Cyber Threat and vulnerability Analysis for Digital Assets of NPPs

Oh Eung-Se(esoh@kepri.re.kr) [a], Seo In-Yong(iyseo@kepri.re.kr) [a] , Kim See-Hong(eunkoo@khnp.co.kr) [b]
[a] *Nuclear Power Lab., Korea Electric Power research Institute(KEPRI), Daejeon, R.O. Korea*
[b] *Project Engineering Dept., Korea Hydro & Nuclear Power Co. LTD(KHNP), Seoul, R.O. Korea*

1. Introduction

Today's computer and communication technology breakthrough make increase plant floor replacement from analog instrumentation and control systems of nuclear power plants to a full-fledged digital system .

The rich functionality and crisp accuracy are one of big advantages of digital technology adaptation, but use of open networks and inherited shared system resources (memory, network, etc.) are well known weak points of digital system. Intended or un-intended cyber attack throughout power plant digital control system's weak point may result to wide area of system failures and that easily defeats system operation and multiple protection safeguards. Well organized cyber security analysis for nuclear plant digital control systems (digital assets) are required.[1]

2. Cyber Threats, Vulnerabilities and Risks of Digital Assets

2.1 Threats

By the different view of cyber triad's (Confidentiality, Integrity, Availability: C-I-A) importance between industry and Information Technology (IT) domain, well known cyber issues of IT domain may have less highlight at plant floor application. Sources of cyber threat come form natural phenomena or artificial entities.[2] Threats take advantage of any existing or possible (system) vulnerabilities. Severity and frequency of threats contribute to risk amount of the digital assets.

An example of threat matrix is shown as Table 1.

Table.1 Threat Matrix

Threat agent		Attack skill/ knowledge	System skill/ knowledge	System accessibility
Internal	Employee	Low	High	Easy/ Frequent
	Contracted Service men	Low	High	Moderate/ Moderate
	System service men	May low	High	Restricted/ Rare
External	Novice hacker	Medium	May low	Restricted/ Rare
	Criminal party (include black hacker)	Very high	May high	Restricted/ Rare

As shown on table, cyber threats can be divided by plant boundary, internal or external.

The one evaluation point of cyber security threat is target digital asset's physical and operational characteristics. In Table 1, one of these factor is expressed as system accessibility. Considering digital assets installed and operation specific characters, threats spectrums can be narrowed and measurement of threat level and magnitude can be more system specific.

Security threats caused by external party are mostly intended and well organized to achieve their objects. They may use internal knowledge to make the attack more effective.

2.2 Vulnerability

Vulnerabilities give pathway of threats to digital assets. Vulnerability can introduce form design, implementation, operation or maintenance phase.

Evaluation for any vulnerability exist and removal of any identified week point should be continued during digital assets all life cycle phase.

If any devices are implemented for counter measuring purpose, vulnerability analysis of the devices is also included. A system may require re-configuration per operational purposes. Security vulnerable operational sequence must be identified. System software or hardware can be changed unintentionally or intentionally throughout system life cycle.

2.3 Risk

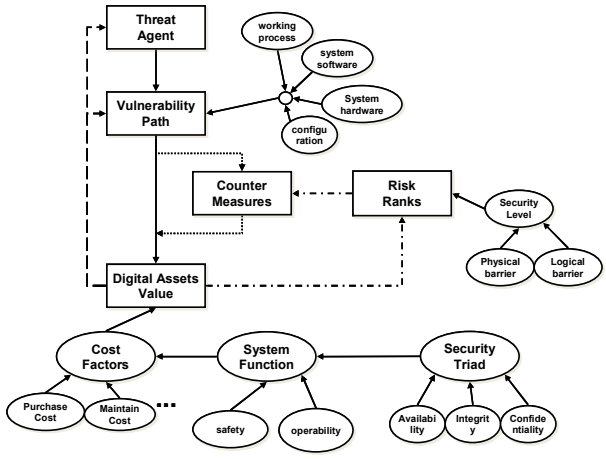

Fig.1. Threat, Vulnerability and Risk Assessments Relation

Risk is a measure of 1) the probability of a successful attack and 2) the consequences of that successful attack.[3] An attack is an actual realization of a threat. Risk can be expressed as follows.

$$cyber\ risk = f_{cyber}(threat, vulnerability, asset\ character) * f_{system}(criticality)$$

Figure 1. shows conceptual relation models for cyber security threat, vulnerability, risk and digital asset value of power plant control system. Generally, nuclear power plant control system's useful life is longer than 15 years, plant function lost cost is higher than digital system's lifetime cost(acquisition, maintain cost, etc.).

3. Conclusions

Example of threat matrix that integrated with target digital assets working environments are shown. Purpose of the integration is to narrow down real threats to the system. That will reduce the efforts of cyber security analysis and assessment.

Cyber threat, system vulnerability, asset value related with plant function and risk analysis relational models are proposed. This scheme shows how and where digital assets characteristics are merged to various steps of cyber security analysis.

Integration of cyber characteristics and plant operating conditions of digital asset will reduce cyber analysis scope and give more meaningful results of threat and vulnerability analysis and assessment.

REFERENCES

[1] Korea Institute of Nuclear Safety (KINS), "Technical Guidelines for Instrumentation and Control Systems of NPPs", KINS/GT-N27, 2007.12
[2] US NRC RG 1.152 Rev.2, "Criteria for use of computer in safety systems of nuclear power plants" 2006
[3] Thomas Kropp, "System Threats and Vulnerability – An EMS and SCADA Security System Overview", IEEE Power & Energy Magazine, 2006.4
[4] US DHS, "Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments", 2009.7
[5] David P. Duggan, John T. Michalski, "Threat Analysis Framework", SAND2007-5792, 2007.9
[6] David P. Duggan et al., "Categorizing Threat – Building and Using a Generic Threat Matrix", SAND2007-5791, 2007.11