Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 10-11, 2007

Towards the Development of a Methodology for the Cyber Security Analysis of Safety Related Nuclear Digital I&C Systems

Parvaiz Ahmed Khand, Poong Hyun Seong
Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology,
371-1, Guseong-dong, Yuseong-gu, Daejeon, 305-701, Republic of Korea
parvaiz@kaist.ac.kr, phseong@kaist.ac.kr

1. Introduction

In Nuclear power plants the redundant safety related systems are designed to take automatic action to prevent and mitigate accident conditions if the operators and the non-safety systems fail to maintain the plant within normal operating conditions. In case of an event, the failure of these systems has catastrophic consequences.

The tendency in the industry over the past 10 years has been to use of commercial of the shelf (COTS) technologies in these systems. COTS software was written with attention to function and performance rather than security. COTS hardware usually designed to failsafe, but security vulnerabilities could be exploited by an attacker to disable the fail safe mechanisms**.** Moreover, the use of open protocols and operating systems in these technologies make the plants to become vulnerable to a host of cyber attacks [1, 2, 3].

An effective security analysis process is required during all life cycle phases of these systems in order to ensure the security from cyber attacks [5].

We are developing a methodology for the cyber security analysis of safety related nuclear digital I&C Systems. This methodology will cover all phases of development, operation and maintenance processes of software life cycle.

In this paper, we will present a security analysis process for the concept stage of software development life cycle.

2. Methods and Results

For security analysis, the waterfall lifecycle phases are considered as a framework for describing specific digital safety system security guidance [5, 6].

The security analysis process for the concept stage of software development is shown in Figure 1. The process involves: (i) Building a conceptual model of system and its IT environment from security perspective, (ii) Analyzing the system and its IT environment from security perspective, (iii) Analyzing the identified security risks posed by threats, (iv) Analyzing the security risks introduced by system itself and its IT environment, (v) Enlisting the new identified security risks and (vi) Making security analysis report.

To carry out the security analysis, concept documentation and preliminary threat and risk assessment (TRA) are used as inputs. The process started by building a conceptual model of the system as shown in Figure 2. The conceptual model will help to identify the system, system boundaries, its IT environment and the limits of resolution.

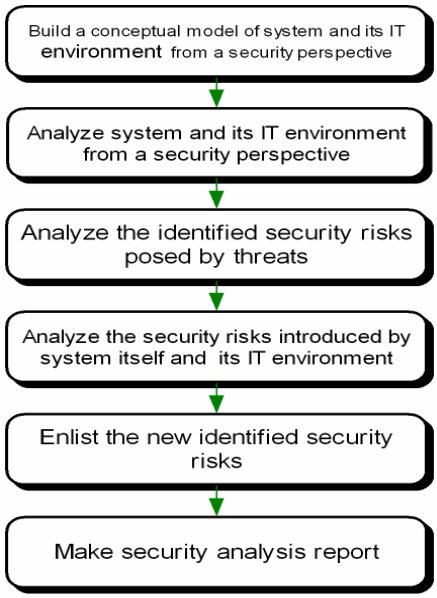

Figure 1. Security analysis process for concept stage

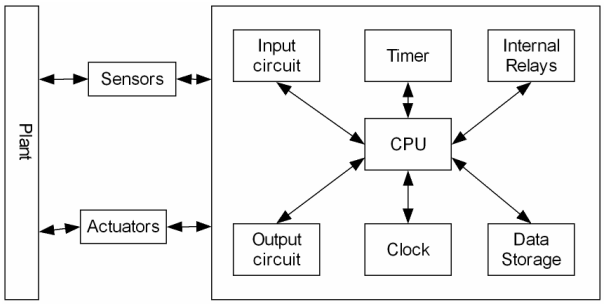

Figure 2. Conceptual model of a safety related system

As a result of analysis of the system, its IT environment and already identified threats, a software integrity level (SIL) matrix [6] was formed according to the severity and probability of occurrence of each threat. The SIL matrix is shown in Figure 3. Based on SIL matrix mitigation strategies were identified and recommendations to eliminate security risks posed by the identified threats were reported in security analysis report. The results reported in the report can be

translated to security requirements as a part of software requirement specification (SRS) documentation.

Error	**Likelihood of occurrence of an operating state that contributes to the error (decreasing order of likelihood)**			
Consequence	**Reasonable**	**Probable**	**Occasional**	**Infrequent**
Catastrophic	--	Buffer overflows, Modifying thresholds/ set points	Corruption of OS	---
Critical	---	Modification of I/O data	I/O data fabrication	---
Marginal	---	Corruption of stored data	Interruption of I/O data	---
Negligible	---	Interception of I/O data	---	---

Figure 3: SIL matrix for the system model

3. Conclusion

A security analysis methodology, based on the waterfall lifecycle phases is considered as a framework for describing specific digital safety system security guidance.

The security analysis process for the concept stage of software development has been developed. The process involves: (i) Building a conceptual model of system and its IT environment from security perspective, (ii) Analysis of the system and its IT environment from security perspective, (iii) Analysis the identified security risks posed by threats, (iv) Analysis the security risks introduced by system itself and its IT environment, (v) Enlisting the new identified security risks, and (vi) Security analysis report.

REFERENCES

[1] Timothy J. McCreary, Allen Hsu, Cyber Secure Systems Approach for NPP Digital Control Systems, Proceedings of NPIC&HMIT, p. 548-559, 2006
[2] Joseph E. Marron, Applications for Cyber Security—System and Application Monitoring, Proceedings of NPIC&HMIT, p. 536-541, 2006
[3] David I. Gertman, Ralph Folkers, Jeff Roberts, Scenario-Based Approach to Risk Analysis in Support of Cyber Security, Proceedings of NPIC&HMIT, p. 542-547, 2006
[4] ISO/IEC 15408, Information technology — Security techniques — Evaluation criteria for IT security, 2005
[5] DG-1130, Criteria for use of Computers in Safety Systems of Nuclear Power Plants, 2004
[6] IEEE STD 1012, IEEE Standard for Software Veification and Validation, 2004