KNS Spring Meeting 2023

Cyber Security Considerations for Technologies Intended in the Future SMR

Yoon Ki Choi, Kyung Jin Lee, Yeon Jun Choo, and Kiwhan Chung

2023. 5. 18.

FNC |주|미래와도전
FNC Technology Co., Ltd.

CONTENTS

1. Introduction

2. Cyber Security Vulnerabilities

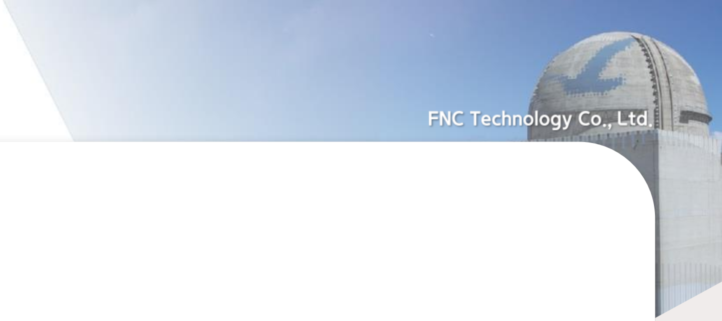
3. Cyber Security Considerations

4. Conclusions

5. Q & A

1 Introduction

1 Introduction



Backgrounds

- Considered Technologies
  - Autonomous Operation
  - Remote Control
  - Load-Following Operation
  - Modularization
- Case Studies in the Current Industry
- Cyber Security Vulnerability

Objectives

- Pre-examination of Cyber Security Vulnerabilities
- Deriving Regulatory and Design Considerations

2 Cyber Security Vulnerabilities

FNC TECHNOLOGY CO., LTD.

2 Cyber Security Vulnerabilities

Autonomous Operation

Reasons to Consider Autonomous Operation

- Reliable Control of Multiple Reactor Modules
- Reduction of the Operator’s Burden

Case Studies in the Current Industry

- Self-Driving Cars and Smart Factories
  - A Demonstration of the “Jeep Cherokee” Hacking in 2015
  - The Discovery of Hyundai Motor’s Blue Link Vulnerability in 2017
  - Stuxnet Incident Discovered in 2010

Cyber Security Vulnerability

- Using communication channels
- External malicious code
- Data and code Threats
- Access to the internal network of unauthorized devices

2 Cyber Security Vulnerabilities

Remote Control

Reasons to Consider Remote Control

- Efficient Role Distribution for Resident Operators

Case Studies in the Current Industry

- Jamming and Spoofing Attacks on Drone in 2016

Cyber Security Vulnerability

- Hacking and Virus
- Spoofing
- Jamming
- Sniffing

2 Cyber Security Vulnerabilities

Load-Following Operation

Definition

- An operation method that adjusts the electrical power of a generator in response to fluctuations in demand or power supply requests in the power system
  - Planned Load-Following Operation
  - Frequency Control

Reasons to Consider Load-Following Operation

- Improvement of the Operating Flexibility of Nuclear Power Plants
- Efficient Combination of Alternative Energy Sources

Applications in the domestic Industry : N/A

Cyber Security issues

- Network Connection with the EMS*
  - Unauthorized Access to the Network
  - System Data and Communication Data Leakage
  - Data Deletion and Destruction of System Data

*EMS: External Power Management System

2 Cyber Security Vulnerabilities

Supply Chain

Reasons to Consider Supply Chains

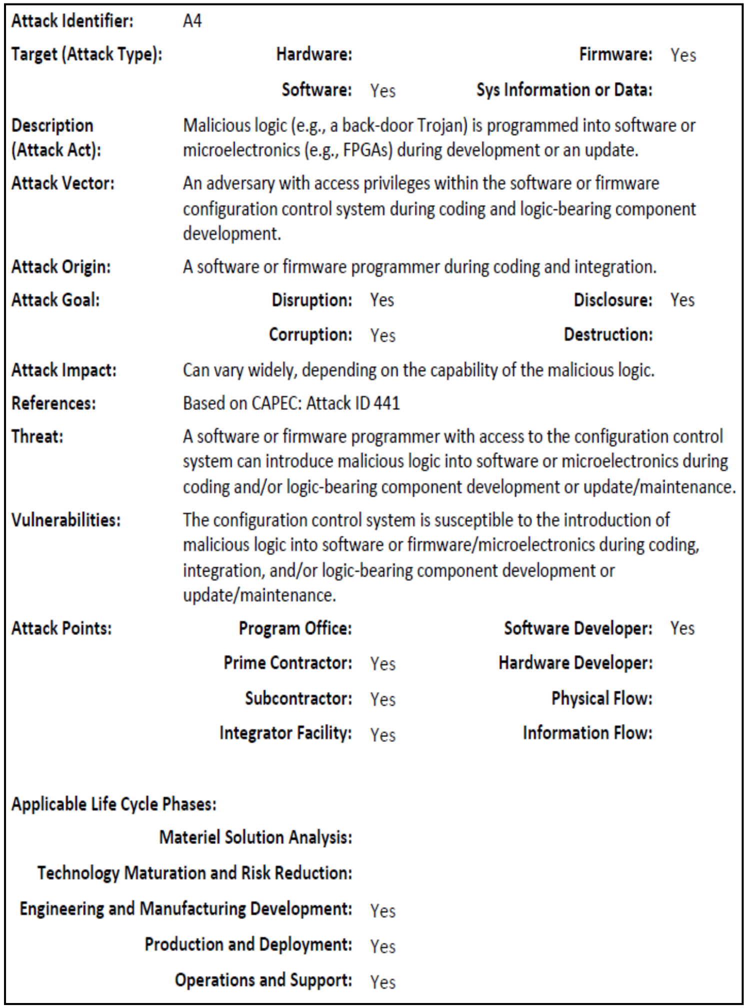
- Increasement of the number of Vendors due to Modularity of SMR

Current Industrial Issues

- SolarWinds Supply Chain Attack
- MITRE Report

Cyber Security Vulnerability

- Malicious Code
- Replacement with Malicious Parts
- Intentional Change of Data
- Increasement of the number of Vendors Requiring Control and Management



Attack Identifier:	A4			
Target (Attack Type):	**Hardware:**		**Firmware:**	Yes
	Software:	Yes	**Sys Information or Data:**	
Description (Attack Act):	Malicious logic (e.g., a back-door Trojan) is programmed into software or microelectronics (e.g., FPGAs) during development or an update.			
Attack Vector:	An adversary with access privileges within the software or firmware configuration control system during coding and logic-bearing component development.			
Attack Origin:	A software or firmware programmer during coding and integration.			
Attack Goal:	**Disruption:**	Yes	**Disclosure:**	Yes
	Corruption:	Yes	**Destruction:**	
Attack Impact:	Can vary widely, depending on the capability of the malicious logic.			
References:	Based on CAPEC: Attack ID 441			
Threat:	A software or firmware programmer with access to the configuration control system can introduce malicious logic into software or microelectronics during coding and/or logic-bearing component development or update/maintenance.			
Vulnerabilities:	The configuration control system is susceptible to the introduction of malicious logic into software or firmware/microelectronics during coding, integration, and/or logic-bearing component development or update/maintenance.			
Attack Points:	**Program Office:**		**Software Developer:**	Yes
	Prime Contractor:	Yes	**Hardware Developer:**	
	Subcontractor:	Yes	**Physical Flow:**	
	Integrator Facility:	Yes	**Information Flow:**	
Applicable Life Cycle Phases:				
	Materiel Solution Analysis:			
	Technology Maturation and Risk Reduction:			
	Engineering and Manufacturing Development:	Yes		
	Production and Deployment:	Yes		
	Operations and Support:	Yes		

MITRE Supply Chain Attack Pattern Template

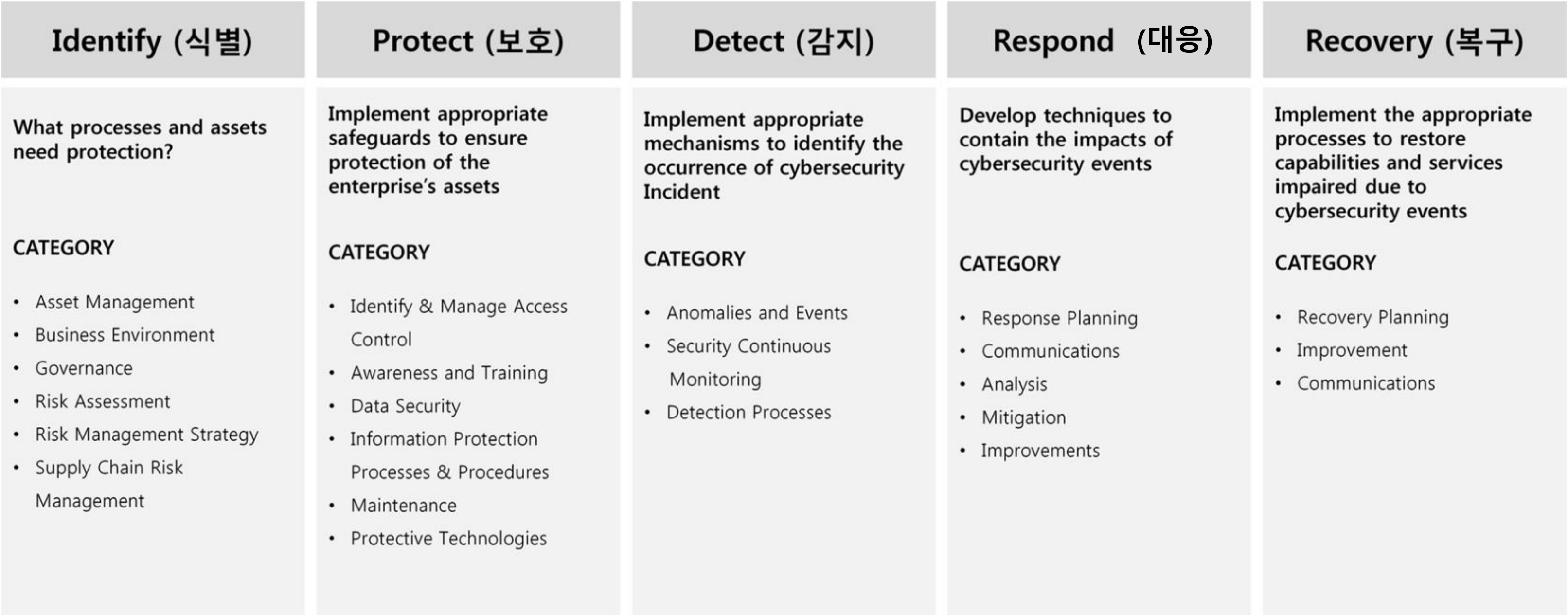
3 Cyber Security Considerations

Autonomous Operation (1/2)

Cyber Security Considerations for Autonomous Operation

Reference of Automotive and Smart Factory Security Standards

NIST CSF System



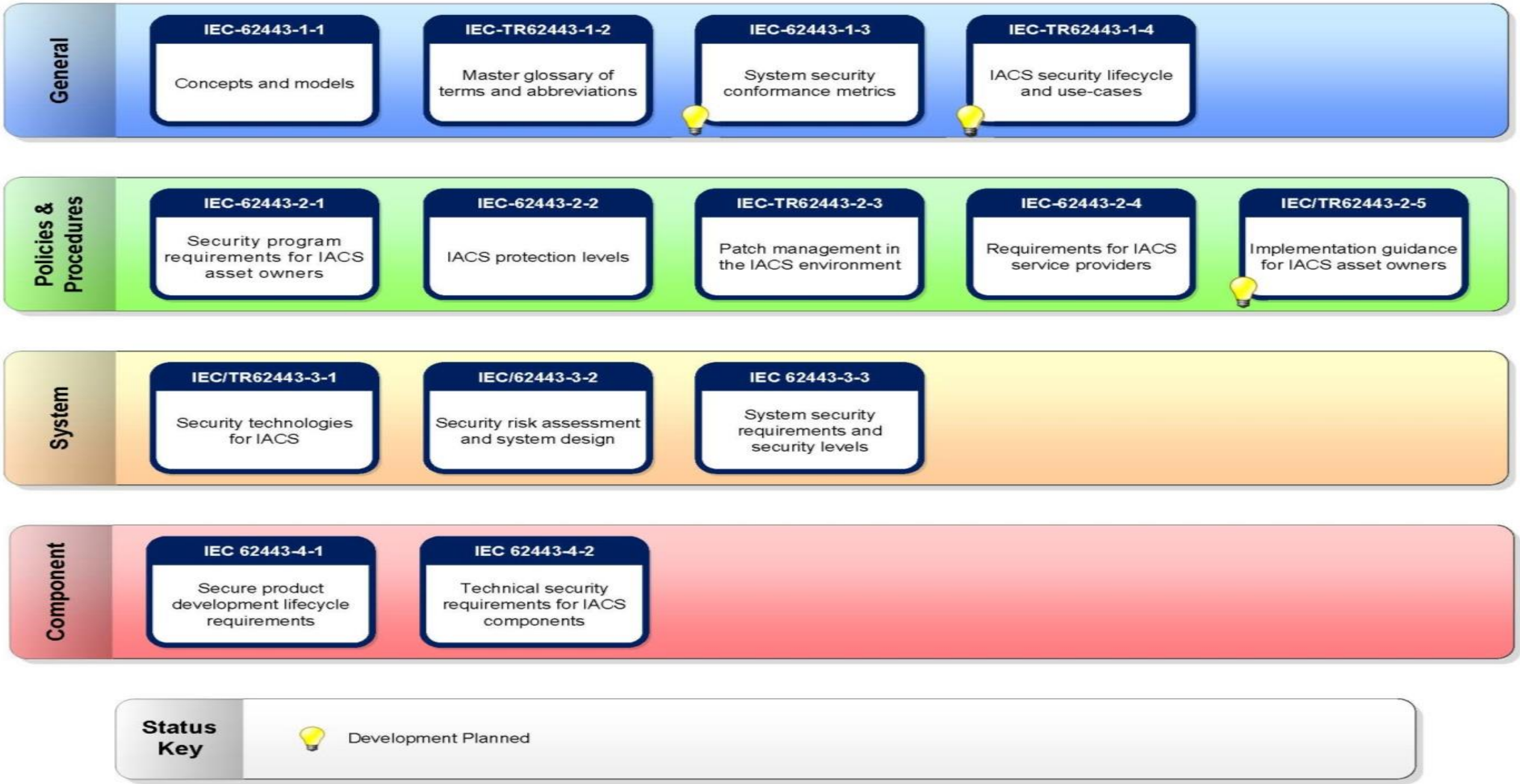
Identify (식별)	Protect (보호)	Detect (감지)	Respond (대응)	Recovery (복구)
What processes and assets need protection?	**Implement appropriate safeguards to ensure protection of the enterprise's assets**	**Implement appropriate mechanisms to identify the occurrence of cybersecurity Incident**	**Develop techniques to contain the impacts of cybersecurity events**	**Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events**
CATEGORY	CATEGORY	CATEGORY	CATEGORY	CATEGORY
• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Supply Chain Risk Management	• Identify & Manage Access Control • Awareness and Training • Data Security • Information Protection Processes & Procedures • Maintenance • Protective Technologies	• Anomalies and Events • Security Continuous Monitoring • Detection Processes	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Recovery Planning • Improvement • Communications

3 Cyber Security Considerations

Autonomous Operation (2/2)

Cyber Security Considerations for Autonomous Operation

- Reference of Automotive and Smart Factory Security Standards
  - ISA/IEC 62443
  - Configuration of Four Groups : General, Policy and Procedures, Systems, Components



General	IEC-62443-1-1 Concepts and models	IEC-TR62443-1-2 Master glossary of terms and abbreviations	IEC-62443-1-3 System security conformance metrics 💡	IEC-TR62443-1-4 IACS security lifecycle and use-cases 💡	
Policies & Procedures	IEC-62443-2-1 Security program requirements for IACS asset owners	IEC-62443-2-2 IACS protection levels	IEC-TR62443-2-3 Patch management in the IACS environment	IEC-62443-2-4 Requirements for IACS service providers	IEC/TR62443-2-5 Implementation guidance for IACS asset owners 💡
System	IEC/TR62443-3-1 Security technologies for IACS	IEC/62443-3-2 Security risk assessment and system design	IEC 62443-3-3 System security requirements and security levels		
Component	IEC 62443-4-1 Secure product development lifecycle requirements	IEC 62443-4-2 Technical security requirements for IACS components			

Status Key	
💡	Development Planned

3 Cyber Security Considerations

Remote Control

Cyber Security Considerations for Remote Control

- Securing the Reliability of the Component Supply Chain to Prevent Virus
- Setting User Access Authority by Condition for Network Connection
- Use Secure Communication Protocols & Encryption Algorithms to Ensure Authentication, Data Integrity and Confidentiality
- Check Integrity of Important Information Stored in Devices and Systems
- Constant Security Updates

Load-Following Operation

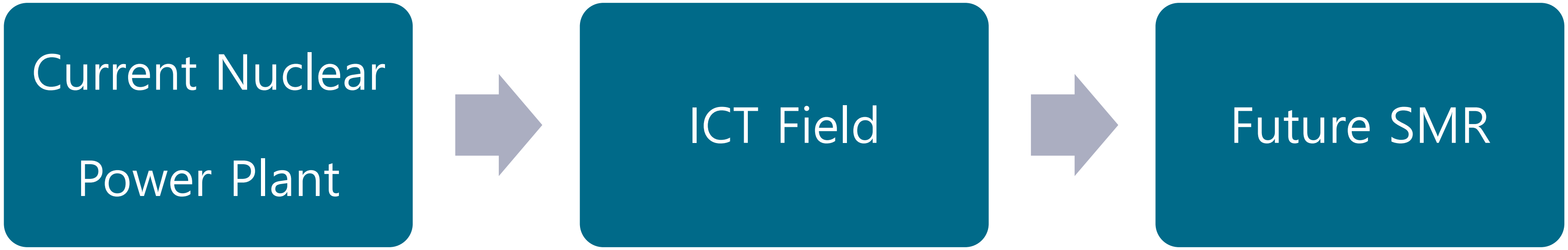
Cyber Security Considerations for Load-Following Operation

- Secure Local and Remote Access Methods
- Setting User Access Authority by Condition for External Network Connection
- Setting Communication Authentication Process from External Network
- Check Whether Information Stored in Devices and Systems has been Tampered with
- Prevention of Leakage of Stored Information

3 Cyber Security Considerations

Supply Chain (1/4)

Approach to Eliciting Supply Chain Considerations



3 Cyber Security Considerations

Supply Chain (2/4)

Regulations for Current Nuclear Power Plants

- NRC RG 5.71
  - Protection of Digital Computers, Communication Systems and Networks
- NRC RG 1.152
  - Standards of Computers Used in Safety Systems
- IAEA TECDOC
  - IAEA TECDOC 919
  - IAEA TECDOC 1169
- International Standards
  - ISO/IEC 27036
  - ISO/IEC 20243

3 Cyber Security Considerations

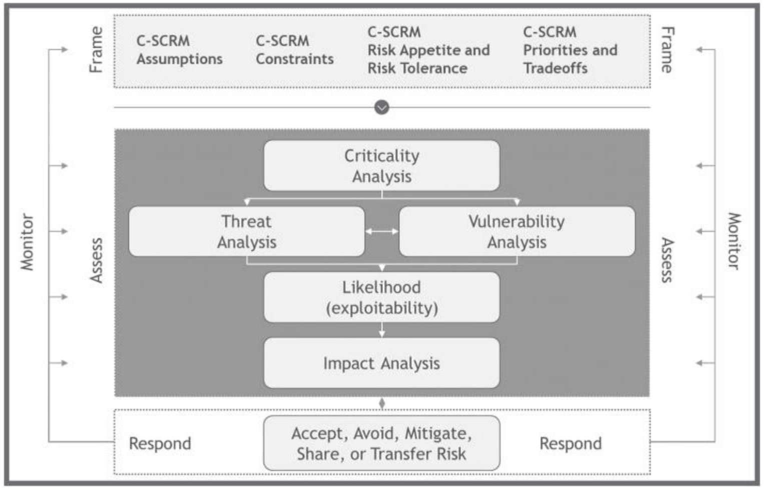
Supply Chain (3/4)

ICT Cyber Security for the Supply Chain

- Lack of Regulations on Current NPPs
- Active Introduction and Utilization of Advanced Supply Chain Management Measures

- UN NIST CSF*
  - C-SCRM*

*CSF: Cyber Security Framework
*C-SCRM: Cyber Supply Chain Risk Management



NIST C-SCRM Structure

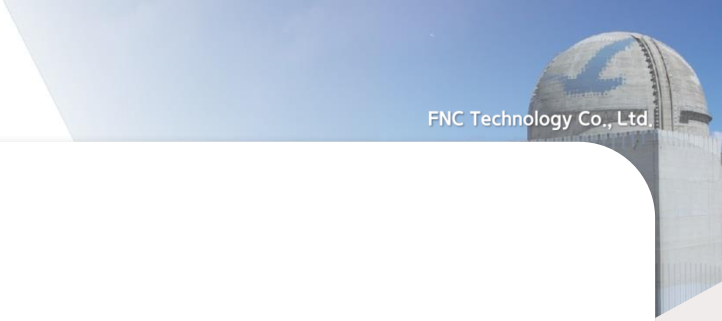
Supply Chain (4/4)

Cyber Security Considerations for the Future SMR

- Analysis of Ecosystem
- Cyber Security Management System
- Cyber Attack Types and Vulnerabilities
- Cyber Crisis Management Framework
- Cyber Security Risk Self-Assessment Program
- Software, Hardware, and Firmware Standards and Guidelines

4 Conclusions

4 Conclusions



Considered Technologies

- Autonomous Operation
- Remote Control
- Load-Following Operation
- Modularization

Cyber Security Vulnerabilities

- External malicious code
- Unauthorized Access to the Network
- Spoofing, Jamming and Sniffing
- System Data and Communication Data Leakage
- Replacement with Malicious Parts

Cyber Security Considerations

- A Framework for Identifying and Addressing Cyber Security Threats in terms of Design or Regulation of Future SMR

5 Q & A

FNC TECHNOLOGY CO., LTD.

ABOUT

미래와도전 본사

16954 경기도 용인시 기흥구 흥덕1로 13, 32층
(영덕동, 흥덕아이티밸리 타워동)
+82-31-8065-5114

대전 지사

대전광역시 유성구 대덕대로 593, 10층 1004-1호
(도룡동, 대덕테크비즈센터)
+82-42-867-5114

미래에너지기술연구소 본관

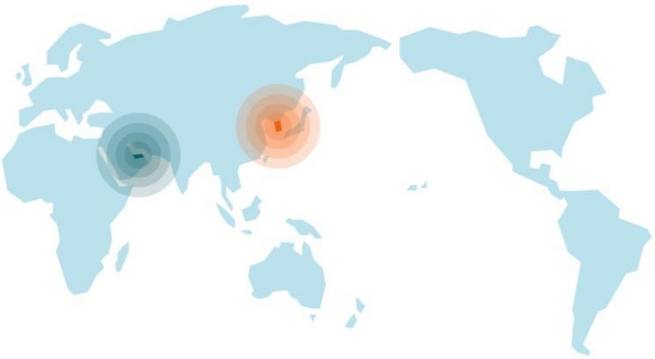
경기도 용인시 기흥구 탑실로 46,
미래에너지기술연구소 본관
+82-31-8005-5618

미래에너지기술연구소 신관

경기도 용인시 기흥구 탑실로 44,
미래에너지기술연구소 신관
+82-31-8005-8236

UAE 아부다비 지사

#2335, Sky Tower, Al Reem Island PO Box 5101041,
Abu Dhabi, UAE
+971-2-406-9719



THANK YOU

FNC TECHNOLOGY CO., LTD.