고려대학교
KOREA UNIVERSITY

Manufacturing Security in Korea

2021. 01. 28.

Keunhee Han
Korea University
Graduate School of Information Security

고려대학교
KOREA UNIVERSITY

Contents

I Smart Factory Status in Korea

II Apply Security Requirements in SMEs

III R&D Activities on ICS Security

IV Q & A

Smart Factory Status in Korea

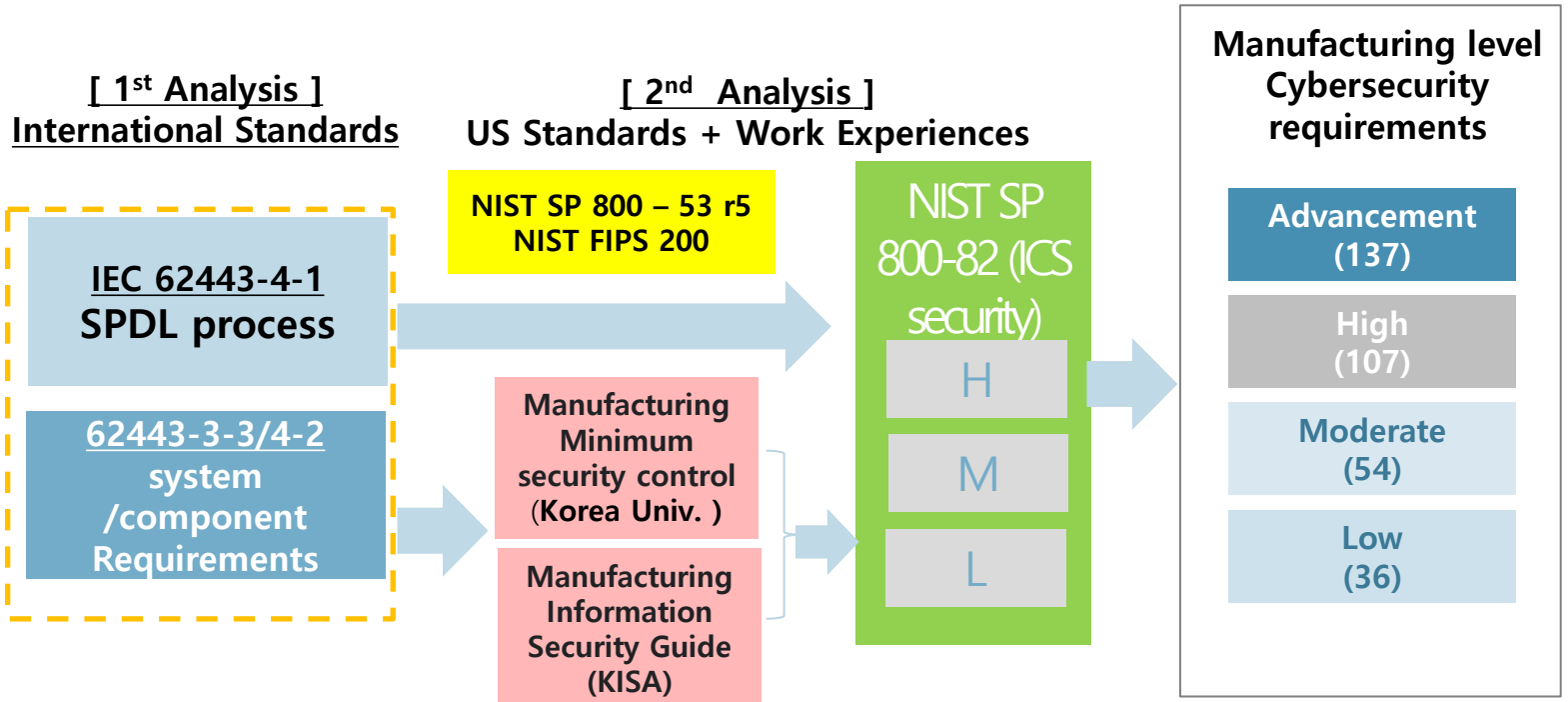
Consideration Criteria

- Manufacturing technology protection requirement groups in SMEs
- Sales Volume:
  - 1458 companies (29.1%) above 10 million (USD) and below 30 million (USD).
  - 972 companies (19.4%) above 5 million (USD) and below 10 million (USD).
- Company size:
  - 2620 companies (52.4%) above 10 people and below 50 people.
  - 987 companies (19.7%) above 50 people and below 100 people
- Systems: MES 74.6%, ERP 13.5%

Manufacturing technology protection output/formulation

❑ Minimum requirement of Manufacturing security policy

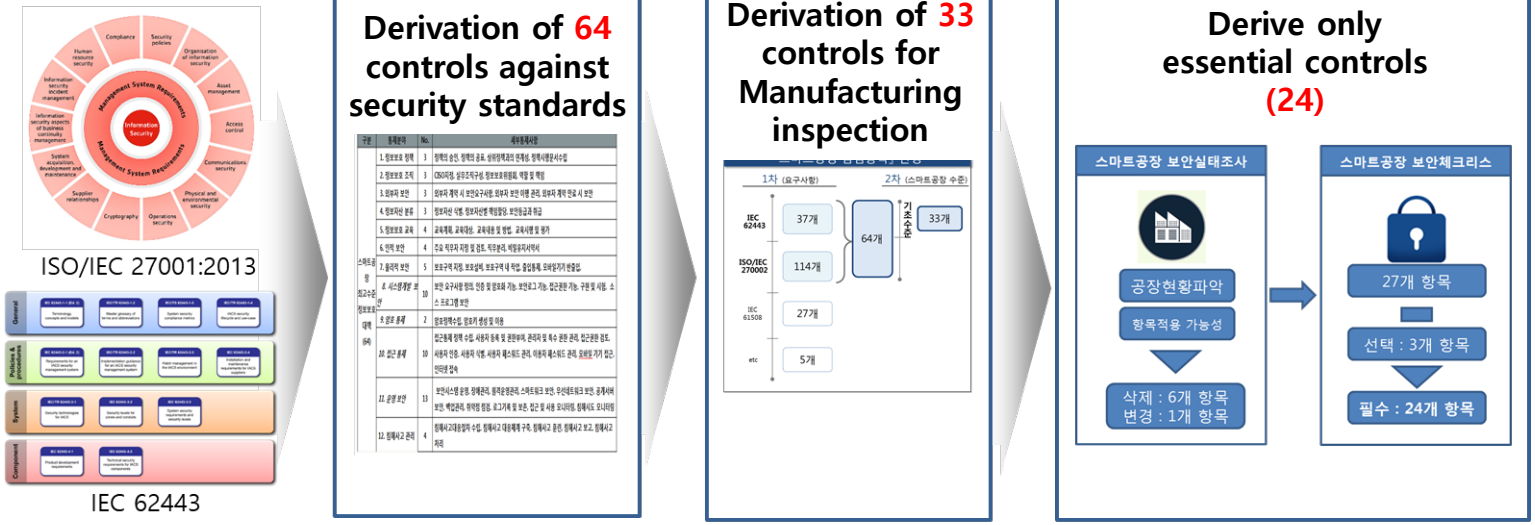
- Bring the output based on the IEC 62443
- Apply "Minimum requirement of Manufacturing security policy" and "Manufacturing information security guide".
- In order to apply security measurement, it should be apply NIST SP 800-82.



Analysis of domestic guidelines at 2016

❑ Manufacturing Minimum Security Principle

- **Considering the size and sales of the company, the management, physical, and technical security controls are derived by level, and a guide for the minimum security level required in a Manufacturing is presented.**



Analysis of domestic and foreign security requirements

Manufacturing security level 3 (High level)

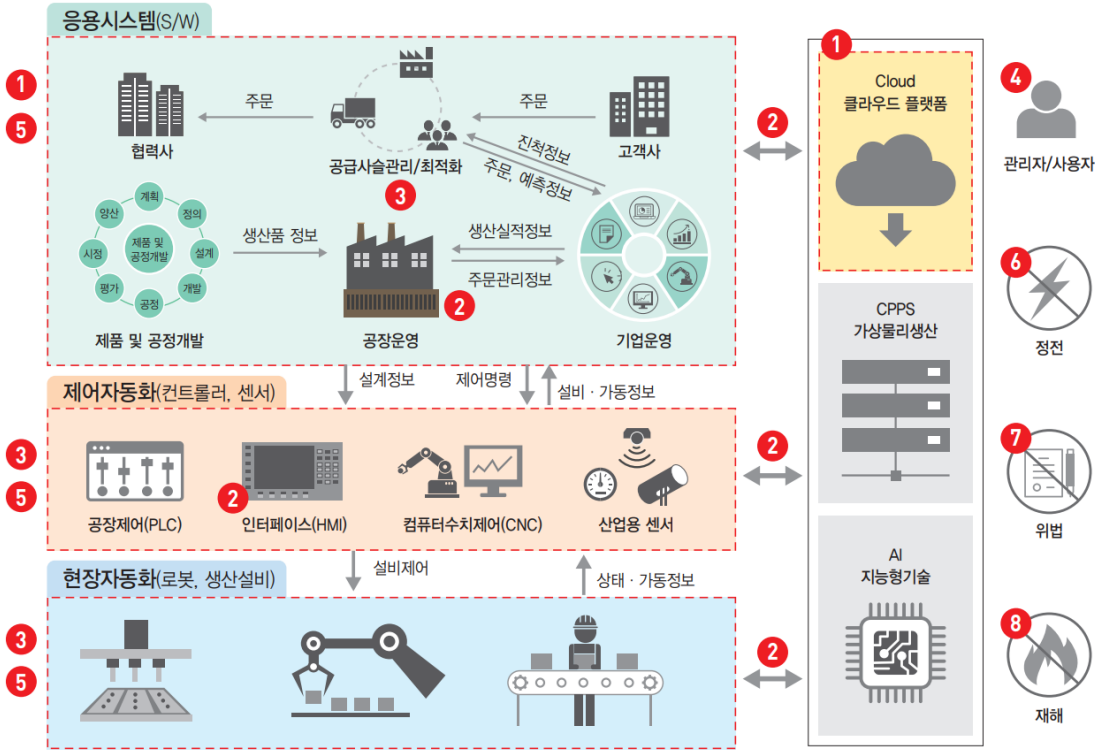
Manufacturing security level 2 (Moderate level)

Manufacturing security level 1 (Basic level)

Analysis of domestic guidelines at 2019

❑ Manufacturing Cyber Security Guide

< Manufacturing Security Threat >



1. Malicious activity
2. Wiretapping
3. Physical attack
4. Accident
5. Breakdown/malfunction
6. blackout
7. Illegality
8. Disaster

< Manufacturing Security Requirements >

Security requirements	Controls
Access control	11
Information Security Operation Policy and Procedure	8
Data protection	5
Safe state	4
Asset management	2
Security accident prevention and response	4

Analysis of U.S.A guidelines

- NIST FIPS 200 (Federal Information Processing Standards Publication)
  - Minimum Security Requirements for Federal Information and Information Systems
  - Description of minimum security requirements for 17 areas

Access control(AC)	Maintenance (MA)
Security awareness training(AT)	Media Protection (MP)
Audit and Accountability (AU)	Physical and Environmental Protection (PE)
Certification, Accreditation, and Security Assessments (CA)	Planning (PL)
Configuration Management (CM)	Personnel Security (PS)
Contingency Planning (CP)	Risk Assessment (RA)
Identification and Authentication (IA)	System and Services Acquisition (SA)
Incident Response (IR)	System and Communications Protection (SC)
	System and Information Integrity (SI)

Analysis of U.S.A guidelines

❑ NIST SP 800-53 r5

- It includes 17 security areas of FIPS 200 and presents each basic security control at 3 levels (upper-moderate-lower) based on the degree of impact.

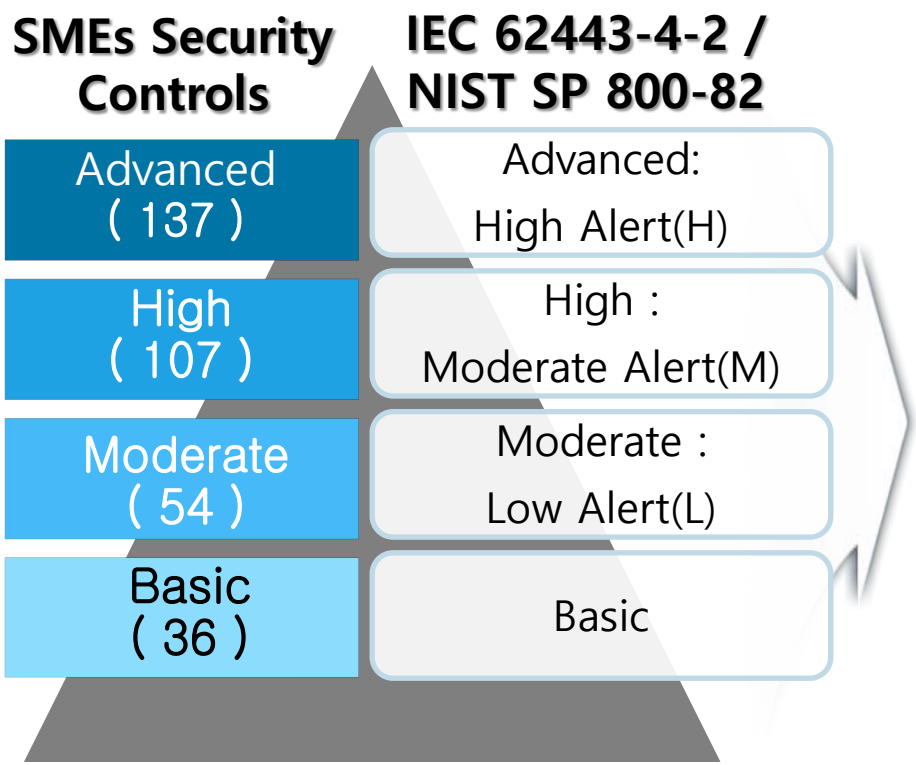
TABLE D-2: SECURITY CONTROL BASELINES[92]

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7

Derivation of technical protection requirements

❑ Technical protection requirements

- **Application of cyber security requirements from the perspective of IEC 62443-4-2, which is based on international standard technology**
- **Based on standards, reflecting national standard technology NIST SP 800-82 ICS security requirements**



Technical protection requirements	
Access control	Media protection
Security awareness training	Physical and environmental protection
audit	Plan
Evaluation and monitoring	Security program management
Setting management	Human Resources management
Emergency plan	Risk assessment
Identification and authentication	System and service purchase
Accident response	System and communication protection
Maintenance	System and information integrity

Target of SMEs ICS Security

Goal

- **Formulate the easy and efficient guide**
- **Basic level commentary**
- **Cloud considered components**
- **Basic level Manufacturing**

Develop about SME Manufacturing Security Guide

- **Project Time: June. 2020~Dec. 2020**
- **Security Requirements**
  - **Security Level 1: 36 Security Controls**
  - **Security Level 2: 54 Security Controls**
  - **Security Level 3: 107 Security Controls**
  - **Security Level 4: 137 Security Controls**

Security Level 1 (Basic) Seurity Control in Korea Model

❑ Minimum requirement of Manufacturing security policy

- **Based on the IEC 62443-4-2 / 3-3 and our experience, we applied "Minimum requirement of Manufacturing security policy" and "Manufacturing information security guide".**
- **We brought 36 security results with the minimum coast as possible.**

Main Category (8)	Sub Category (36)
User security (6)	Account management
	Identification and authentication
	Password management
	Access control procedure
	Manager and Special authority management
	External authority management
Data protection (3)	Data in transit protection
	Data at rest protection
	Encryption protection
Component security (4)	System hardening
	Mobile device management
	Malware control
	Up-to-date security patch
Network And communication security (4)	Network segmentation
	Network access control
	Secure wireless network
	Secure remote access
Asset management (2)	Asset list management
	System setup and change management
physical Access security(2)	Protected area designation
	Access control
Security organization and policy(5)	Establish cyber security policy
	Designation of security officer and person in charge
	Cyber security training
	System, equipment and service purchase security process
	Security evaluation
Event and incident management(4)	Emergency plan establishment
	Information system backup
	Log management and monitoring
	Protection against denial of service attacks

R&D Activities on ICS Security in Korea

Standard Issues

- The Countries such as the EU, Asia, and the United States enforce the IEC 62443-4-1 Standards When the companies are in the development and production stage.
- The United States requires UL, and Germany requires TuV. All of those standards are based on ISA/IEC 62443 Series

Korean Agency for Technology and Standards(KATS) developed KS standards based on IEC 62443 Series.

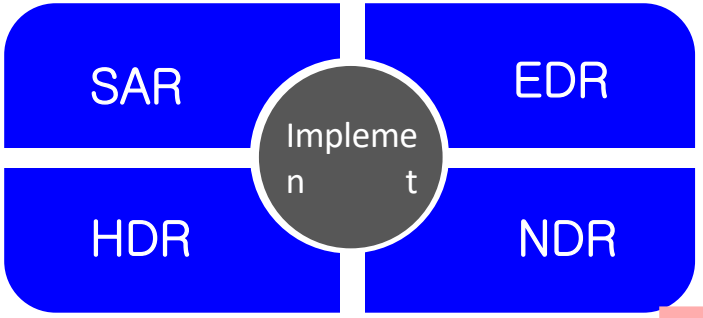
- 2019: KS X IEC 62443-1-1, 2-1, 4-2
- 2020: KS X IEC 62443-4-1
- 2021: KS X IEC 62443-3-3, 2-4

General interface for security elements in embedded system

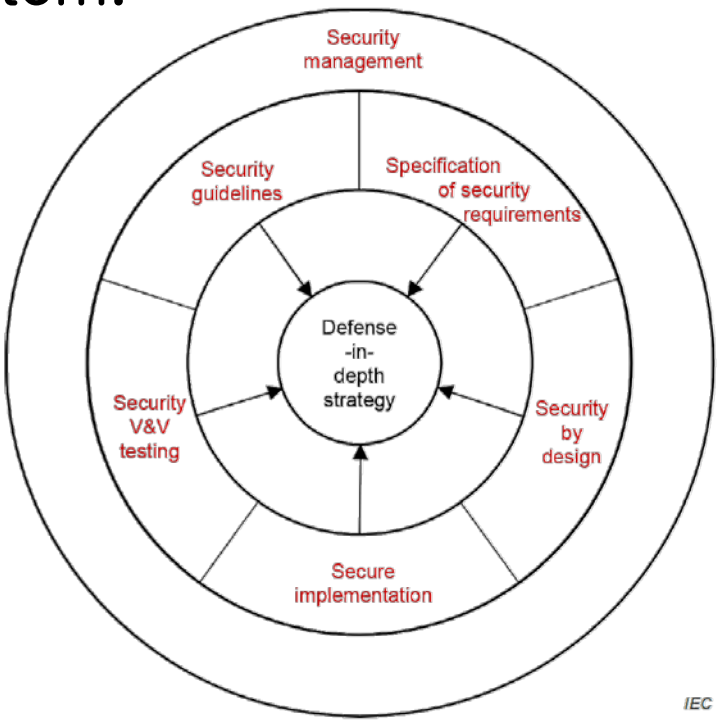
- In order to develop a secure and safe device/software/system, the international standard should apply to those device/software/system.

- Apply the international security standards to the embedded system's interface

[standard : IEC 62443-4-2]



- EDR : Embedded device requirements
- HDR : Host device requirements
- SAR : Software application requirement
- NDR : Network device requirements



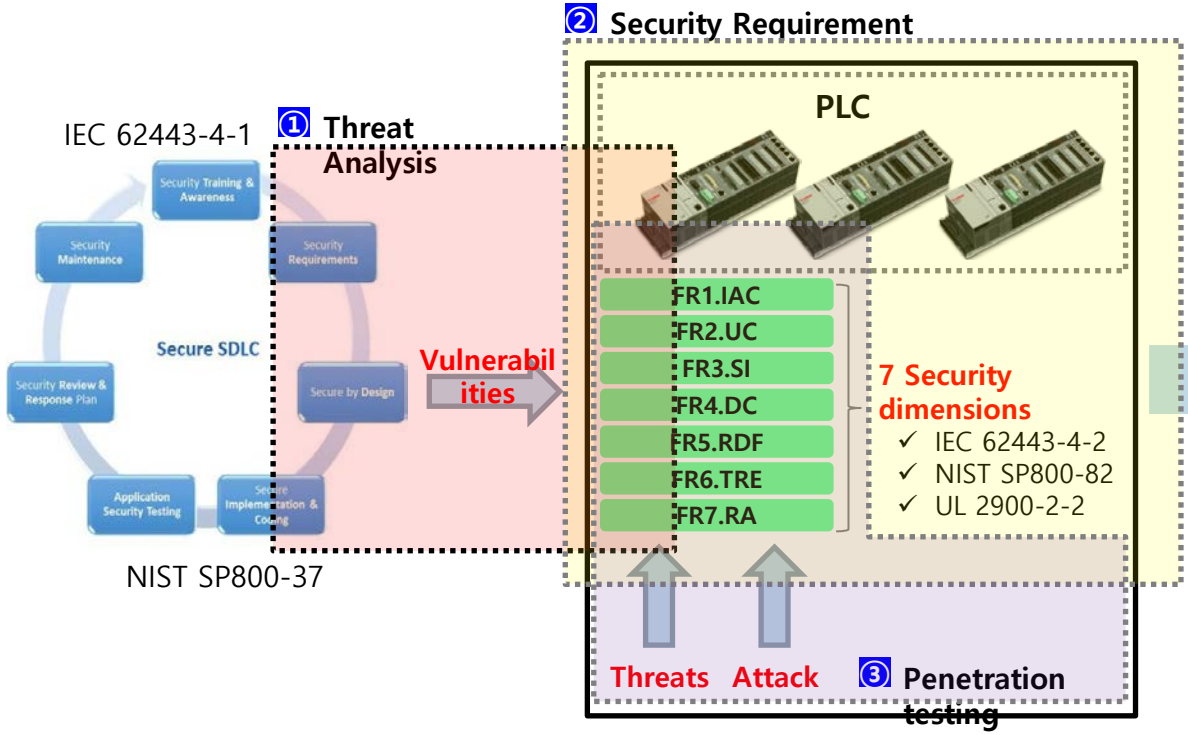
[IEC 62443-4-1, Defense in Depth Strategy]

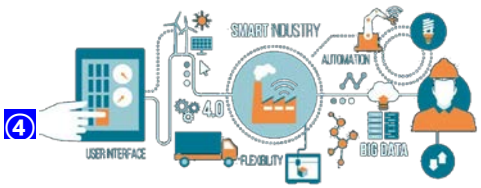
Need to become a basic category

Select and reflect only necessary category

General interface for security elements in embedded system

- Implemented in major communication interfaces for domestic companies that produce PLCs that are mainly applied to smart factory

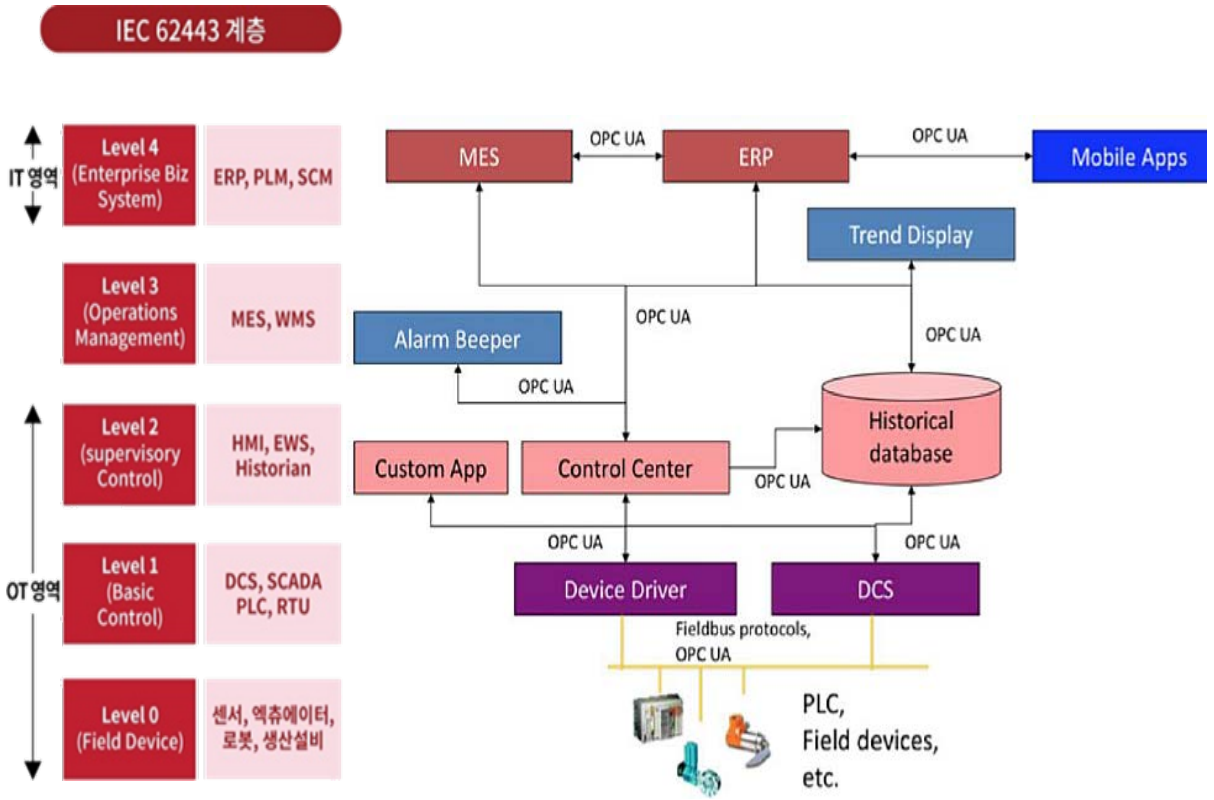




- This can be applied Smart factory embedded products (including HW, SW) with built-in security.
- This can Satisfying security certification requirements essential for product development an manufacturing when promoting global export.

OPC UA Security

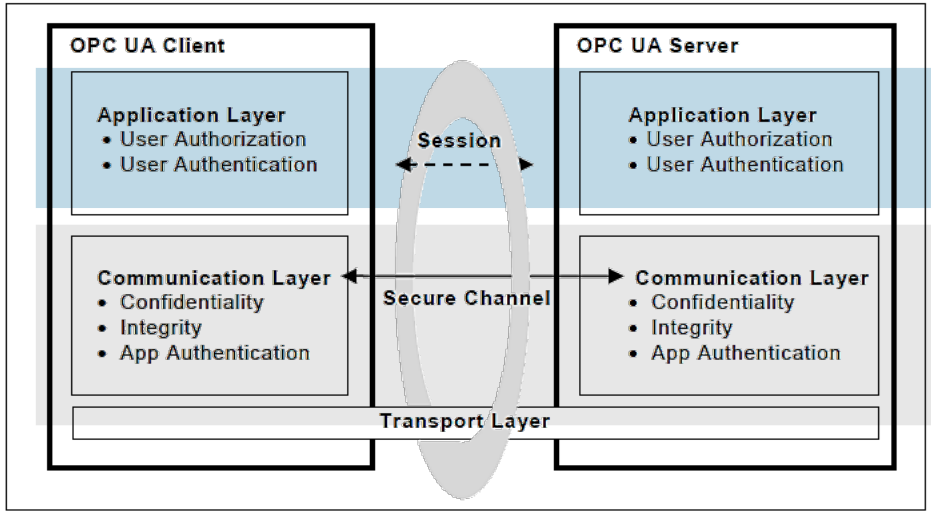
- Based on the IEC 62541-2 planned to applied the OPC UA security model and confirmed this model operates securely and safely in the industry environment.



Security in OPC UA

- To successfully establish the secure channel in the OPC UA, Three major components must be applied in the model
  1) In order to establish successful network communication among devices, X.509 v3 PKI should be implemented.
  2) The CA certification and authorization must be implemented.
  3) Cryptography technology must be implemented for the technology to securely functioned.
  4) The Client and the Server to securely exchange cryptographic keys and secret information in an insecure environment

[IEC TR 62541-2, OPC UA security architecture]



[Applied technology]

X.509 v.3 PKI (Lightweight, Full Ver.)

CA certification and authorization

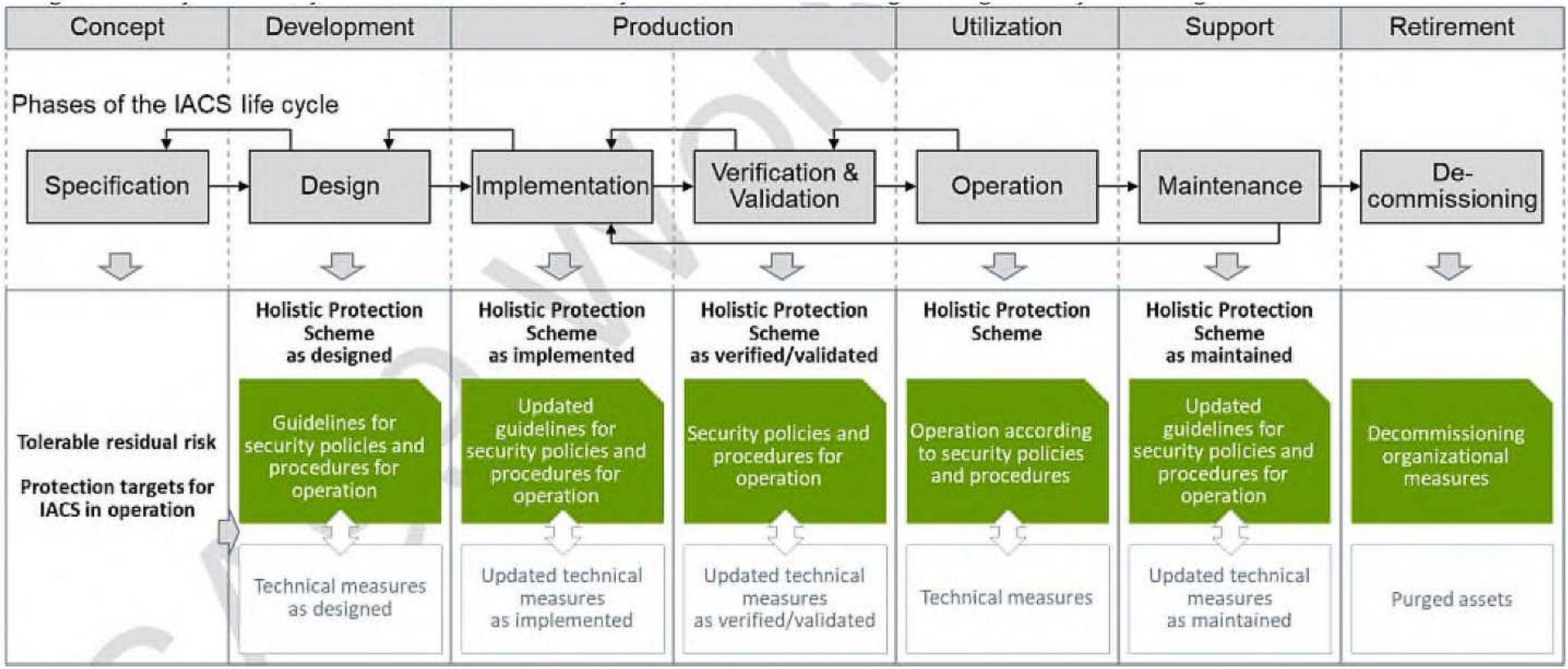
Cryptography(Lightweight, Full Ver.)

TLS(Transport Layer Security)

Development and operation of a holistic protection scheme

- The goal is to build the product comply IEC 62443-4-1 SPDL Process standards.

Stages of the System Life Cycle Model of IEC 24748 "Systems and Software Engineering – Life Cycle Management"



IEC 62443-2-2 Security for IACS 2-2 IACS security program ratings – Mar.2020 2ndCD

Development strategy plan

- Based on IEC 62541-2 OPC UA Security Model, developing international protocol to protect the infrastructure and system in the smart factory system.

  1) conduct research on X.509 v3 authentication system In smart factory infrastructure and ICT.

  2) initiated development of the authentication system on the Smart factory system and ICT.

- Development of smart factory and ICT system complies with secure communication and access control technology in the network environment.

  1) Development of OPC UA based security protocol in the smart factory.

  2) Developing a smart factory and ICT security testing environment for the newly created security platform.

Question & Answer

Keunhee Han
Korea University
Graduate School of Information Security
khhan1@korea.ac.kr