Status of Cyber Security R&Ds for Korean NPPs
(국내 원자력 사이버보안 기술개발 및 적용 현황)

May 11, 2016

Jae-Gu Song, Jung-Woon Lee,
Cheol-Kwon Lee

KAERI Korea Atomic Energy Research Institute

Agenda

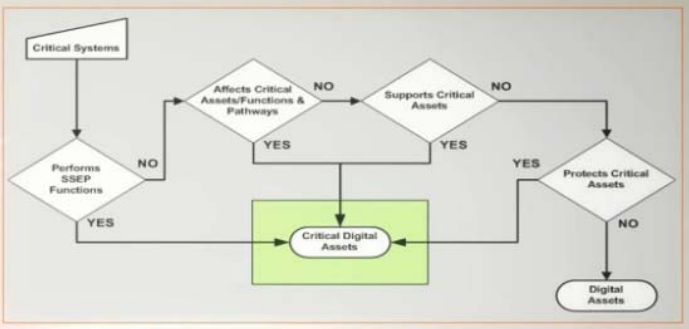
1. CSAMS(Cyber Security Assessment and Management System)
2. Establishment of Test-bed for Cyber Security R&Ds
3. Development of APR1400 Korean MMIS Security Controls (Plan)
4. Collaborations & Supports

1 CSAMS
(Cyber Security Assessment and Management System)

Background

Key Cyber Security Assessment Activities in Regulatory Requirements

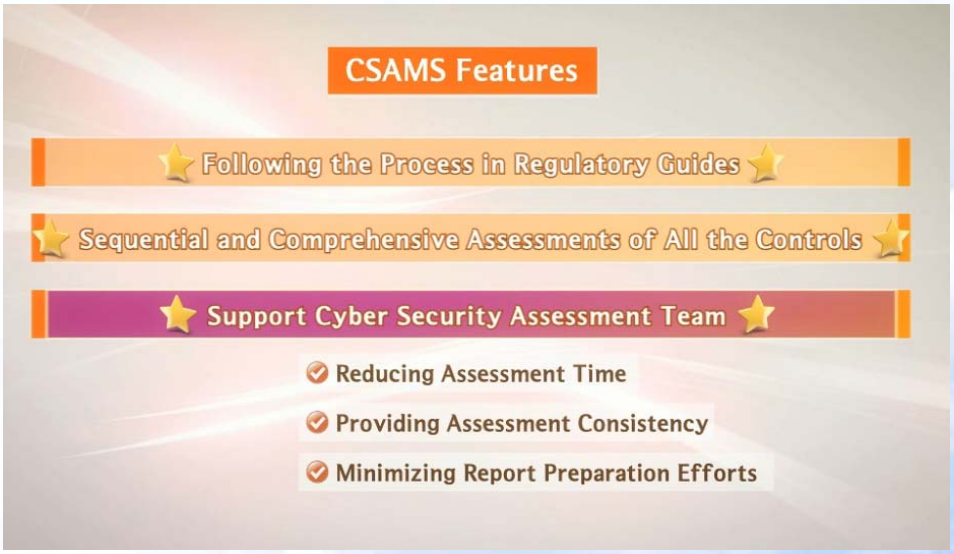
- Formation of Cyber Security Assessment Team
- Identification of CS
- Identification of CDA
- Establishment of Defense-in-Depth Strategies
- Assessment & Implementation of Security Controls
  - Security Controls (>140) for Each CDA
    - Technical Controls
    - Operational & Management Controls



Background

Purposes of CSAMS

- **CSAMS**
  - For the operating plants.
  - To help CSAT(Cyber Security Assessment Team) in NPPs.
  - In checking the compliance of plant cyber security program status with RS-015.



Checklist formation

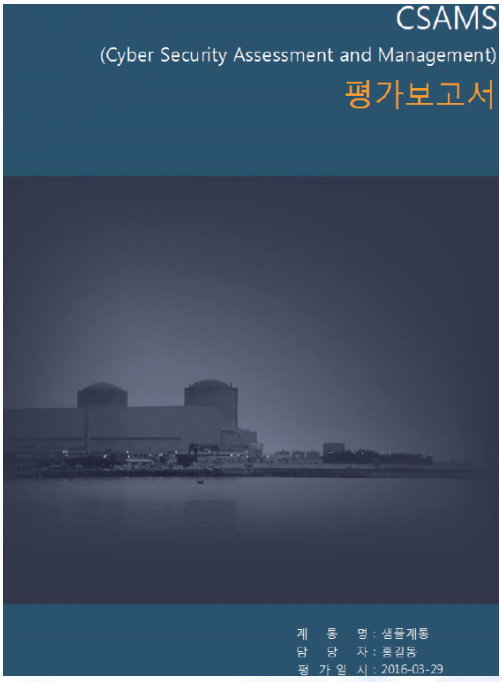
- **Collection of technical security control requirements**
  - Breaking requirements into sentence by sentence
  - From Appendix B : Technical Security Controls – excluding non-technical sentences
  - From Appendix C : Operational and Management Security Controls – including design features
  - Analysis of the applicability

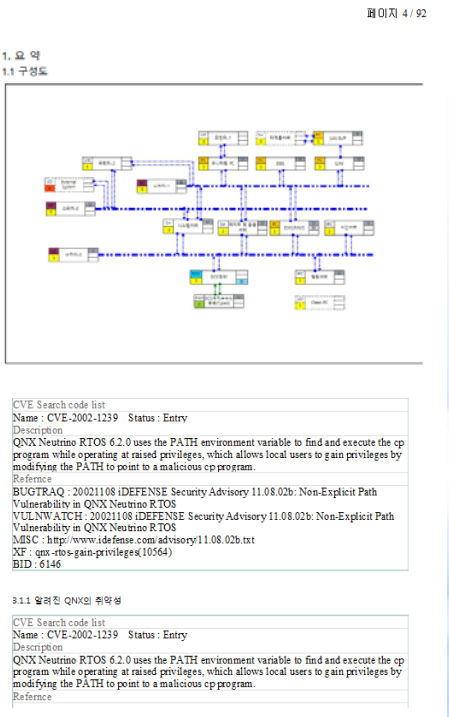
Example requirements in Appendix C to be treated as technical controls

Titles of Control Requirements	Requirements	Reason for inclusion
1. Error Handling	Error conditions are identified, Error messages are revealed only to authorized personnel.	Should be implemented into the system
2. Incident Monitoring	[Licensee/Applicant] tracks and documents security incidents on an ongoing basis using automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	Automated mechanisms should be implemented into the system.

Documentation of results

- **Documentation of results**
  - Sorted by CDAs
  - Sorted by RS-015 requirements





2 Establishment of Test-bed for Cyber Security R&Ds

Scope

- **Test-beds Scoping Considerations**
  - Not a whole scope of MMIS
  - Urgency of making Test-beds (by importance of cyber attack impacts)
    - Safety Systems > Non-safety Systems
  - Applicability & Expandability (Variety of Components)
  - Availability of Test-bed Equipment (by Korean I&C Vendors)
- **KAERI Test-beds for I&C Systems**
  - One channel of ESF-CCS for Safety Systems
  - One channel of DPS for Non-safety Systems
  - One set of NIMS for individual monitoring systems
  - One simplified set of IPS for plant network and monitoring
  - One set of FPGA-based RPS

- ESF-CCS: Engineered Safety Features – Component Control System
- DPS : Diversity Protection System
- NIMS : Nuclear Integrity Monitoring System
- IPS : Information Processing System

Purposes

- Cyber threat information analysis, response, and management
- Cyber security tests and evaluation for change management & periodic assessments
- Technical support for Site incident response and remediation
- Cyber security awareness and training

Design Requirements

- Simulation of System Behavior
  - Behavior of a subject system including interfaces with others
- Emulation of Cyber Attacks
  - Cyber attacks that are possible to happen
- Analysis and Diagnosis Support Functions
  - system responses to cyber attacks
- Other Support Functions
  - Vulnerability analyses
  - Risk assessments
  - Test-bed maintenance
  - Cyber security training & education

Logging System

- Functions
  - Display and storage of various information
    - System error information
    - User and device access information
    - System related information : CPU usage, memory usage, time, etc.
    - Process and File usage information
  - Detection and analysis of changes in the system status
  - Information acquisition, storage, and monitoring
- Design Considerations
  - All exchanged information between the communication modules
  - Data acquisition → not interrupt the performance
  - Store and manage → real time
  - Information from interfacing emulators
  - Collection of device diagnostic signals

3 Development of APR1400 Korean MMIS Security Controls (Plan)

Development of APR1400 Korean MMIS Security Controls (Plan)

1. Development of security functions for safety grade PLC

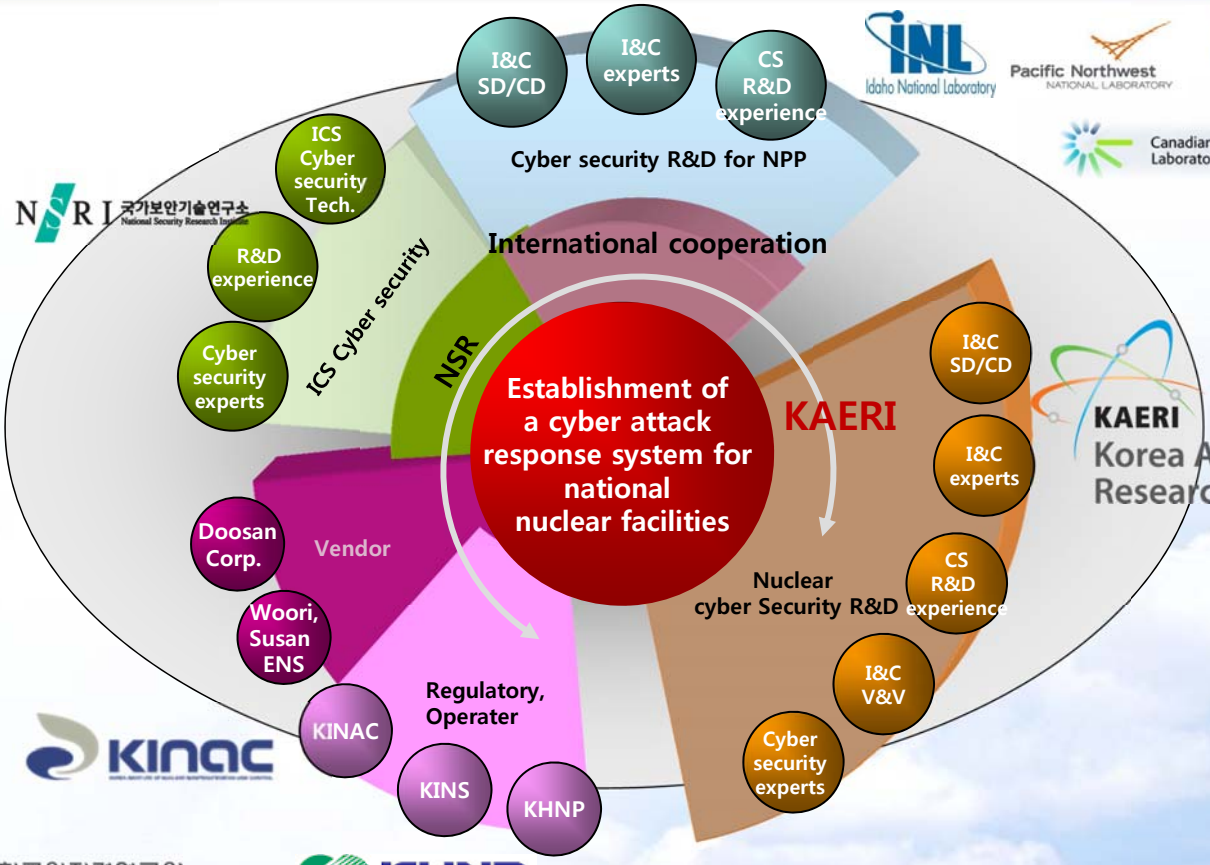
2. Development of security functions for non-safety DCS

3. Development of security functions for non-safety networks

4. Development of penetration testing tools for NPP I&C systems

4 Collaborations & Supports

Collaborations & Supports



Q&A

E-mail
Jae-Gu Song jgsong@kaeri.re.kr
Jung-Woon Lee leejw@kaeri.re.kr
Cheol-Kwon Lee cklee1@kaeri.re.kr