Review on Cyber Security Programs for NPP Application

Oh Eung-Se (esoh@kepri.re.kr)
Nuclear Power Lab., KEPCO Research Institute (KEPRI), Daejeon, R.O. Korea

1. Introduction

Increased history records of cyber security (CS) attacks and concerns for computers and networks technical mishaps pull out cyber security to open places. In spite of secrete nature of security, transparent and shared knowledge of many security features are more required at modern plant floors.
Korea Institute of Nuclear Safety (KINS), US Government and Nuclear Regulatory Commission (NRC) requested to develop cyber security plans and enforce their implementing to the NPPs. [KINS] [CFR] [RG 5.71]
This paper reviews various cyber security guidelines and suggests an applicable cyber security program development models during the life cycle of NPP's Instrumentation and Control (I&C) systems.

2. Cyber Security Life Cycle Programs

2.1 Life Cycle Model

In nuclear industries, are well known waterfall life cycle model for a nuclear system development.
The life cycle model consists of the following phases as concept, requirement, design, implementation, test, installation with acceptance test, operation, maintenance and retirement. This model is referenced by many NRC documents. [0800][1.152][BTP]
Another type of waterfall model is initiation, development (acquisition), implementation, operation & maintenance and disposal as referenced by NIST SP 800-64. The model is referenced as IT system development and related security activities identification purpose.
Another guide, RG 5.71, mainly focus on 'security life cycle' process itself instead of others 'system life cycle'.
The security life cycle process activities are consist of establishment, integrate, monitoring, review, change control and record retention. These activities are not sequel and orders can be changed afterward establishment.

Table 1 System Life Cycle Model

KINS/ GT-N27	Planning	Requirements	Design	Implementation	Integration Validation	Installation	Operation and Maintenance	
RG 1.152	Concept	Requirement	Design	Implementation	Test	Installation	Operation / Maintenance	Retirement
NIST SP 800-64(*)	Initiation	Development/Acqiusition		Implementation/Assessment			Operation and maintenance	Disposal
IEC 61508-1	Concept/ Scope Definition/ Risk analysis	Requirements/ Allocation	Planning (O&M, validation, installation...)	Realization		Installation/ Validation	Operation and maintenance	Disposal

Table 1 shows various life cycle models. Life cycle phase can be divided differently depend on their domain view and acceptance.

2.2 Cyber Security Program Establishment

RG 5.71 describes detail activities and technical attributes pertaining to CS program establishment step. The steps are recommended as following;

1) analyze digital assets include networks
2) review security related information (location, connectivity, infrastructure interdependency, existing security controls
3) develop and apply security defensive architecture
4) implement security controls (technical, operational, management)
5) implement security life cycle activities

RG 1.152 recommends CS program establishment at installation phase of system life cycle.
NIST SP 800-53 suggests developing the programs with organization-wide accepted security controls first and add system specific security control to reduce program development costs.

2.3 Cyber Security Activities

For each design phase, specific CS risks are analyzed and commensurate measures are required. [1.152] [0800]
RG 1.152 describes high level security guidelines for each waterfall life cycle phase. This RG provides guides on security features for safety system and on security activities related to development phase (requirements, design, implementation, test and installation).
Overall CS controls can be grouped as technical controls, operational controls and management controls.[5.71] The simplified security controls and CS program relationship can be expressed as Figure.1.
Technical CS controls are allocated to machines (system) automatically perform security features (‘A’).
Operational CS controls are human (operator) acting security features to maintain system function (‘B’).
Management CS controls cover system, human and various CS related programs (‘C’).

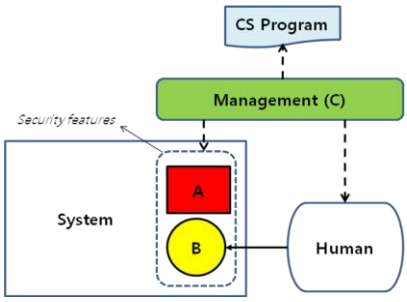

Figure 1 Security Controls and CS Program

NIST SP 800-53 lists minimum set of security control items for IT systems and wide range of security control catalog at the appendices.

3. Conclusions

Different types of system life cycle model for cyber security applications are reviewed. Guidelines describe examples of security activity or features recommended for each life cycle phase. Due to closed loop process of security life cycle, 'when' the activities should included is considered not as much important as to 'how' and 'what'.

Guideline recommends CS program establishment till installation life cycle phase. CS control activities pertaining to the establish steps can be sub-divided as technical, operation and management.

Minimum sets of required security controls selected from various IT security control elements are exampled in the guideline.

One fact of security programs is that those security programs are living documents and continuous reviews and optimization processes are required as other management process.

REFERENCES

[KINS] Korea Institute of Nuclear Safety, Cyber Security of Instrumentation and Control Systems in Nuclear Facilities, KINS/GT-N27, 2007

[CFR] Code of Federal Regulations, Protection of digital computer and communication systems and networks, 10CFR Part 73.54, 2009

[1.152] US NRC, CRITERIA FOR USE OF COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS, NRC Regulatory Guide 1.152 Rev.2, 2006

[5.71] US NRC, CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES, NRC Regulatory Guide 5.71, 2010

[0800] US NRC, Standard Review Plan, NUREG-0800 Rev. 5, 2007

[BTP 7-14] US NRC, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems, NRC Branch Technical Position (BTP) 7-14 Rev. 5, 2007

[27001] IEC/ISO, Information technology - Security techniques - Information security management systems - Requirements, IEC/ISO 27001, 2005

[61508-1] IEC, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements, IEC 61508-1, 1998

[800-64] National Institute of Standards and Technology (NIST), Security Considerations in the System Development Life Cycle, NIST SP 800-64 Rev.2, 2008

[800-53] NIST, Recommended Security Controls for Federal Information Systems, NIST SP 800-53 Rev.2, 2007