for "modelling the addition of security controls in an attack model" [46].

First three steps of the method are very similar to ones that have been described in the sections 2.4, 2.6 and 2.7. Therefore, to use the method in this step it should be followed from the fourth step. In the method, the introduction of a node for a SC that forms a sibling to the attack tree node under an "AND" node can be justified by the fact that the attacker has to launch the attack(s) for exploiting the SC in addition to the attack(s) represented by that node. The list of possible SCs for the scenarios prepared during the "cyber security risk assessment" step should be used for the selection of suitable SCs. The risk analysis and assessment procedures in the method are very similar to ones that have been described in the sections 2.4, 2.6 and 2.7. However, it has been added in this method because it would be easier to analyze and assess a small portion of the tree for a particular scenario instead of analyzing and assessing the whole tree for all scenarios. Moreover, it would also be easier to determine the change in the SRL of the root node by using the procedure described in the section 2.7. A list of suitable SCs for each scenario should be prepared after the evaluation.

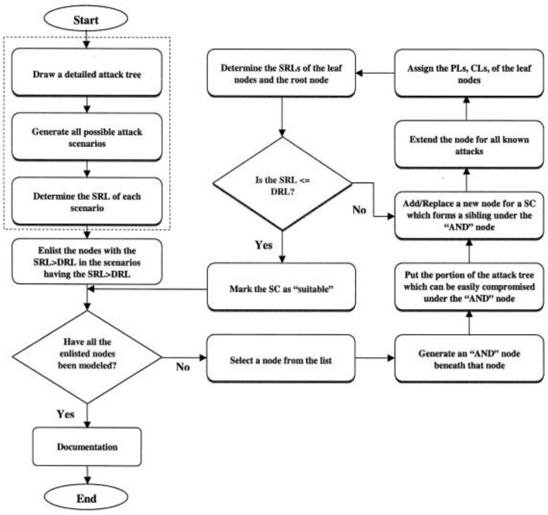

Start
Draw a detailed attack tree
Generate all possible attack scenarios
Determine the SRL of each scenario
Enlist the nodes with the SRL>DRL in the scenarios having the SRL>DRL
Have all the enlisted nodes been modeled?
Yes
Documentation
End
No
Select a node from the list
Generate an "AND" node beneath that node
Put the portion of the attack tree which can be easily compromised under the "AND" node
Add/Replace a new node for a SC which forms a sibling under the "AND" node
Extend the node for all known attacks
Assign the PLs, CLs, of the leaf nodes
Determine the SRLs of the leaf nodes and the root node
Is the SRL <= DRL?
No
Yes
Mark the SC as "suitable"

Figure 3. Evaluation method for security controls.

An example to demonstrate the usefulness of the method (Figure 3) is presented here. Consider the attack tree in Figure 2 with P_2, P_4, P_3 and P_3, and C_3, C_2, C_2 and C_3 as the PLs and CLs for its leaf nodes G_3, G_4, G_5, and G_6 respectively. The SRL for the root node comes out to be SL_3 after determining the SRLs of leaf nodes using Table 3 and then propagating the leaf node values upto the root node in a bottom-up manner. Assume that the DRL must not be above the SL_4. Two attack scenarios <G_3, G_5, G_6> and <G_4, G_5, G_6> have the SRL above the DRL (each has the SRL SL_2). The node G_3 has the highest SRL (SL_2) in the first scenario. Suppose there are four SCs: SC_1, SC_2, SC_3, and SC_4 available to bring the SRL of the node down. In order to bring the SRL of the node down to the DRL, we replaced the leaf node with an "AND" node (named it G_3) and then put two siblings G_7 and G_8 under it: one for the old leaf node and the other for the SC_2. Suppose SC_2 is "malicious code (e.g., viruses, worms, and logic bombs) detection and handling system" and G_8 will represent the attack to disrupt the SC_2. The

SRLs for G_7, G_8, and G_3 were determined as SL_2, SL_4, and SL_4 respectively and consequently the SRL of the root node found out as SL_4; therefore, SC_2 is selected. Similarly, other SCs and the scenario can be evaluated.

2.9 Reporting, review and feedback

This step refers to an ongoing activity that examines the analysis process during different steps. A report about the results of the analysis should be generated at the completion of each step. The report should be sent to the reviewer(s) for verifying the results of the analysis and for finding something left during the analysis. The results of review should be feedback to the analyst(s) before the start of the next step so that any modifications suggested in the analysis is carried out in a timely manner.

In addition, if the SRs are elicited then their suitability to address the known threats can be checked by using the following procedure [35, 47]. First, the atomic attacks (leaf nodes) should be related with the known threats. Then the relationships between the threats and Security Objectives (SOs), and the SOs and SRs should be found. Furthermore, the results of analysis should be documented for future use. The documents should contain the following items: (i) the list of system components, their functions and tasks, and method, mode and frequency of communication; (ii) the list of entry points to the system; (iii) the list of threats for each identified threat sources; (iv) the detailed attack tree; (v) the list of attack scenarios; (vi) the SRLs of the leaf nodes, attack scenarios, and root node; (vii) the list of selected SCs; and (viii) the list of SRs.

3. Case Study

The methodology has been applied to analyze the cyber security of a BP in the channel No. 1 of RPS (RPS_BP1). The stepwise application of the methodology is given below.

3.1 System identification

The RPS is the part of the Digital Plant Protection System (DPPS) which uses fully digitalized I&C technology. The DPPS has four redundant channels and three sub systems: RPS, Safety Actuation System (SAS), and Local Testing Processor (LTP). Four redundant sets of DPPS cabinets are located in a separate I&C equipment room. Each cabinet contains signal conditioning and processing equipment, BP, Coincidence Processors (CPs), LTP, Local Testing and Maintenance Panel (TMP), Processor based gateways and other hardware for the interface with other DPPS channels. RPS uses trip logic to protect the core fuel design limits and Reactor Coolant System (RCS) pressure boundary for Anticipated Operational Occurrences (AOO) [48] and to provide assistance in mitigating the consequences of accidents. The SAS has similar features to the RPS, used to reduce the influence of other reactor accidents. The LTP used for manual and/or automatic surveillance testing based on user's input via a Human-Machine Interface (HMI) for testing called as TMP and DPPS status monitoring [49-51]. The RPS architecture consists of four redundant channels and each channel has two redundant BPs and four CPs [49]. The architecture of the one channel of the RPS is shown in Figure 3. BP design integrates various system components, features, and functions into a microprocessor-based unit. The BP sends the bistable trip outputs to the associated cross channel communications. Isolated fiber optic links transfer the bistable trip states to CPs in other channels. Software ensures predictable system performance and response under all conditions. It consists of Operating System (OS) and application software. RPS has interfaces to other systems for operator interaction, alarm annunciation and manual and automatic testing. Processor based gateways are used for data communication to the monitoring systems. Operator Panel (OP) is located in Main Control Room (MCR) and is used for entering constants, trip channel bypass, operating bypass and variable set point reset. TMP is a man-machine interface for testing and is used for manual testing of bistable trip functions, trip channel bypasses, operating bypasses and variable set point resets. Control of access for the RPS include the following: (i) system software is protected against unauthorized alterations by administrative controls; (ii) access for changing set points and bypasses is also restricted by the door key lock; (iii) access to workstations is administratively or password controlled; and (iv) RPS cabinet doors are locked and equipped with "door open" alarms [49-50].

Table 4. Summary of cyber security risk assessment results.

No.	Threats	Threat Source	Attack Scenarios	SRL	Suitable SCs
1.	Corrupt Operating software	Digruntled plant insider	$<G_{q+1}>$	SL_5	Security awareness, Security operating procedures
2.			$<G_{q+2}>$	SL_5	(1) + Security training, limiting access to absolute minimum
3.			$<G_{s+1}, G_{s+4}, G_{t+1}, G_{t+2}>$	SL_4	(1) + Limiting access, Secret coding of door keys, safety locks for cabinets
4.			$<G_{s+2}, G_{s+4}, G_{t+1}, G_{t+2}>$	SL_4	(2) + (3)
5.			$<G_{q+5}, G_{s+1}, G_{s+4}, G_{t+1}, G_{t+2}>$	SL_3	(3) + Malicious code detection and handling, biometrics based authentication
6.			$<G_{q+5}, G_{s+2}, G_{s+4}, G_{t+1}, G_{t+2}>$	SL_3	(4) + (5)
7.			$<G_{q+6}, G_{s+1}, G_{s+4}, G_{t+1}, G_{t+2}>$	SL_4	(6) + control removable media
8.			$<G_{q+6}, G_{s+2}, G_{s+4}, G_{t+1}, G_{t+2}>$	SL_4	(7) + two-person rule
9.		Corporate employee	$< G_{r+3}, G_{r+4}, G_{r+5}>$	SL_4	Network IDS
10.		Maintainer	$< G_{q+5}>$	SL_3	Approved and qualified person for maintenance, Malicious code detection and handling
11.			$< G_{q+6}>$	SL_4	(10) + control removable media
12.	Corrupt Application module	Digruntled plant insider	$<G_{q+1}>$	SL_5	Same as (1)
13.			$<G_{q+2}>$	SL_5	Same as (2)
14.			$<G_{s+1}, G_{s+4}, G_{t+1}, G_{t+2}>$	SL_4	Same as (3)
15.			$<G_{s+2}, G_{s+4}, G_{t+1}, G_{t+2}>$	SL_4	Same as (4)
16.			$<G_{q+5}, G_{s+1}, G_{s+4}, G_{t+1}, G_{t+2}>$	SL_3	Same as (5)
17.			$<G_{q+5}, G_{s+2}, G_{s+4}, G_{t+1}, G_{t+2}>$	SL_3	Same as (6)
18.			$<G_{q+6}, G_{s+1}, G_{s+4}, G_{t+1}, G_{t+2}>$	SL_4	Same as (7)
19.			$<G_{q+6}, G_{s+2}, G_{s+4}, G_{t+1}, G_{t+2}>$	SL_4	Same as (8)
20.			$<G'_{q+1}>$	SL_5	Same as (1)
21.			$<G'_{q+2}>$	SL_5	Same as (2)
22.			$<G'_{s+1}, G'_{s+4}, G'_{t+1}, G'_{t+2}>$	SL_4	Same as (3)
23.			$<G'_{s+2}, G'_{s+4}, G'_{t+1}, G'_{t+2}>$	SL_4	Same as (4)
24.		Corporate employee	$< G_{r+3}, G_{r+4}, G_{r+5}>$	SL_4	Same as (9)
25.		Maintainer	$< G_{q+5}>$	SL_3	Same as (10)
26.			$< G_{q+6}>$	SL_4	Same as (11)
27.	Disable/ damage network cables	Digruntled plant insider	$<G_{s+1}, G_{s+4}, G_{t+1}, G_{t+2}, G_{12}>$	SL_4	Same as (3)
28.			$<G_{s+2}, G_{s+4}, G_{t+1}, G_{t+2}, G_{12}>$	SL_4	Same as (4)
29.	Disable/ damage hardware	Digruntled plant insider	$<G_{s+1}, G_{s+4}, G_{t+1}, G_{t+2}, G_{v+1}>$	SL_4	Same as (3)
30.			$<G_{s+2}, G_{s+4}, G_{t+1}, G_{t+2}, G_{v+1}>$	SL_4	Same as (4)
31.			$<G_{s+1}, G_{s+4}, G_{t+1}, G_{t+2}, G_{v+2}>$	SL_3	Same as (5)
32.			$<G_{s+2}, G_{s+4}, G_{t+1}, G_{t+2}, G_{v+2}>$	SL_3	Same as (5)
33.		Maintainer	$< G_{v+2}>$	SL_4	Same as (11)

Interactions between the BP and the other main components of the system and with the other systems are shown in Figure 4 [49]. BP gets data of plant processes from sensors and transducers through the signal conditioning and processing equipment cabinet and the core protection calculation system. BP sends bistable trip outputs to the associated cross channel communications. Isolated fiber optic links transfer the bistable trip states to CPs in other channels. BP exchange information within a channel over a data communication network with OP and TMP through the LTP, and with the monitoring systems through the gateway. Hence, BP has interfaces for following functions: (i) operator interaction with OP and TMP; (ii) alarm annunciation with OP, TMP, and the monitoring systems; and (iii) manual and automatic testing with OP and TMP through LTP. Moreover, the plant network is isolated from outside world, no remote access is allowed and the physical access control of the plant is tightly controlled [49, 51].

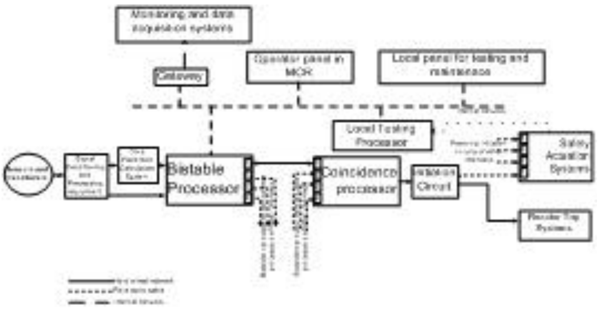


Figure 4. A generic architecture of the reactor protection system channel No. 1.

3.2 Threats identification

Threats that can exploit the vulnerabilities are identified and classified according to their threat source in Table 4. Threat sources are insiders or outsiders in collusion with the insiders. However, there is no possibility of an outsider threat. The threat sources include disgruntled plant insiders (operators and administrators), employees in the corporate network (on-site technical support and emergency facilities), and maintainers. Disgruntled employee has a malicious intent and they can pose a threat to the system individually or in collusion with malicious outsider(s). They can violate the security procedures, get access to restricted areas, use social engineering to get confidential information and disrupt the software and hardware. Social engineering relies on lies and seduction that can trick plant staff into disclosing confidential information or facilitating a cyber attack. Maintainer can pose a threat by installing the update or patch containing malicious code either for BP software or BP hardware firmware or for both. They can do so either due to the malicious intent or due to careless behaviour. They can be in collusion with malicious outsider(s) and arrange a media for software update containing the malicious code. There are two possibilities due to their careless behaviour, first they can be victim of social engineering by an insider or outsider and use a media for software update that contains malicious code. Second, they download the software and copies it to a media that contain malicious software. The consequences of malicious code installation on the system can be severe. It can disrupt the BP software, it can block the data transmission lines, or it can corrupt the firmware. Hence, it can severely affect the availability and reliability of the system. The malicious corporate employee can get access to the system from the associated data link from the plant network.

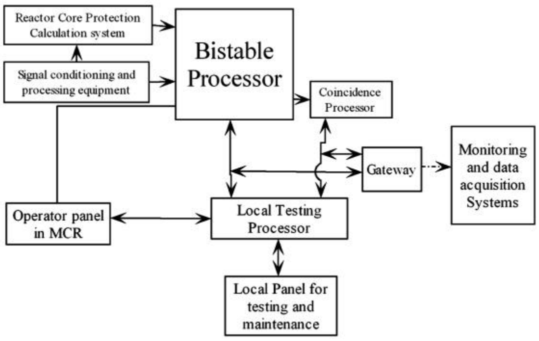
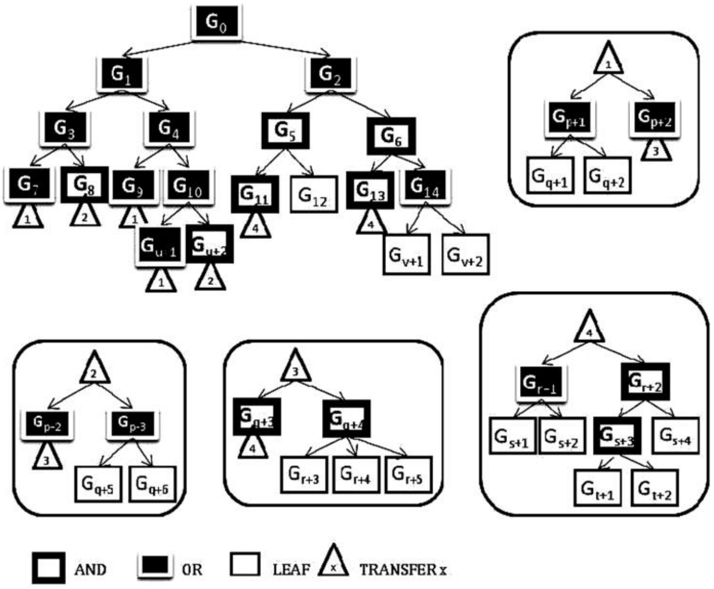

Reactor Core Protection Calculation system
Signal conditioning and processing equipment
Bistable Processor
Coincidence Processor
Gateway
Monitoring and data acquisition Systems
Operator panel in MCR
Local Testing Processor
Local Panel for testing and maintenance

Figure 5. Interaction of the bistable processor of the reactor protection system with other components and systems.

3.3 Attack tree construction

An attack tree for RPS_BP1 is shown in Figure 6. It represents how the attackers can launch atomic attacks by exploiting the vulnerabilities present in a system and its operational environment to reach the attack goal “disrupt the RPS_BP1”. We constructed the tree by first identifying the attack goal, sub-goals and then broken down the successive sub-goals to atomic attacks and connecting them with connective nodes (AND/OR). We constructed the attack tree by considering the attacker point of view—i.e., how an attacker, with infinite resources, knowledge and motivation, can breach the entry points to RPS_BP1 and disrupt it.

We found that the construction of the tree without any tool support is tedious. However, the use of transfers for the similar portions of the attack tees reduces the complexity of tree and the construction process becomes simple. Moreover, we also found that the existing numbering schemes such as in [36] are very difficult to apply. The left to right rule (from the top) was followed while numbering the subscripts in the nodes—i.e.,



G_0	Disrupt RPS_BP1
G_1	Disrupt Software
G_2	Disrupt Hardware
G_3	Disrupt the Operating System
G_4	Disrupt the Application Program
G_5	Disrupt Cables
G_6	Disrupt BP Hardware
G_7	Send spurious commands
G_8	Install malicious code
G_9	Change Set points
G_{10}	Corrupt Application Program Module
G_{11}	Get access to DPPS cabinet
G_{12}	Use Special equipment to damage cables
G_{13}	Get access to DPPS cabinet
G_{14}	Use Special equipment to damage BP hardware
G_{u+1}	Send Spurious Commands to corrupt application module
G_{u+2}	Install malicious Code to corrupt application module
G_{v+1}	Use special hardware to disrupt BP hardware
G_{v+2}	Install the firmware update containing the malicious code through TMP
G_{p+1}:	Get access to OP
G_{p+2}:	Get access to TMP

G_{p+3}: Arrange software update

G_{q+1}: Masquerade to get access inside MCR

G_{q+2}: Bribe plant operator

G_{q+3}: Get access to DPPS cabinet

G_{q+4}: Get access to local network

G_{q+5}: Download the software update containing the malicious code

G_{q+6}: Get the software update from a third party containing the malicious code

G_{r+1}: Go unobserved to I&C equipment room

G_{r+2}: Get access to I&C equipment room

G_{r+3}: Get access to business network

G_{r+4}: Get access to monitoring system

G_{r+5}: Disrupt gateway

G_{s+1}: Masquerade

G_{s+2}: Bribe security personnel

G_{s+3}: Open I&C equipment room door

G_{s+4}: Disable DPPS cabinet door alarm

G_{t+1}: Steal key

G_{t+2}: Arrange special equipment

Figure 6. Attack tree for the bistable processor of the reactor protection system.

first the subscript in the root node was numbered, then the subscripts in the nodes one level below the root node (from left to right) and so on. We used the lower case alphabets plus a number (by following a sequence) for numbering the subscripts of the nodes in transfers. The first alphabet in the sequence represents the topmost row in a transfer and the smallest number represents the leftmost node in a transfer. When the topmost and leftmost node in a transfer represents the leftmost node in a row of the main tree then the value of the alphabet will be equal to the value of subscript of the rightmost node in the preceding row of the main tree. Similar convention can be used while numbering the subscripts in the succeeding rows of a transfer. For example, the value of p in the node G_{p+1} (in transfer 1 under the node G_7) will be 14. Similarly, the value of q in the node G_{q+1} (in the second row of transfer 1) will be v+2 (the rightmost node in the preceding row of the main tree). In other case, the value of the subscript of the leftmost node should be followed from the immediate right node in the same row of the main tree. We notice that further research for the development of a numbering scheme will be extremely valuable.

Furthermore, we also observed that the present formulation of attack trees has limited capability to represent the attacks in which an order or a sequence must be followed. For example, G_{q+3} will occur only if G_{r+1} precedes G_{r+2} in transfer 4, and G_{q+4} cannot occur if G_{r+3}, G_{r+4}, and follow an order of occurrence from left to right and G_{r+5} cannot occur unless G_{r+3} has occurred before the occurrence of G_{r+4} in transfer 3. However, the use of the "AND" nodes for both cases do not consider either an order or a sequence for the occurrences of their children. Hence, addition of some new nodes in the present attack tree formulation to accommodate aforementioned attack formats will be worthy.

3.4 Attack tree analysis

All possible attack scenarios have been generated from the attack tree (Figure 6) for the identified threat sources. Attack scenarios for the disgruntled employee were obtained by deleting the G_{q+4} node from the attack tree. The nodes G_8, G_9, G_{u+2}, G_{p+1}, and G_{q+3} were eliminated from the attack tree in order to obtain the attack scenarios for the corporate employee. While we got the attack scenarios for the maintainer by effacing the nodes G_5, G_7, G_9, G_{15}, G_{13}, G_{v+1}, and G_{p+2} from the attack tree. The generated attack scenarios are shown in Table 4. Twenty-six attack scenarios represent how the disgruntled employee might reach the attack goal; five scenarios show that how the maintainer might reach the attack goal, while there are only two scenarios in which the corporate employee can reach the attack goal.

The possibility level of a leaf node represents the possibility (likelihood) of occurrence of the attack. While the consequence level represents the consequences of the attack on the RPS_BP1 and its operational environment. The SRL represents the qualitative level of cyber security risk posed by a threat and is determined by combining the consequence and possibility level based on subjective estimates. The subjective estimates reflect an individual's or group's degree of belief or confidence that a particular attack will occur. The factors involved in assigning the possibility levels include the attacker's motivation and level of difficulty to carry out the attack. In the absence of information about the capabilities and motivation of threat sources, we considered the highest motivation level while perceiving the motivation of attacker. The level of difficulty to launch a cyber attack towards a system is highly depends on two factors. First, counter measures (SCs) placed in the operational environment of the system to counter the attacks and the second, resilient features of the system against the attacks. Qualitative values of possibility, consequence, and risk for atomic attacks (leaf nodes) are shown in a radar chart (Figure 7). The levels of possibility, consequence and security risk are minimal at the origin (centre) of the chart whereas their maximal levels are represented by the outer boundary of the chart. The SRLs of the root node and attack scenarios were determined according to the procedure described earlier in section 2.6. The SRLs of the root node for the disgruntled employee and for the maintainer were obtained as SL_3, whereas the same for the corporate employee was determined as SL_4. While nine attack scenarios have the SRL SL_3, eighteen have the SRL SL_4, and the other six have the SRL SL_5. The SRLs of the attack scenarios are shown in Table 4.

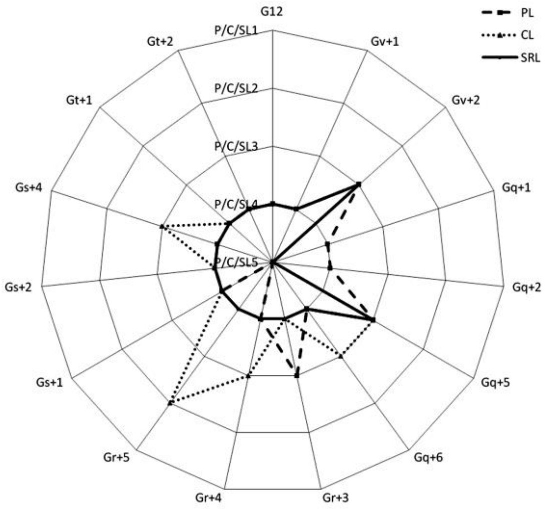


Figure 7. Possibility levels, consequence levels and security risk levels for the leaf nodes.

We have ascertained that the process of analyzing the attack tree is very cumbersome in the present formulation of attack trees. We need to construct a new tree or at least have to efface some portions or nodes of the tree while determining the SRL of the root node for a different threat source. In addition, while evaluating the SRL of different designs of a system during the system development process some portions of an already built tree for the system may became irrelevant for a certain design configuration. For example, while

Table 5. Relationship between the atomic attacks and threats.

Atomic attacks vs. threats	G_{v+1}	G_{v+2}	G_{q+1}	G_{q+2}	G_{q+5}	G_{q+6}	G_{r+3}	G_{r+4}	G_{r+5}	G_{s+1}	G_{s+2}	G_{s+4}	G_{t+1}	G_{t+2}
Intrusion			✓				✓	✓		✓				
Disclosure			✓	✓	✓	✓	✓			✓	✓		✓	
Disruption	✓	✓			✓	✓		✓	✓			✓		✓
Modification	✓	✓			✓	✓						✓		✓
Destruction	✓													✓

developing a new system similar to one described in section 3.1 (Figure 3) if a designer decides to eliminate the system's link to the monitoring systems through the gateway. Then the attack paths originated from the attack scenario <G_{r+3}, G_{r+4}, G_{r+5}> will become irrelevant in the attack tree (figure 6). We therefore, foresee a need for development a mechanism that can turn "ON" or "OFF" some nodes or potions of the attack tree. Furthermore, the development of a tool that can support the construction, analysis, and assessment of the tree will be worthwhile.

Table 6. Relationship between the threats and security objectives.

Threats vs. SOs	Destruction	Disclosure	Disruption	Intrusion	Modification
Control of malicious code	✓		✓		✓
Limiting access		✓		✓	
Maintenance management	✓		✓		✓
Right identification, authentication and authorization		✓		✓	
Security awareness and training		✓			
Security monitoring				✓	

3.5 *Cyber security risk assessment and risk mitigation*

The SRL of the system must be equal to the DRL (assuming SL_5). The SRL of the system was above the DRL for all the identified threat sources. Moreover, only six attack scenarios have the DRL. Possible risk mitigation options (SCs) were suggested according to the SRL of each scenario and are shown in Table 4. However, the SCs were not evaluated for suitability, as it will be very difficult to retrofit those in the present designs of I&C systems [21, 52]. The risk mitigation options, include the managerial controls (shown in Table 4), which can be placed in the operational environment of RPS_BP1 to minimize the possibility of occurrence of attacks.

Moreover, the SRs were elicited and shown in Table 7. The SRs will help in developing the CSP for present systems and in developing new secure systems in future. The suitability of the SRs that those will address the real threats to the systems was checked by using the procedure described in section 2.9. The relationships between SRs, SOs, atomic attacks (leaf nodes), and threats is shown in Tables 5 to 7 respectively.

Table 7. Relationship between security objectives and security requirements.

SOs vs. SRs	Control of malicious code	Limiting Access	Maintenance management	Right identification, authentication and authorization	Security awareness and training	Security monitoring
Approved and qualified person for maintenance			✓			
Biometrics based authentication				✓		
Control of removable media	✓					
Intrusion detection system						✓
Limiting access to absolute minimum		✓				
Malicious code detection and handling	✓					✓
Safety locks for cabinets		✓				
Secret coding of keys		✓				
Security awareness					✓	
Security operating procedures			✓		✓	
Security training					✓	
Strong password management				✓	✓	
Two-person rule		✓		✓		

4. Conclusions

The attack tree based methodology provides a systematic and effective method to model and understand the attacks towards nuclear digital I&C systems. We expect that this methodology will be very useful for identifying key security issues, for documenting plans and possibility of attacks. It will also help system developers, system administrators, and system owners. System administrators can understand the potential impact of attacks on the operations and that will help them to justify the expenditures on security. If the generic type of vulnerabilities and their consequences are known then the developers can avoid those during the system development. Moreover, the attack scenarios can help to build simulators, which will be useful for security awareness and training of plant staff.

Although, the application of attack trees to analyse the cyber security of the components and subsystems provide very good results. However, to analyse the security at system level requires the construction of a system level tree. It will be very difficult to construct the system level tree using the conventional attack tree formulation [53]. In some cases, a large combination of "AND/OR" nodes is required to model attacks towards certain system mechanisms; consequently, the resulting tree becomes very complicated and difficult to evaluate. While in some other cases the formulation lack ability to model the attacks that require the exploitation of vulnerabilities in fault or intrusion tolerant mechanisms. Therefore, enhancements and improvements in the conventional formulation of attack trees will be worthwhile.

Acknowledgement

The author is very thankful to two anonymous referees for their very useful remarks to improve the quality of this paper.

References

[1] M. Oba et al., I&C design features for fully computerized systems in the US-APWR, Int. Cong. Advances NPPs, Nice, France (2007), www.sfen.fr/icapp2007.

[2] J. Timothy McCreary, A. Hsu, Cyber Secure Systems Approach for NPP Digital Control Systems, NPIC&HMIT (2006) p.548-559.

[3] NUREG/CR-6842, Advanced reactor licensing: experience with digital I&C technology in evolutionary plants, U.S. Nuclear Regulatory Commission (2004).

[4] S. S. Lee, M. Chiramal and E. J. Lee, Potential vulnerability of plant computer network to worm infection, NRC Information Notice 2003-14, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission (August 29, 2003) http://www. nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2003/.

[5] K. Poulsen, Slammer worm crashed Ohio nuke plant network, Security Focus, http://www.securityfocus.com/news/6767 (2003).

[6] B. Littlewood, S. Brocklehurst, N. Fenton, P. Mellor, S. Page and D. Wright, J. Comput. Security **2** (1993) 211.

[7] F. Gong et al., Characterizing intrusion tolerant systems: Using a state transition model, Proc. DARPA Information Survivability Conf. and Exposition (2001).

[8] B. B. Madan et al., Modeling and quantification of security attributes of software systems, Proc. Int. Conf. Dependable Sys. Networks (2002) p.505-514.

[9] B. Karabacak and I. Sogukpinar, Comput. Security **24,** No. 2 (2005) 147.

[10] Cost-Of-Risk Analysis (CORA), www.IST-USA.com

[11] C. Taylor, A. Krings and J.A. Foss, Risk analysis and probabilistic survivability assessment (RAPSA): An assessment approach for power substation hardening, Proc. ACM Workshop Scientific Aspects Cyber Terrorism (2002) p.1–9.

[12] C. Fung et. al., Survivability analysis of distributed systems using attack tree methodology, IEEE Military Commun. Conf., Atlantic City, New Jersey (2005) p. 583- 589.

[13] N.G. Leveson, System Safety and Computers, Safeware, Addison Wesley Publishing Company, USA (1995) Ch. 13, p. 290.

[14] CERT, Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), www.cert.org/octave/

[15] KINS/GT-N27, Cyber Security of instrumentation and control systems in nuclear facilities, Korea Institute of Nuclear Safety (KINS), Republic of Korea (2007).

[16] J. Aagedal et al., Model-based risk assessment to improve enterprise security, Proc. 6th Int. distributed object computing Conf. (2002).

[17] Control Objective for Information and related Technology (COBIT), www.isaca.org/cobit/

[18] E. Adar and A. Wuchner, Risk management for critical infrastructure protection (CIP) challenges, best practices & tools, Proc. 1st IEEE Int. Work. Critical Infrastructure Protection (2005).

[19] B. Blakley, E. McDermott and D. Geer, Information security is information risk management, Proc. Workshop New Security Paradigms (2001) p.97–104.

[20] M. Gerber and R.V. Solms, Comput. Security **24,** No.1 (2005)16.

[21] INL/EXT-06-11478, Control systems cyber security: defense in depth strategies, Idaho National Laboratory, USA (2006) p.8.

[22] E.J. Byres, M. Franz and D. Miller, The use of attack trees in assessing vulnerabilities in SCADA systems, Proc. Int. Infrastructure Survivability Work., Lisbon, Portugal (2004).

[23] K. Edge, R. Raines, R. Bennington and C. Reuter, The use of attack and protection trees to analyze security for an online banking system, Proc. 40th Hawaii Int. Conf. Sys. Sci. (2007).

[24] B. Schneier, Attack Trees, Dr. Dobb's Journal **24,** No.12 (1999) 9.

[25] CERT/CC Statistics, CERT Coordination Center, http://www.cert.org/stats/

[26] All Net Security Database, Fred Cohen & Associates, http://www.all.net/CID/threat/threat.html.

[27] Security bulletin, Microsoft Corporation, http://www.microsoft.com/technet/security/.

[28] Common Vulnerabilities and Exposures (CVE) and Common Configuration Enumeration (CCE) Statistics, National Institute of Standards and Technology (NIST) USA, http://nvd.nist.gov/.

[29] Open Vulnerability and Assessment Language (OVAL), http://oval.mitre.org/oval /about/index.html.

[30] Open Source Vulnerability Database (OSVDB), http://osvdb.org/.

[31] Symantec threat explorer, Symantec Corporation http://www.symantec.com/ business/security_response/threatexplorer

[32] E. J. Byres and J. Lowe, The myths and facts behind Cyber Security Risks for Industrial Control Systems, Proc. VDE Congress, Berlin (2004).

[33] Control systems - overview of cyber vulnerabilities, US-CERT, http://www.uscert. gov/control_systems/csvuls.html

[34] IAEA-Nuclear Security Series, Security of Information and I&C Systems at Nuclear facilities (2007) p.16-17, http://entrac.iaea. org/I-and-C/TM_IDAHO 2006/CD/CyberSec Doc_v1_rev20070206_AC_secure.pdf

[35] ISO/IEC 15408, Information technology — Security techniques — Evaluation criteria for IT security, 2005, Part 1-3, www.iso.org/

[36] P. Moore et al., Attack Modeling for Information Security and Survivability, Software Engineering Institute, Carnegie Mellon University (CMU), Technical note: CMU/SEI-2001-TN-001.

[37] IEEE Std 1012-2004, IEEE Standard for Software Verification and Validation , IEEE Computer Society (2005) Annex B, p.88-89

[38] AS/NZS 4360, Risk management, Standards Association of Australia, www.wales.nhs. uk/ihc/documents/A.4.1.4_ Australia_and_New_Zealand_Methodology_ AS_NZ%204360_1999.pdf (1999) App. E, p.34-35

[39] Y. Kang, C.H. Jeong and D.I. Kim, Regulatory approach on digital security of instrumentation, control and information systems in nuclear power plants, Proc. IAEA Technical Meeting Cyber Security NPP I&C Info. Sys. (2006).

[40] NIST SP 800-53, Recommended security controls for federal information systems, National Institute of Standards and Technology (NIST) (2007) http://csrc.nist. gov/publications/PubsSPs.html.

[41] NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology (NIST) USA (2007) Ch. 6.

[42] ISA-TR99.00.01-2004, Security technologies for manufacturing and control systems (2004) www.isa.org.

[43] ISO 17799, Information Technology – Code of practice for information security management (2005) www.iso.org/.

[44] Maria Karyda et al., Comput. Security **24,** No. 3 (2005) 246.

[45] SAND 2005-1002C, Framework for SCADA Security Policy, Sandia National Laboratories Report (2005).

[46] P. A. Khand and P. H. Seong, An Attack Model Development Process for the Cyber Security of Safety related Nuclear Digital I&C Systems, Proc. Korean Nuclear Society fall meeting, Jeju Island, Republic of Korea (2007).

[47] R.Watabe, T. Oi and Y. Endo, The security design of remote maintenance system for nuclear power plants, based on ISO/IEC 15408, Proc. IAEA Technical Meeting Cyber Security NPP I&C Info. Sys. (2006).

[48] R. Lamarsh and J. Baratta, Introduction to Nuclear Engineering, Addison-Wesley, 3rd ed. (2001).

[49] P.H. Seong, Nuclear Power Plant Instrumentation Systems, NQE-532 Notes, Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology (KAIST), Republic of Korea, (2005) p.717-815.

[50] P.H. Seong, Nuclear Power Plant Instrumentation System Design, NQE-631 Notes, Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology (KAIST), Republic of Korea, (2006) Ch.8.

[51] S. R. Koo et al., Nucl. Eng. Tech. **38,** No. 3 (2006) 259.

[52] V. M. Igure et al., Comput. Security **25,** No.7 (2006) 498.

[53] D. M. Nicol et al., IEEE Trans. Dependable Secure Computing **1,** No.1 (2004) 48.