Cyber Threat Response System Design and Test Environment

Taewoo Tak, Taejin Kim, Young Jun Lee
Korea Atomic Energy Research Institute

Presenter: Taewoo Tak (ttwispy@kaeri.re.kr)

November 03-07, 2024

Ⅰ Research Necessity and Overview

01. Necessity of Research

02. Scope of Research

03. Contents of Research

Development of core technologies for detecting and responding to cyber threats based on intelligent information technology

- Development of technologies for detecting and responding to cyber threats in nuclear power plants

- Development of AI detection algorithms and simulation-based attack packet generation technologies for Nuclear power plants

- Design of a cyber threat response system for nuclear power plants

01. Necessity of Research

□ Internal-External Risk factors in operating a NPPs (Nuclear Power Plants)

- External Risks Factors: (1) Earthquake, (2) Typhoon(strong wind, heavy rain), (3) Aircraft collision, (4) Tsunami(earthquake, storm), (5) Cyber threats

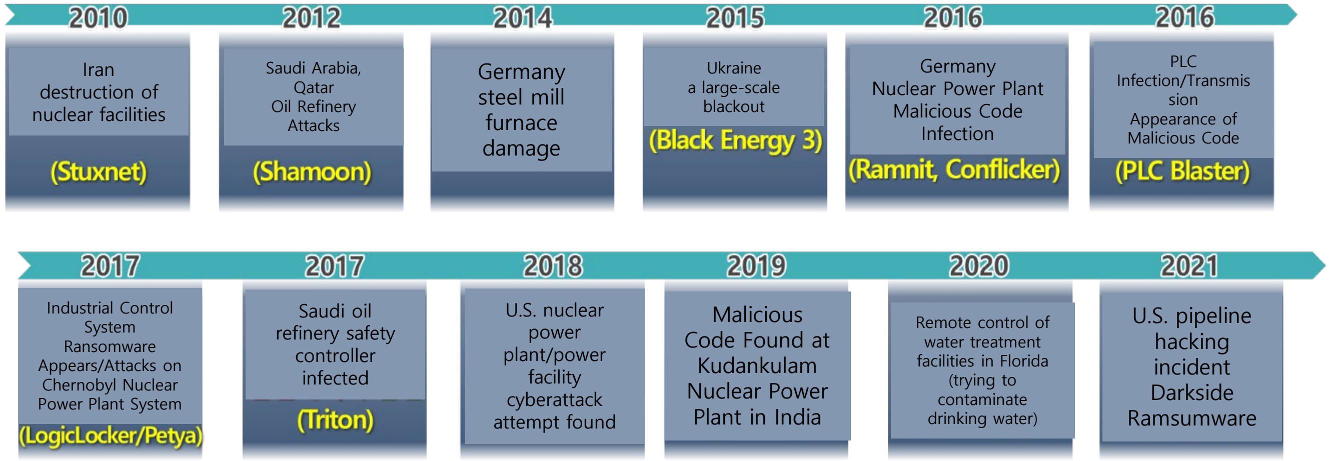
Risk Facors		Limitations in Response	Issues if Unresolved
External	Earthquake	Domestic seismic characteristics and structural deterioration not considered	Loss of core equipment, emergency power supply system, and reactor building function due to an earthquake exceeding design basis
	Typhoon/Tsunami	Stress tests not considering domestic characteristics	Loss of heat removal source on primary/secondary side due to external disasters exceeding design basis (tsunami, storm surge, etc.)
	Aircraft	Vibration and internal fire potential due to aircraft collision not considered	Damage to internal system equipment due to vibration, internal fire caused by leaked aviation fuel upon collision
	Multiple Units	Accident management focused on single unit	Simultaneous core damage and progression to severe accident for multiple units on site
	Cyber Threats	Lack of cybersecurity technology for nuclear power plant systems	Operational errors, power reduction, unexpected shutdowns, abnormal states, loss of safety system functions
Internal	Long-term Operation	Inadequate monitoring and performance degradation assessment system for aging core equipment/components, lack of accident analysis technology considering material characteristics	Potential radioactive material leakage and progression to design basis accident due to core equipment damage, increased likelihood of fuel assembly damage and radioactive material leakage due to loss of internal structural component support capability
	Human Error	Despite preparation of procedures and training, human error accounts for about 47% of all accidents/failures	Increased likelihood of unexpected shutdowns due to operator judgment/response errors in normal/abnormal operation procedures, potential progression to accident state/severe accident
	Fire Protection	Conservative evaluation using US fire characteristics information.	Core damage and severe accident due to failure of fire safety shutdown

01. Necessity of Research

□ **Increasing cyber threats to major infrastructure** including domestic and international a NPP.

□ **New types of threats** due to the advancement of cyber threat technologies.

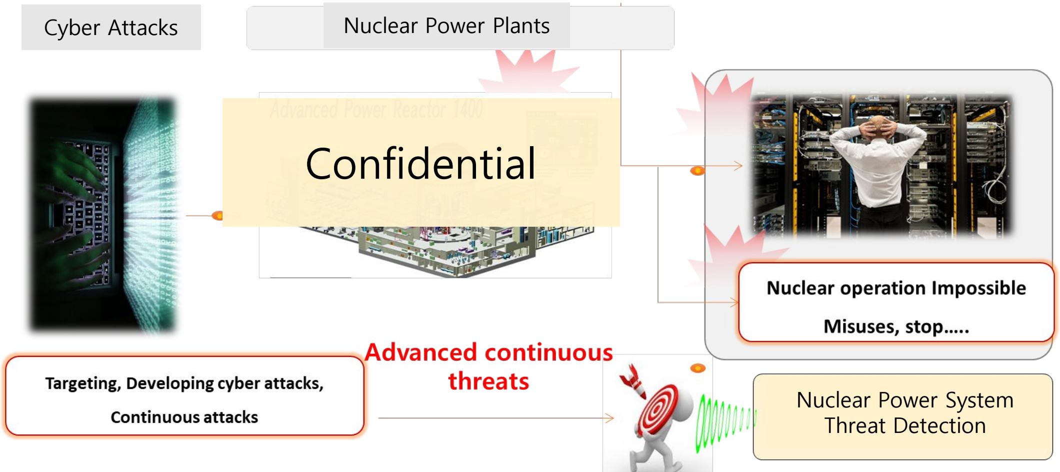
- **Cyber threats** targeting Industrial Control Systems (**ICS**) are highly **sophisticated** and **intelligent**, often prepared over several years (APT, Advanced Persistent Threats).
- Intelligent and complex cyber-attacks such as **manipulation of sensor signals/control logic** and **modification of HMI** (Human Machine Interface) information.
- **Difficult to detect intelligent cyber-attacks** on ICS with only IT security technologies → necessitating **specialized detection technologies** for nuclear power plant systems.



2010	2012	2014	2015	2016	2016
Iran destruction of nuclear facilities (Stuxnet)	Saudi Arabia, Qatar Oil Refinery Attacks (Shamoon)	Germany steel mill furnace damage	Ukraine a large-scale blackout (Black Energy 3)	Germany Nuclear Power Plant Malicious Code Infection (Ramnit, Conflicker)	PLC Infection/Transmission Appearance of Malicious Code (PLC Blaster)

2017	2017	2018	2019	2020	2021
Industrial Control System Ransomware Appears/Attacks on Chernobyl Nuclear Power Plant System (LogicLocker/Petya)	Saudi oil refinery safety controller infected (Triton)	U.S. nuclear power plant/power facility cyberattack attempt found	Malicious Code Found at Kudankulam Nuclear Power Plant in India	Remote control of water treatment facilities in Florida (trying to contaminate drinking water)	U.S. pipeline hacking incident Darkside Ramsumware

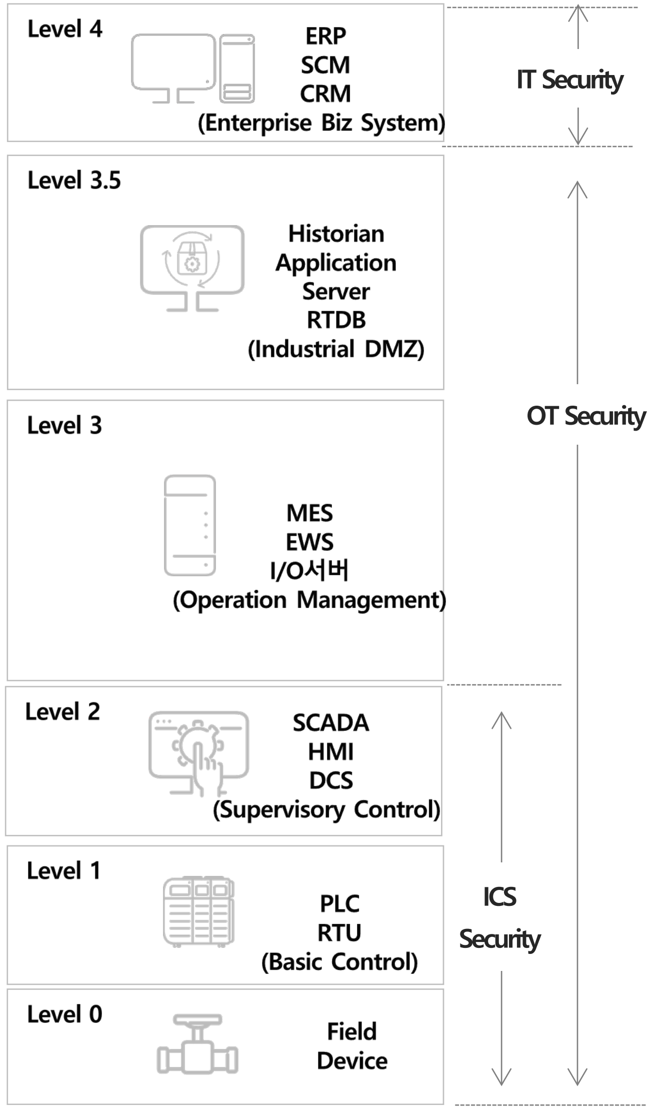
<Cyber threat of major infrastructure such as nuclear facilities >


Cyber Attacks
Nuclear Power Plants
Advanced Power Reactor 1400
Confidential
Nuclear operation Impossible
Misuses, stop…..
Targeting, Developing cyber attacks,
Continuous attacks
Advanced continuous threats
Nuclear Power System Threat Detection

<Cyber Threat Detection Function Need to Nuclear Facility>

01. Necessity of Research

□ Technology for detecting Level 0~2 cyber threats is under development

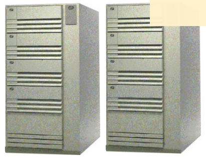


NO KINAC Regulatory Target

KINAC Regulatory Target(SSEP)

"Unique design and platform usage for each site (Cooperation from designers, operators, and device manufacturers is essential for the development and application of security features)."

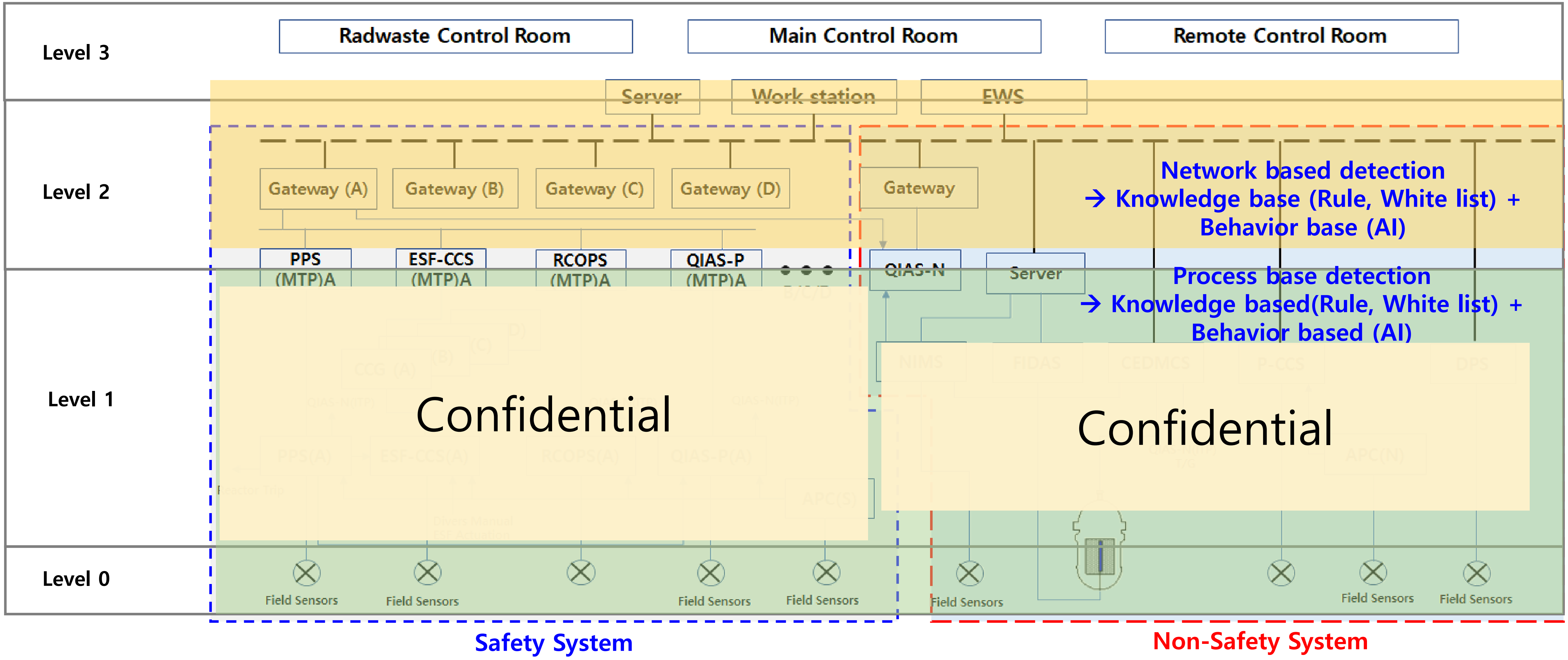
Confidential



02. Scope of Research

□ Research on Power Plant Information : Design and Operation Information-Based Detection Technology Research (Focusing on Safety System Process Information)

□ Research on the Applicability of Innovative Technologies : Deriving new technology utilization plans through the application of AI technology



Level 3

Radwaste Control Room

Main Control Room

Remote Control Room

Server

Work station

EWS

Level 2

Gateway (A)

Gateway (B)

Gateway (C)

Gateway (D)

Gateway

Network based detection
→ Knowledge base (Rule, White list) + Behavior base (AI)

PPS (MTP)A

ESF-CCS (MTP)A

RCOPS (MTP)A

QIAS-P (MTP)A

• • •

QIAS-N

Server

Level 1

Process base detection
→ Knowledge based(Rule, White list) + Behavior based (AI)

Confidential

Confidential

Level 0

Field Sensors

Field Sensors

Field Sensors

Field Sensors

Field Sensors

Field Sensors

Field Sensors

Safety System

Non-Safety System

02. Scope of Research

□ Detection System Configuration

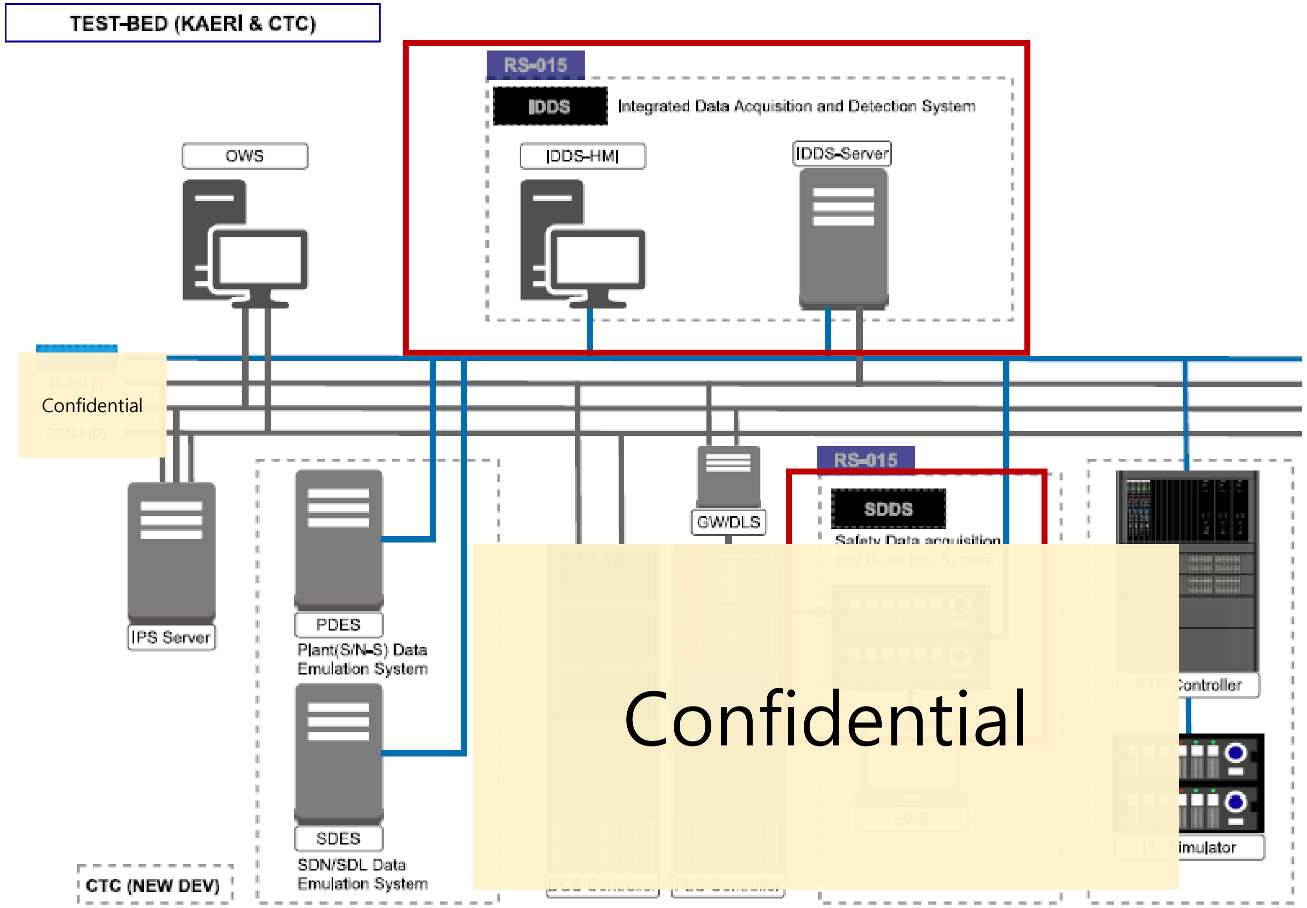
- IDDS
  - IPS Network Threat Detection in Level2
  - IPS Network AI based Threat detection in Level2
  - Non-safety Logic based threat detection
  - Process signal AI based threat detection
- SDDS
  - Safety System Network threat detection in Level1
  - Safety System Logic based threat detection

□ Implement Detection System

- SDDS/IDDS Hardware Implementation
- Level 1/2 Data Interfacing Implementation
- Data Emulation

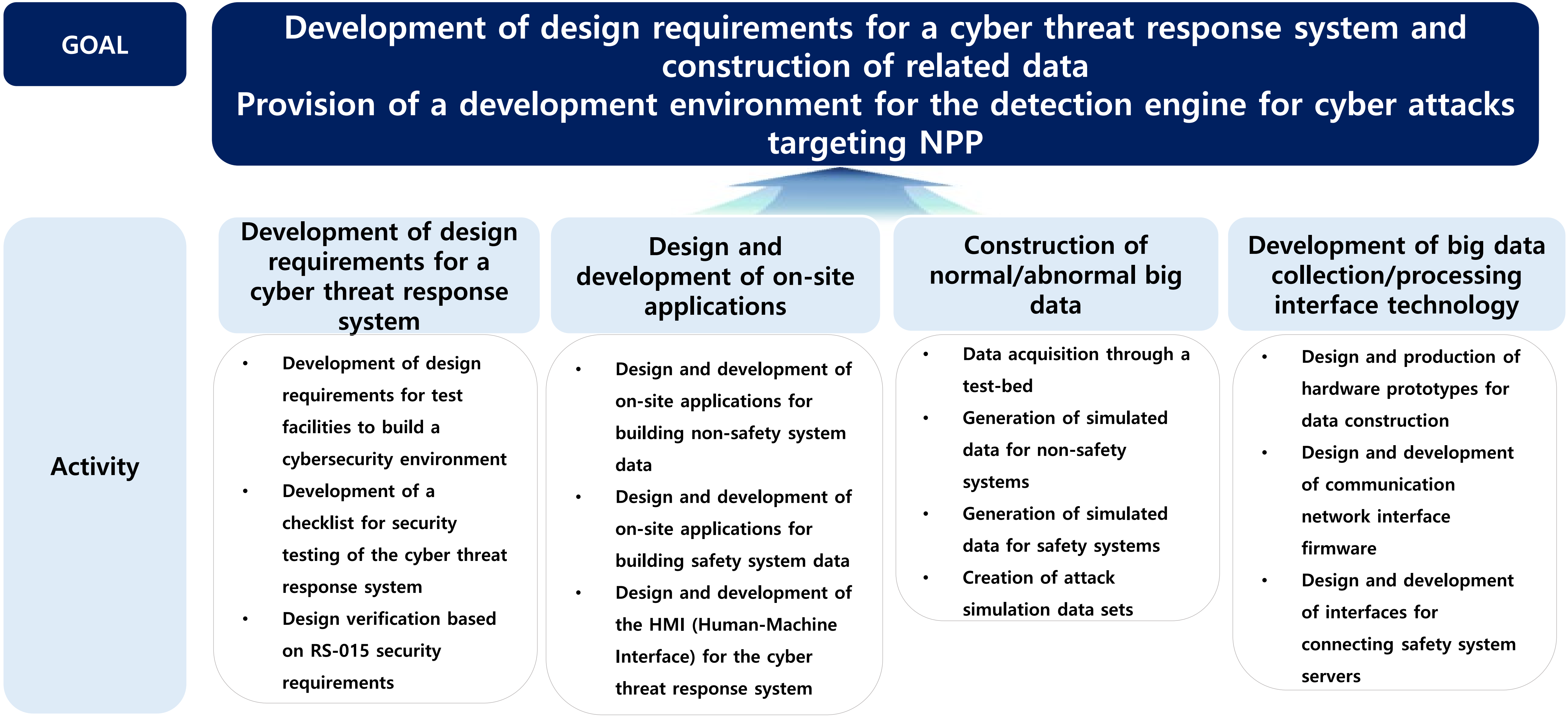
□ Detection system Testing

- Threat Scenario development and threat data generation



<KAERI TEST-BED based Detection system configuration>

03. Contents of Research



GOAL

Development of design requirements for a cyber threat response system and construction of related data
Provision of a development environment for the detection engine for cyber attacks targeting NPP

Activity

Development of design requirements for a cyber threat response system

- Development of design requirements for test facilities to build a cybersecurity environment
- Development of a checklist for security testing of the cyber threat response system
- Design verification based on RS-015 security requirements

Design and development of on-site applications

- Design and development of on-site applications for building non-safety system data
- Design and development of on-site applications for building safety system data
- Design and development of the HMI (Human-Machine Interface) for the cyber threat response system

Construction of normal/abnormal big data

- Data acquisition through a test-bed
- Generation of simulated data for non-safety systems
- Generation of simulated data for safety systems
- Creation of attack simulation data sets

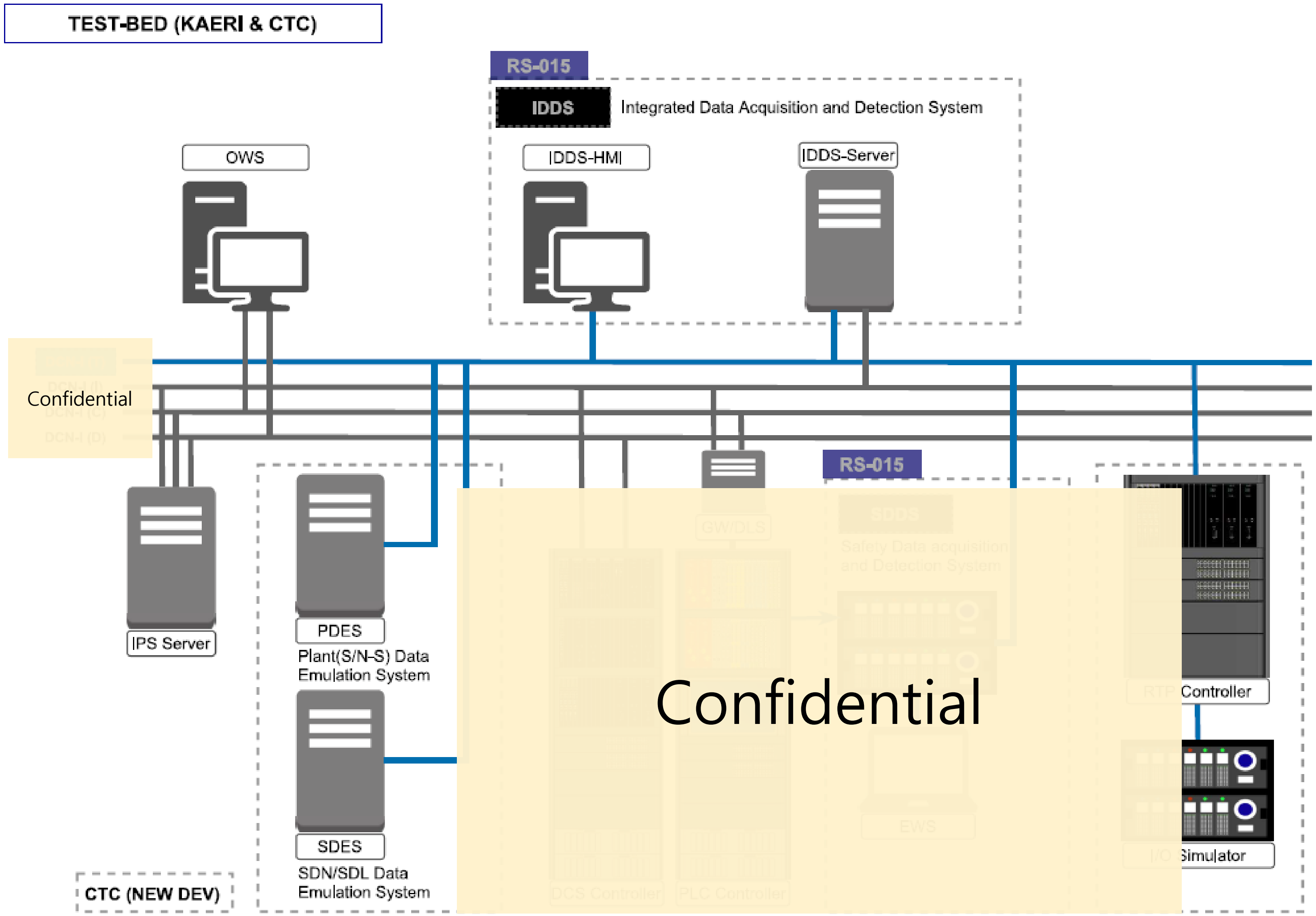
Development of big data collection/processing interface technology

- Design and production of hardware prototypes for data construction
- Design and development of communication network interface firmware
- Design and development of interfaces for connecting safety system servers

03. Contents of Research

□ System Configuration

- **IDDS**(Integrated Data Acquisition and Detection System)
- **SDDS**(Safety Data acquisition and Detection System)
- **PDES** (Plant (S/N-S) Data Emulation System)
  - Safety/Non-Safety Emulation S/W
- **SDES** (Data Emulation System)
  - Safety Data Emulation S/W



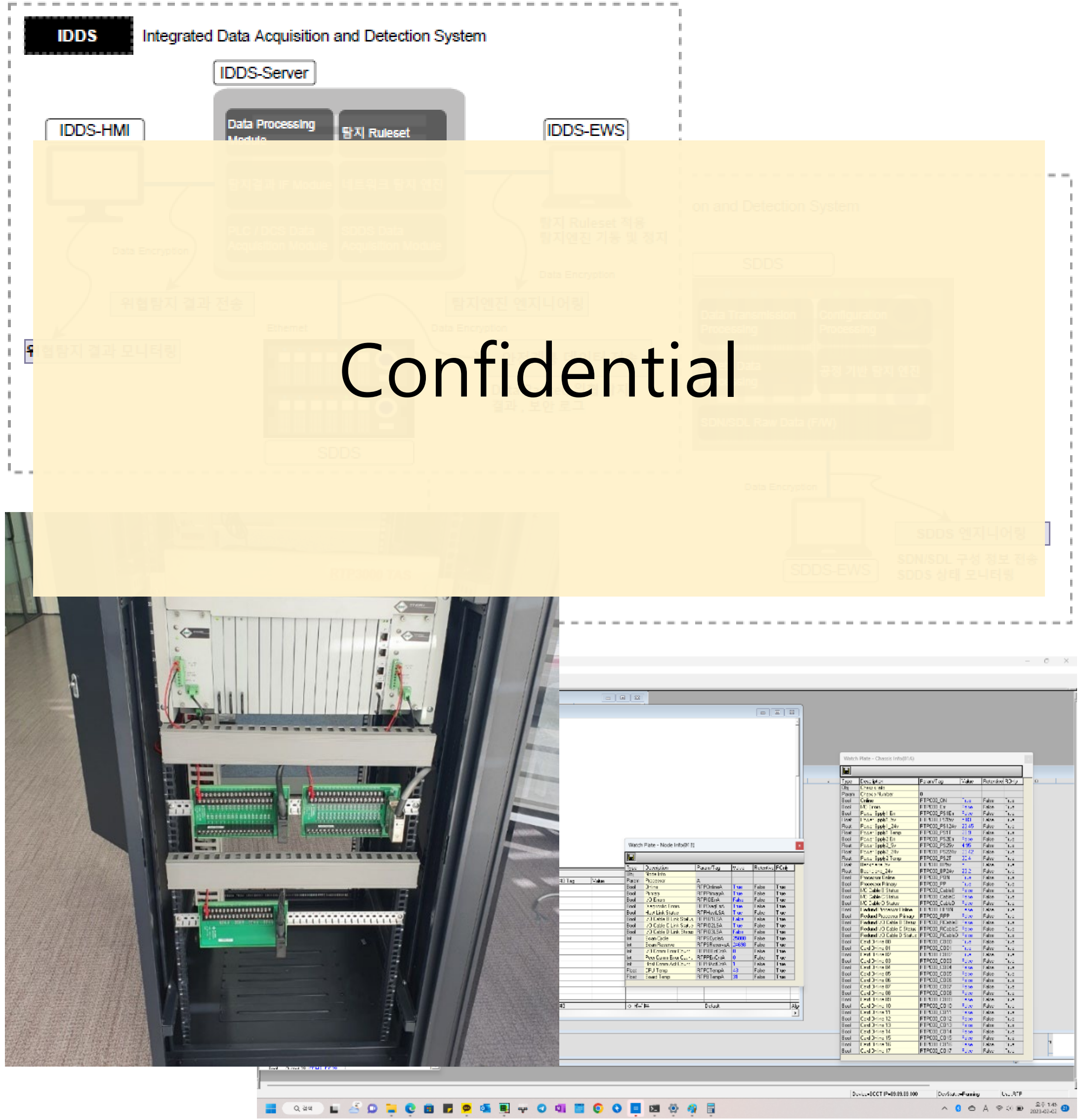
03. Contents of Research

□ **Design and development of on-site applications for building non-safety system data**

- Design and development of IDDS HMI and interface modules
  - Design for data interface and display of detection information
- Design and development of the IDDS SERVER
  - Preparation of requirements and design documents based on RS-015 security requirements
  - Design and development of MDB, ALARM, and HDSR functions
- Design and development of SDDS / IDDS EWS
  - Preparation of requirements and design documents based on RS-015 security requirements
  - Design and development of engineering tools for SDDS and network-based detection engines

□ Design and production of non-safety systems based on RTP

- Design and development of I/O Simulator software

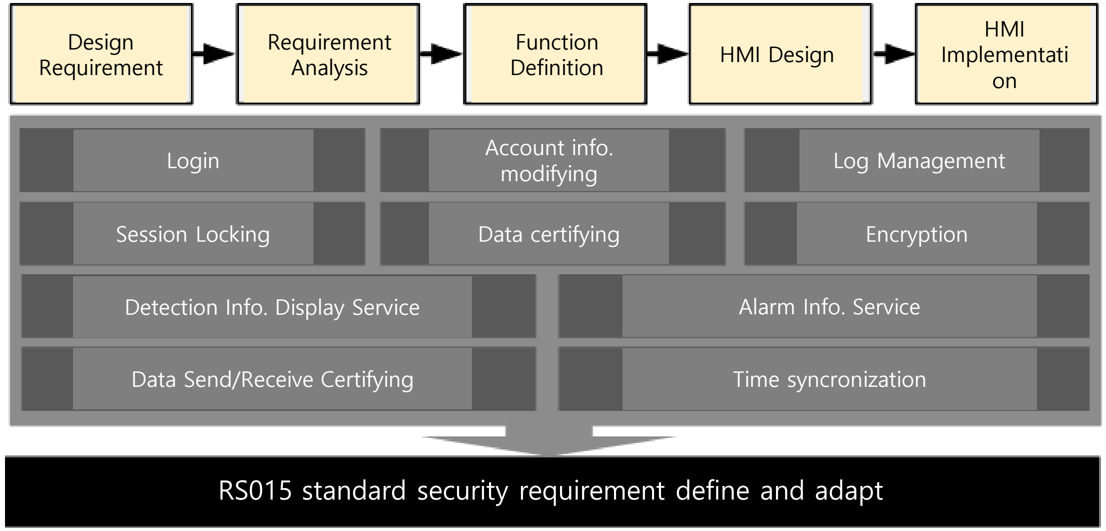


Confidential

03. Contents of Research

□ Design and development of the HMI (Human-Machine Interface) for the cyber threat response system

- Implementation of the cyber threat detection HMI
  - Design, implementation, and verification of symbol functionality/process screens
  - Design of display screens for network-based detection results
  - Design of display screens for process-based detection results
- HMI design for implementing cyber detection screens



Design Requirement → Requirement Analysis → Function Definition → HMI Design → HMI Implementation

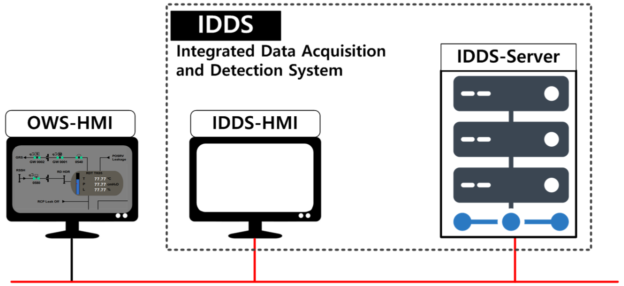
Login | Account info. modifying | Log Management

Session Locking | Data certifying | Encryption

Detection Info. Display Service | Alarm Info. Service

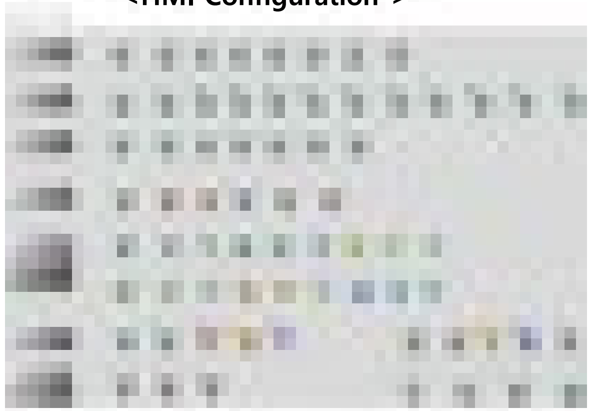
Data Send/Receive Certifying | Time syncronization

RS015 standard security requirement define and adapt

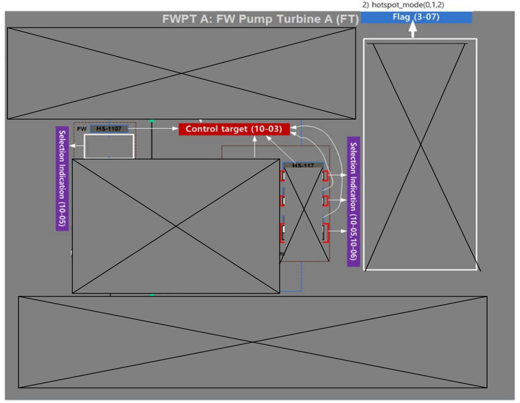


<HMI Configuration >

<Symbol Function Design>

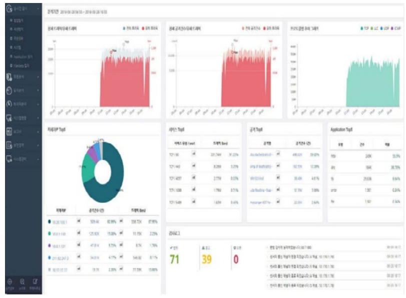


<Symbol Function Verification >

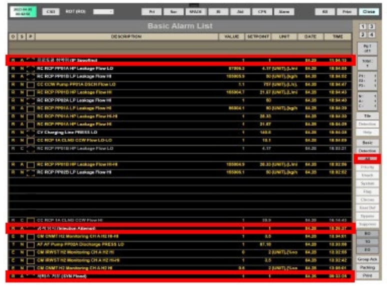

FWPT A: FW Pump Turbine A (FT)
Flag (3-07)
Control target (10-03)
FW
HS-1107
Selection Indication (10-05)
Selection Indication (10-05,10-06)

<Process Display Design>

<Process Display Verification>



<Network, Detection Display>

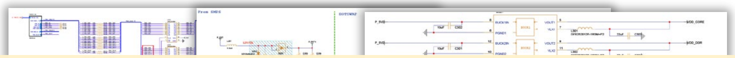


<Detection Alarm Display>

03. Contents of Research

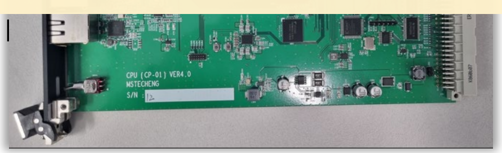
□ Interface Design and Development for safety system server connection.

- Hardware Design for server connection



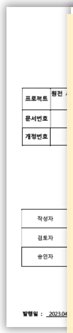
Confidential

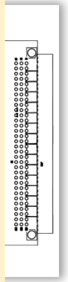
for server interface (manufactu



□ Hardware prototype design and manufacture for safety system data implementation

- Interface hardware design for safety system data implementation



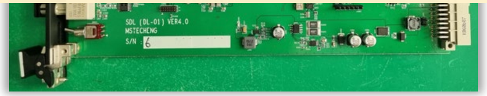


<H

Confidential

- Co

<Comm-01>



<Comm-02>

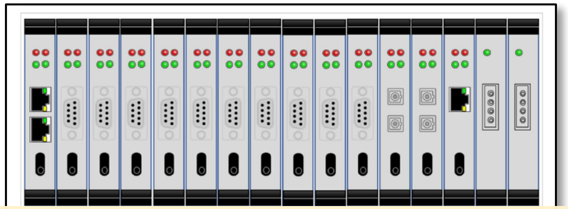
03. Contents of Research

□ **Design and development of communication network interface system firmware for building a safety system data**

- System firmware development (kernel/device driver: boot config Device Driver, and 17 other items, Firmware: Configuration Module and 6 other types)

□ **Other items**

- System integration and implementation



Confidential

<Prototype Production>

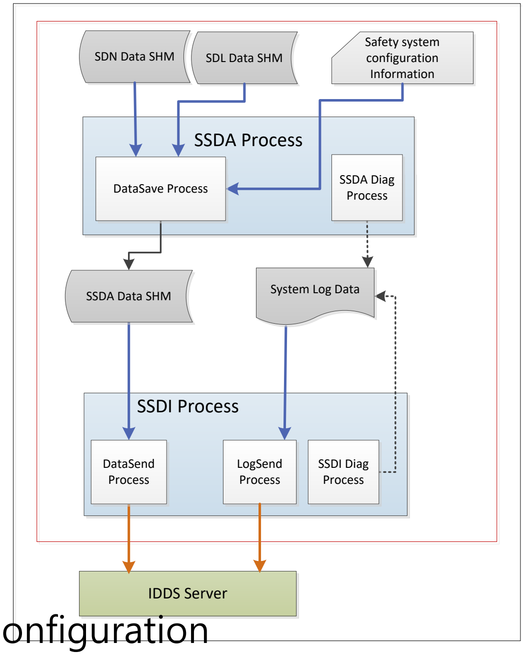
- Patent Application: Safety System Communication Network Interface and Nuclear Power Plant Cybersecurity System and Method Using the Same

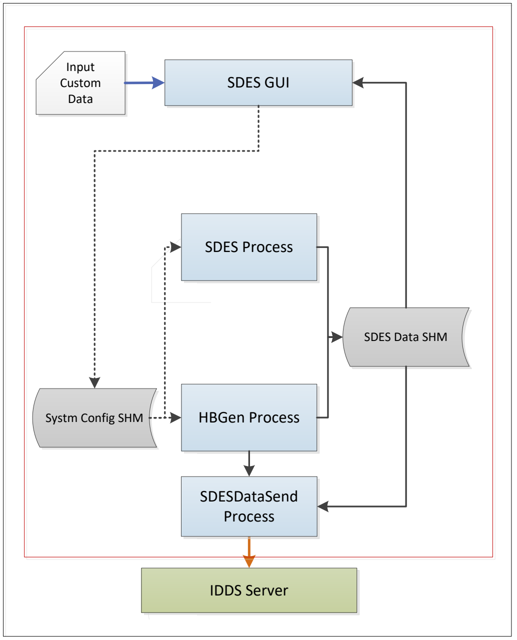
Confidential

03. Contents of Research

□ Cyber Threat Response System Design and Implementation (Safety System)

- Collect/Process and Interface SW detailed design and implementation for Safety System Data Construction
  - SSDA Process , SSDI **Process Module Configuration**
  - SDDS receive SDN/SDL Data collection
  - Data collect and interface process diagnosis log collection
  - Data and diagnosis log data encryption send
  - Shared memory data architecture and comm. Protocol definition





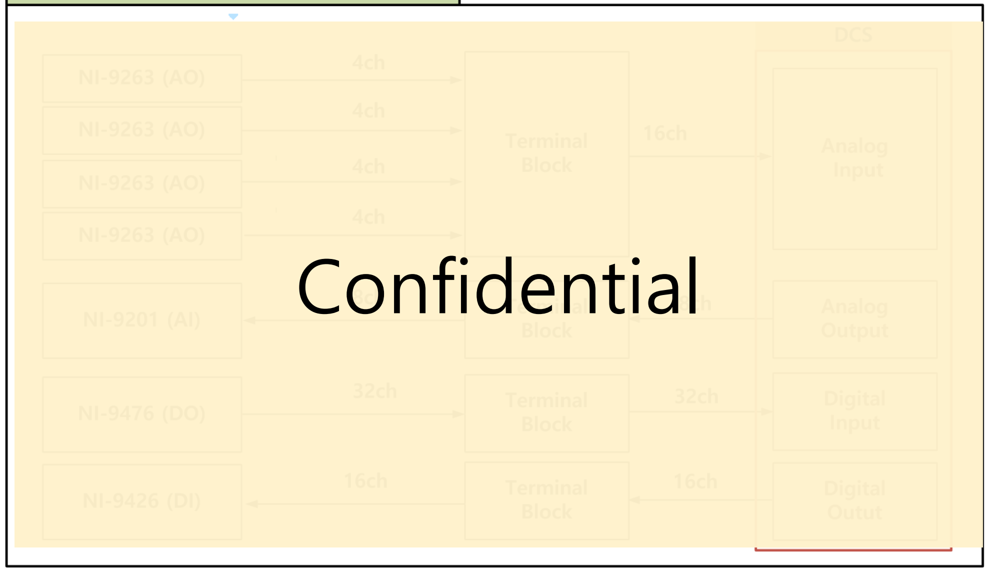
- **Safety Data Emulation SW detailed design and development**
  - SDES GUI, SDES Process, HBGen Process, SDESDataSend Process modules configuration
  - Controller SDN/SDL input signal and output signal emulation / HeartBeat signal emulation
  - Emulation data monitoring
  - Emulation data encryption sending
  - Shared memory data architecture and communication protocol definition

03. Contents of Research

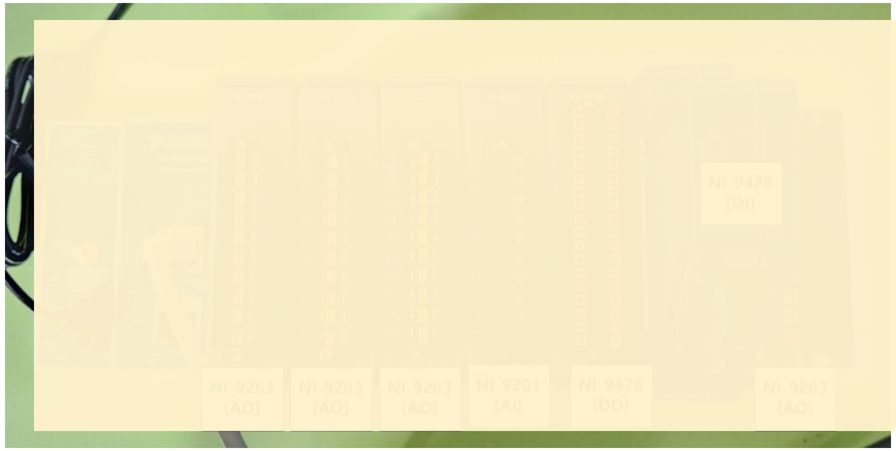
□ I/O Hardware implementation and SW development for safety sy signal emulation

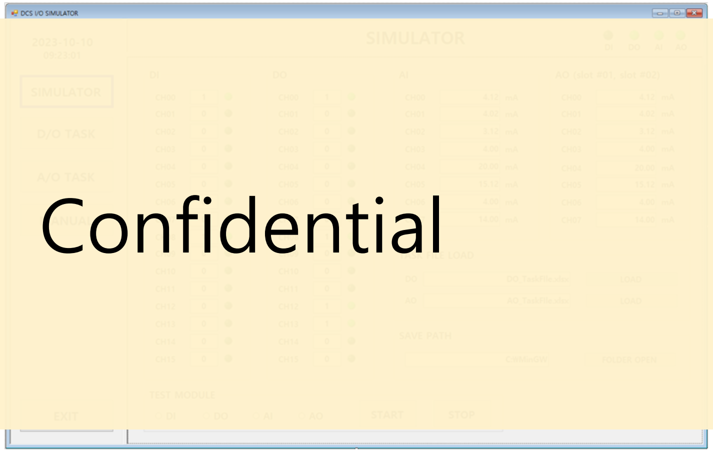
- **Hardware implementation**
  - DI(16 channels), DO(32 channels), AI(8 channels), AO(16 channels)
- **SW development**
  - Safety system auto operation mode using working file loading function
  - System signal manual operation mode for each bit control
  - Testing process file auto save function and trend analysis function

cDAQ-9189 (8 slot) (for DCS)

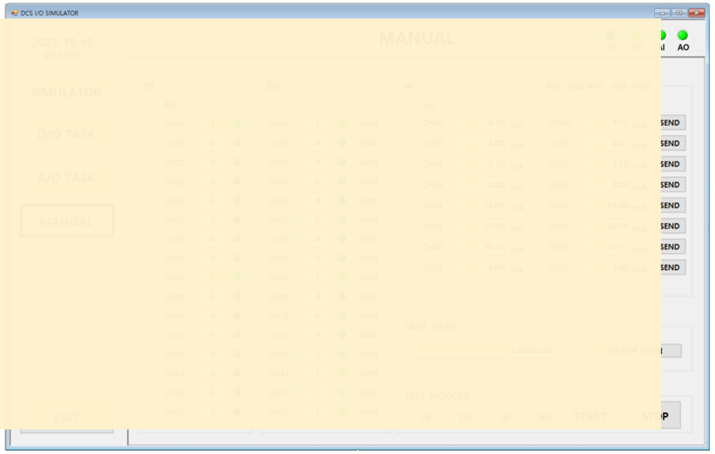


Confidential





Confidential



03. Contents of Research

□ **Safety/Non-safety system data emulation SW design for Normal/Abnormal Big Data**

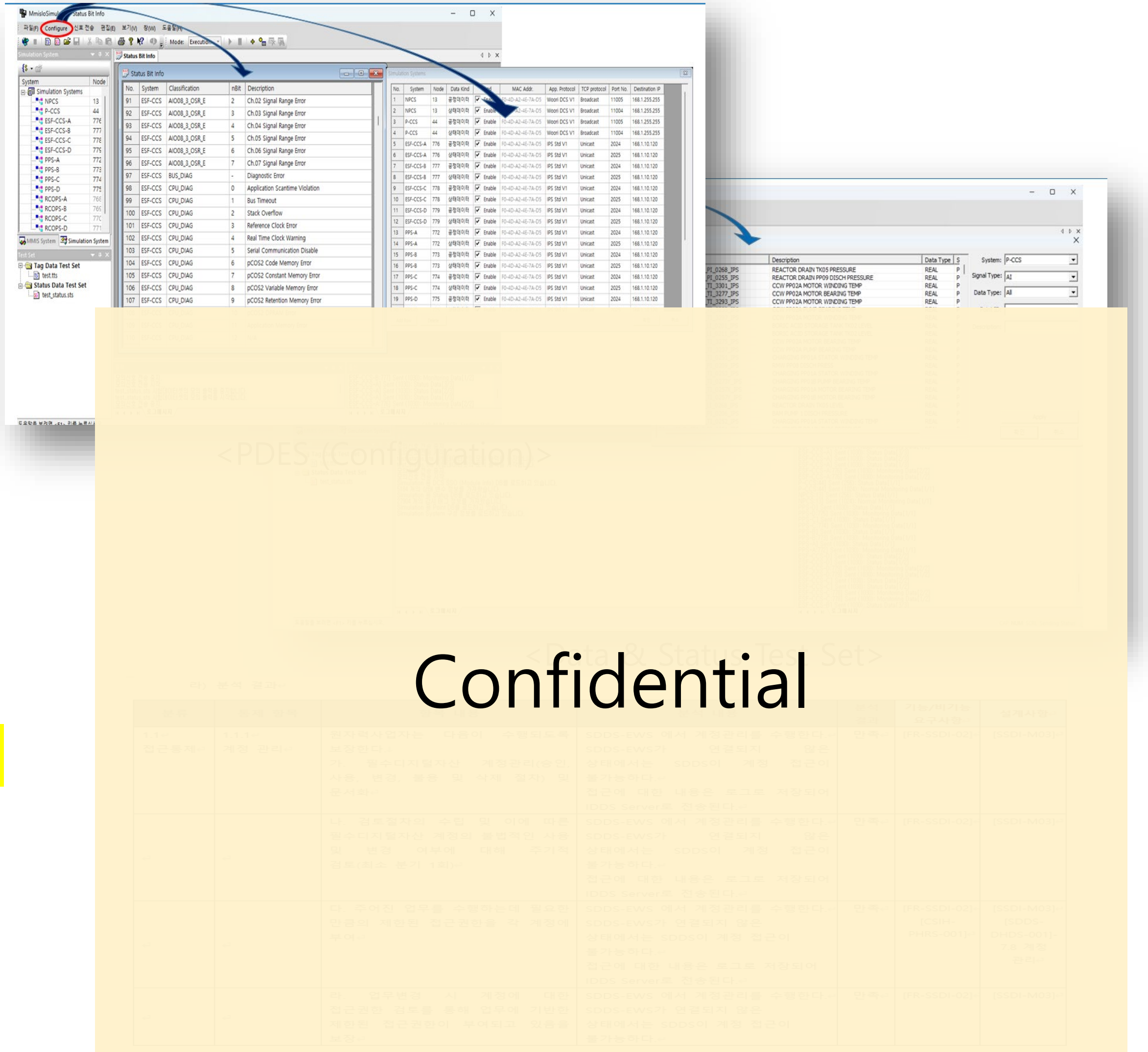
- Safety/Non-safety system emulation SW design and development
- Testing environment support and Test-Bed interface installation

□ **Interface SW design and development for Big data of non-safety system**

- API support to generate data with safety/non-safety scenarios

□ **Cyber threat response system regulation requirement design verification**

- **RS-015 security regulation and secure features design verification** (Requirement Specification, System Design, Requirement Traceability Matrix

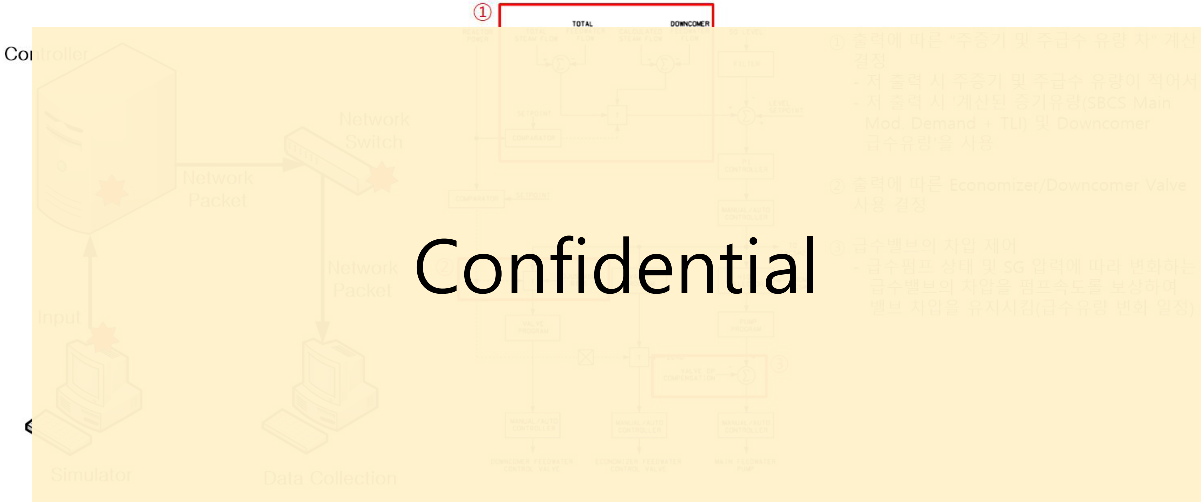


<Requirement RTM based RS-015 security regulation>

03. Contents of Research

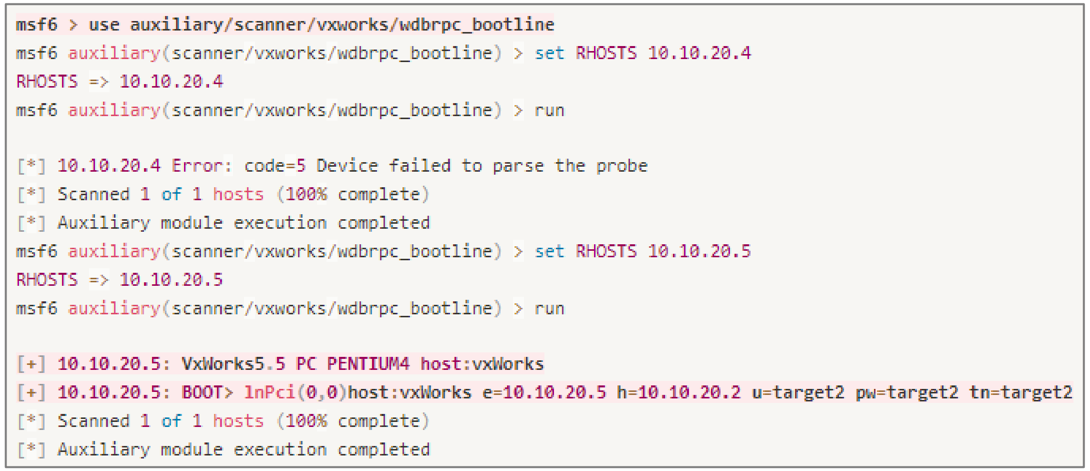
□ Normal/Abnormal data generation scenario design based Distributed Control System

- Cyber attack environment setting of DCS OS
  - Nuclear non-safety system(FWCS) target set and analysis
  - Process and Network data collect environment set
- Cyber attack scenario design of DCS
  - Attack scenario design based DCS OS vulnerability
  - Attack scenario design based DCS operation environment
- Cyber attack make and analysis of
  - Exploit make for cyber attack
  - Process and Network data collect after cyber attack with scenarios



<process and network data collect environment>

<Nuclear non-safety system target set and analysis>



```
msf6 > use auxiliary/scanner/vxworks/wdbrpc_bootline
msf6 auxiliary(scanner/vxworks/wdbrpc_bootline) > set RHOSTS 10.10.20.4
RHOSTS => 10.10.20.4
msf6 auxiliary(scanner/vxworks/wdbrpc_bootline) > run

[*] 10.10.20.4 Error: code=5 Device failed to parse the probe
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vxworks/wdbrpc_bootline) > set RHOSTS 10.10.20.5
RHOSTS => 10.10.20.5
msf6 auxiliary(scanner/vxworks/wdbrpc_bootline) > run

[+] 10.10.20.5: VxWorks5.5 PC PENTIUM4 host:vxWorks
[+] 10.10.20.5: BOOT> lnPci(0,0)host:vxWorks e=10.10.20.5 h=10.10.20.2 u=target2 pw=target2 tn=target2
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

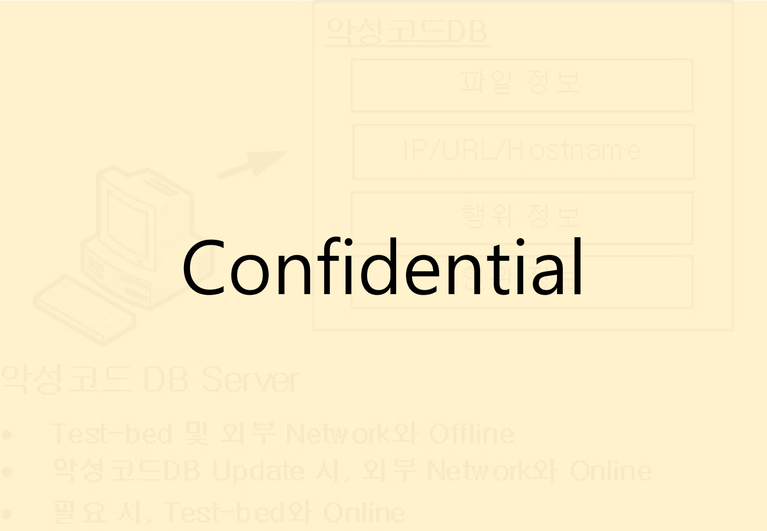
<Cyber attack action>
(OS vulnerability)

03. Contents of Research

□ **Normal/Abnormal deriving threat information (malicious code) collecting device and DB design**

- **OS vulnerability analysis of major system in Test-Bes**
  - Nuclear system safety/non-safety OS vulnerability analysis
  - Nuclear system server OS vulnerability analysis
- **DB design for malicious code data**
  - Malicious code survey/collect based predefined OS
  - Malicious DB architecture design based surveyed malicious code

<Malicious code DB architecture>



Confidential
악성코드DB
파일 정보
IP/URL/Hostname
행위 정보
악성코드 DB Server
Test-bed 및 외부 Network와 Offline
악성코드DB Update 시, 외부 Network와 Online
필요 시, Test-bed와 Online

□ **Development Program(SDDS/IDDS) SW function verification**

- SW function verification for safety system program
  - Verification methods setting for SDDS SW
  - Verification perform for SDDS SW
- SW function verification for non-safety system program
  - Verification methods setting for IDDS SW
  - Verification perform for IDDS SW

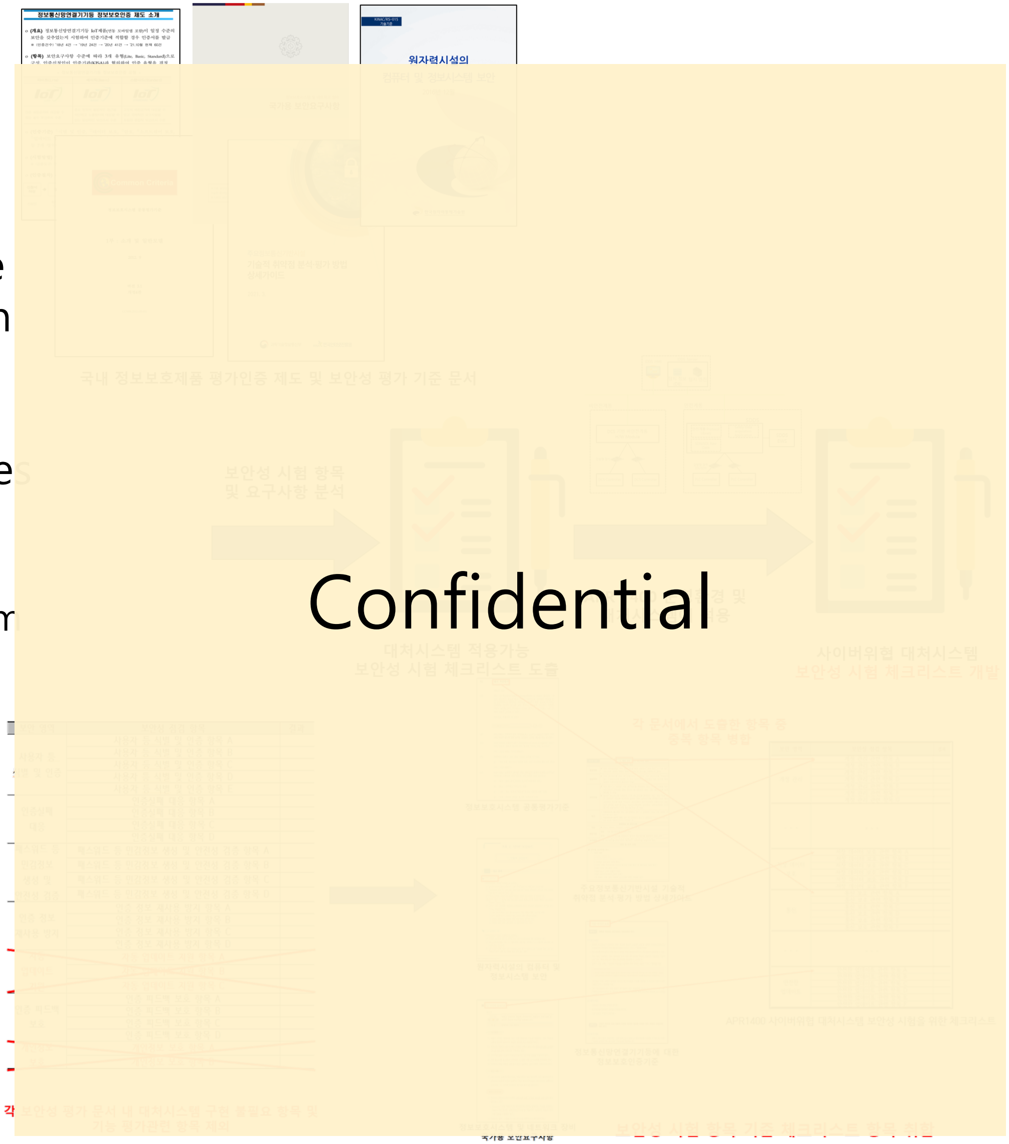
Traceability	IEEE Std. 1012	Interface Analysis
Correctness	Correctness	Correctness
Consistency	Consistency	Consistency
Completeness	Completeness	Completeness
	Accuracy	Rightness
	Readability	Testability
	Testability	

<SW function verification and validation methodology>

03. Contents of Research

□ Development of a checklist for testing the security of systems for dealing with cyber threats

- Research and analysis of security testing for intrusion detection systems within the domestic information protection product evaluation and certification system.
- Derivation of security test checklist items applicable to cyber threat response systems
  - Providing criteria for items excluded from evaluation and certification systems and security evaluation documents
- Development of a security test checklist by compiling security test items derived from each document
  - Categorizing security test items into areas such as security audit, communication, cryptographic support, user data protection, identification and authentication, security management, system security functions, resource utilization, system access management, and secure path/channel

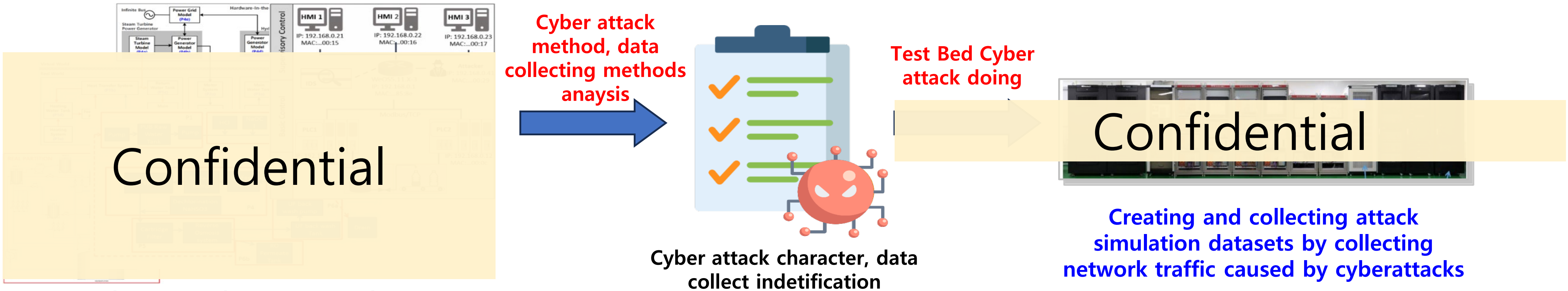


Confidential

03. Contents of Research

□ Development of an attack simulation dataset for testing cyber threat response systems

- Case study on using an attack simulation dataset for performance testing of anomaly detection systems targeting con trol systems
- Development of an attack simulation dataset for detection performance testing of cyber threat response systems
  - Analysis of cyber attack execution methods and data collection strategies for control system testbeds through case analysis of each attack simulation dataset
  - Completion of analysis on six datasets, including the National Security Research Institute's HIL (Hardware-in-the-Loop) based augmented ICS (HAI) testbed dataset



Attack scenario dataset gen. and utilization analysis

Cyber attack character, data collect indetification

Creating and collecting attack simulation datasets by collecting network traffic caused by cyberattacks

Thank you.