ROK's Regulatory Framework for Cyber Security of Nuclear Facilities

2016. 5. 11

Ickhyun Shin
Director
Division of Cyber Security
Korea Institute of Nuclear nonproliferation And Control (KINAC)

사단법인 한국원자력학회 KOREAN NUCLEAR SOCIETY

Workshop on Cyber Security of Nuclear Facilities

KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
KINAC

Agenda

- Cyber Security Incidnets
- Implications from incidents
- ROK's Regulatory Framework
- Current Regulatory Activities
- Cooperation and R&D
- Future Plan
- Conclusions

International Issues

- **2014 Nuclear Security Summit**
  - ROK VIP Remarks “steps should be taken to tackle the emerging threat of cyber terrorism against nuclear facilities”

- **2016 ROK’s National Progress Report for NSS**
  - Help IAEA developing Cyber Security Guidance Doc.
  - Participate IAEA CRP for Cyber Incident Response
  - Hold Training Courses
  - By ROK’s NSF*
    *Nuclear Security Fund

KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
KINAC

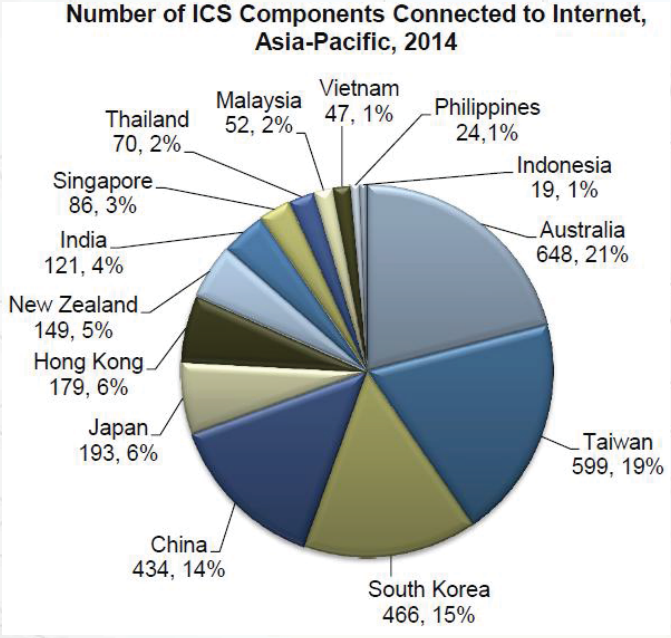
Cyber Security Incident

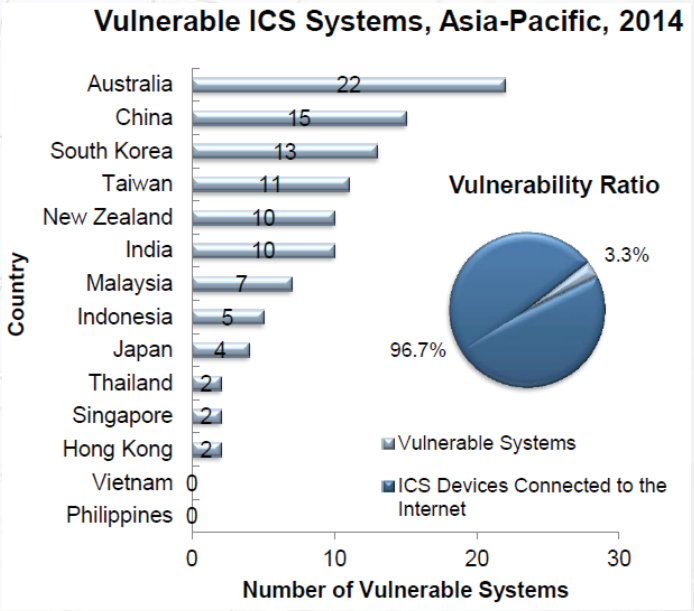
- **Shutdown of German RWE NPP**
  - Malware infected on Fuel Handing System*
    * Monitoring Computer
  - 18 Portable Media were also infected
  - No effect on the Fuel Handling and Operation of Plant

	Stuxnet	W32.Ramnit	Conficker
Target System	Simmens Control System	Windows Operating System	
Functions	PLC Logic Alteration while tricking monitoring data	Data Theft Unable to patch & anti-virus engine update	Remote Access User Monitor Theft User Credentials
Characteristics	APT, Air-gapped	Internet Connection is needed	

Threat Environment

- **ICS is getting more vulnearable to Cyber Threat**





Source: NSHC; Frost & Sullivan

KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
KINAC

Threat Environment

- **Various Attack Vectors**
  - Watering Hole Attack : Compromised Website/Firmware File
  - Social Engineering : Phishing
  - Removable Media : Infiltration into an air-gapped system
  - Virtual Private Networks : “Heartbleed” vulnerability
  - Wireless Networks and Regue WiFi Hotspots

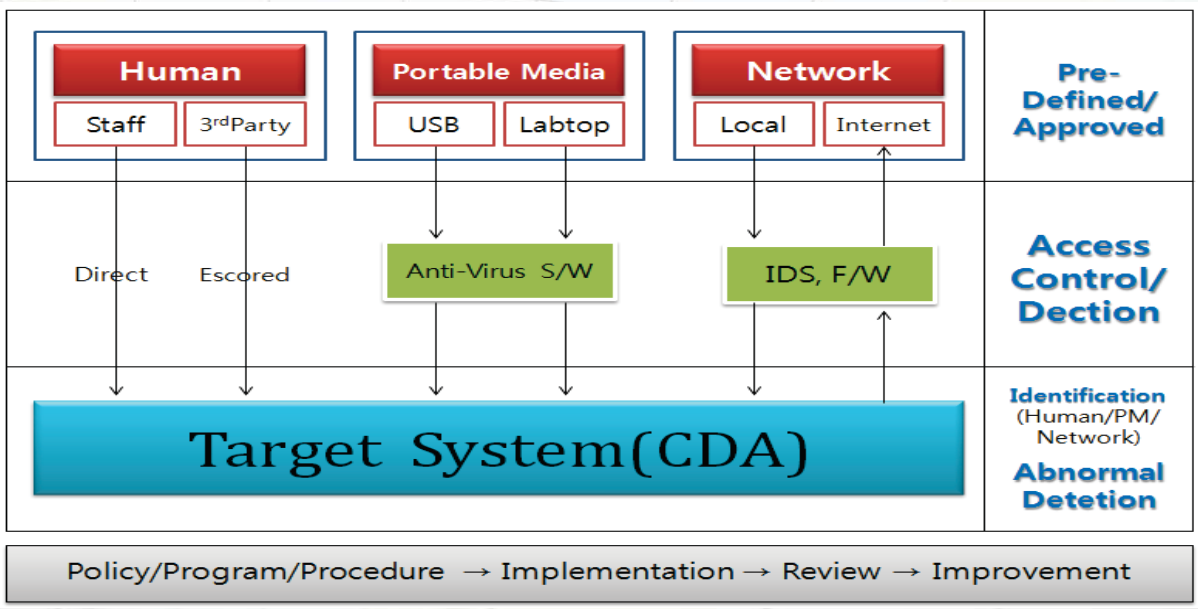
- **Unintentional Insider Threat**

An unintentional insider threat is (1) a ***current or former employee****, contractor, or business partner (2) who has or* ***had authorized access to an organization’s network****, system, or data and who, (3) through action or inaction* ***without malicious intent****,2 (4)* ***causes harm*** *or substantially increases the probability of future serious harm to the* ***confidentiality, integrity, or availability*** *of the organization’s information or information systems.*

Source : www.sei.cmu.edu

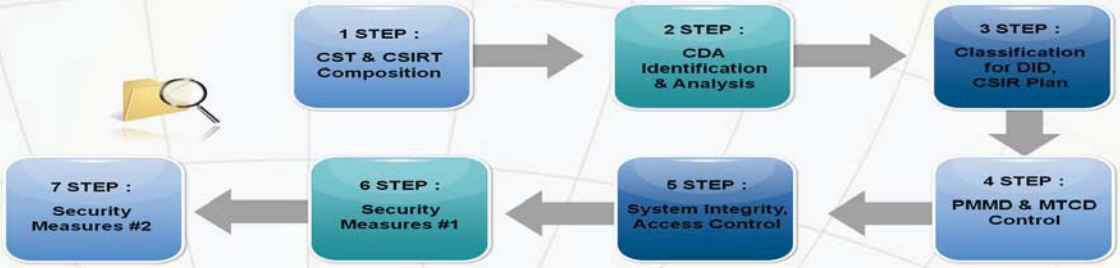
Implications

- **Key Security Measures**
  - Portable Media Protection : USB, CD, etc
  - System Hardening : HIDS, Integrity
  - Protection from Insider Threat : Seperation of Duty, Least Priviledge



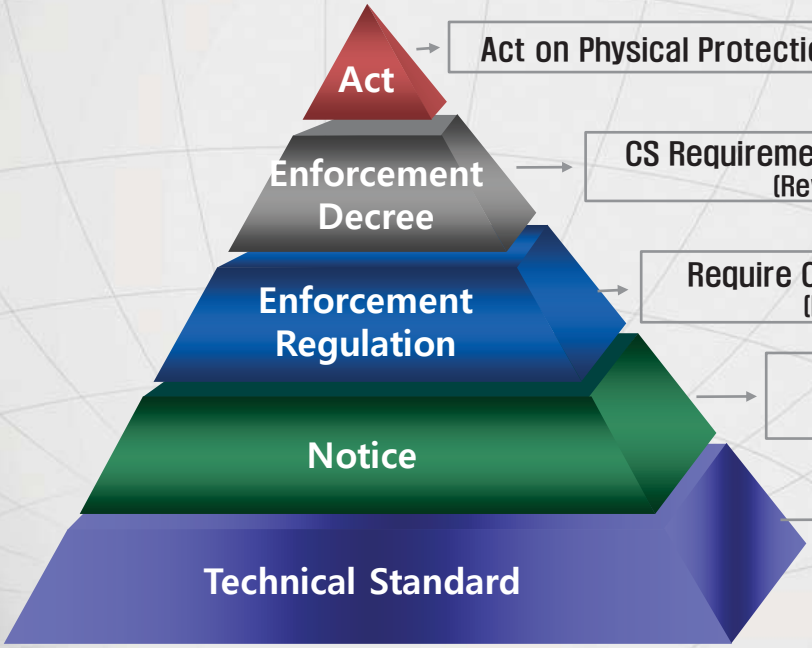
Regulatory Approaches

- **Cyber Security Plan : 7 Steps**



- **Cyber Security Program**
  - Cyber Design Basis Threat
  - Applying Security Contorls
    - Defense-In-Depth Strategy, Diversity, Redundancy
    - 101 Security Controls in KINAC RS-015
  - Continuous Monitoring & Assessment
    - Periodic Assessment of Security Controls, Change Control
  - Cyber Security Incident Response

ROK's Regulatory Framework

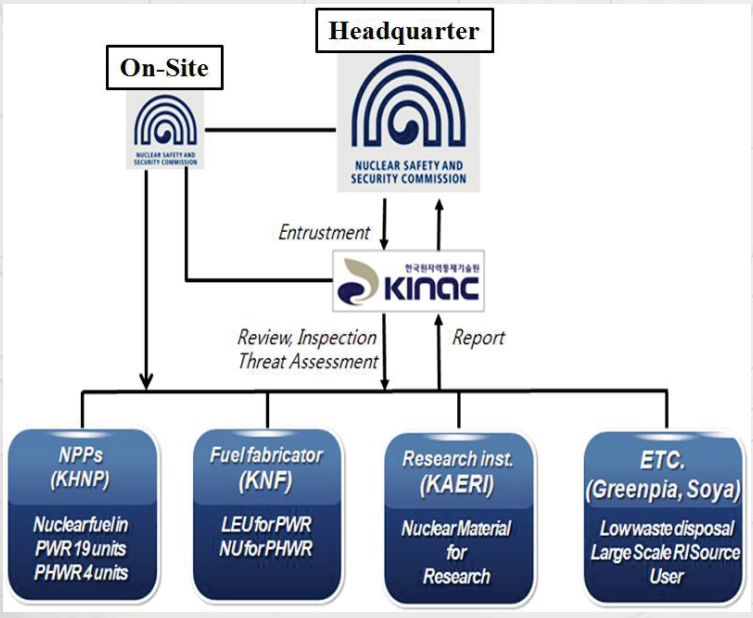


- Act: Act on Physical Protection & Radiological Emergency
- Enforcement Decree: CS Requirements against Sabotage, Theft (Revised on Dec. 2013)
- Enforcement Regulation: Require CSP to be approved by NSSC (Revised on Dec. 2013)
- Notice: Details of CSP (Revised on Nov. 2014)
- Technical Standard: Baseline for Inspection KINAC_RS015.01 (Nov. 2014)

KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
KINAC

Regulation Scope

Companies subject to NSSC's Inspection



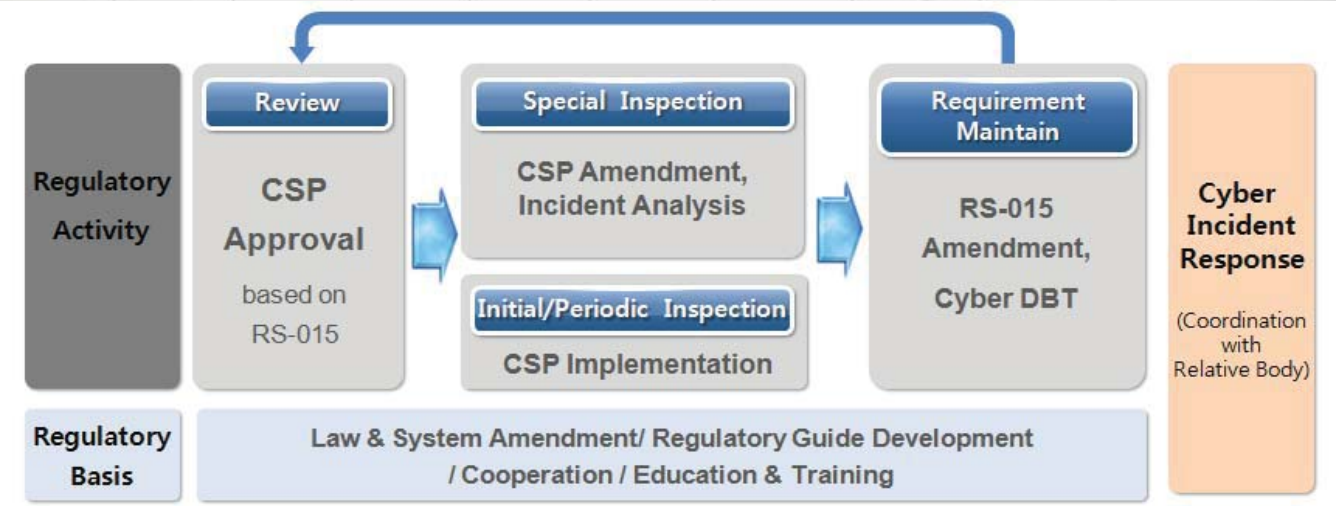
Critical Digital Assets

Computer Systems related with functions

- **Safety, Important-to-safety (S)**
- **Security (S)**
- **Emergency Preparedness (EP)**
- **Support Systems** (* which, If compromised, adversely impact SSEP)

Regulation Overview

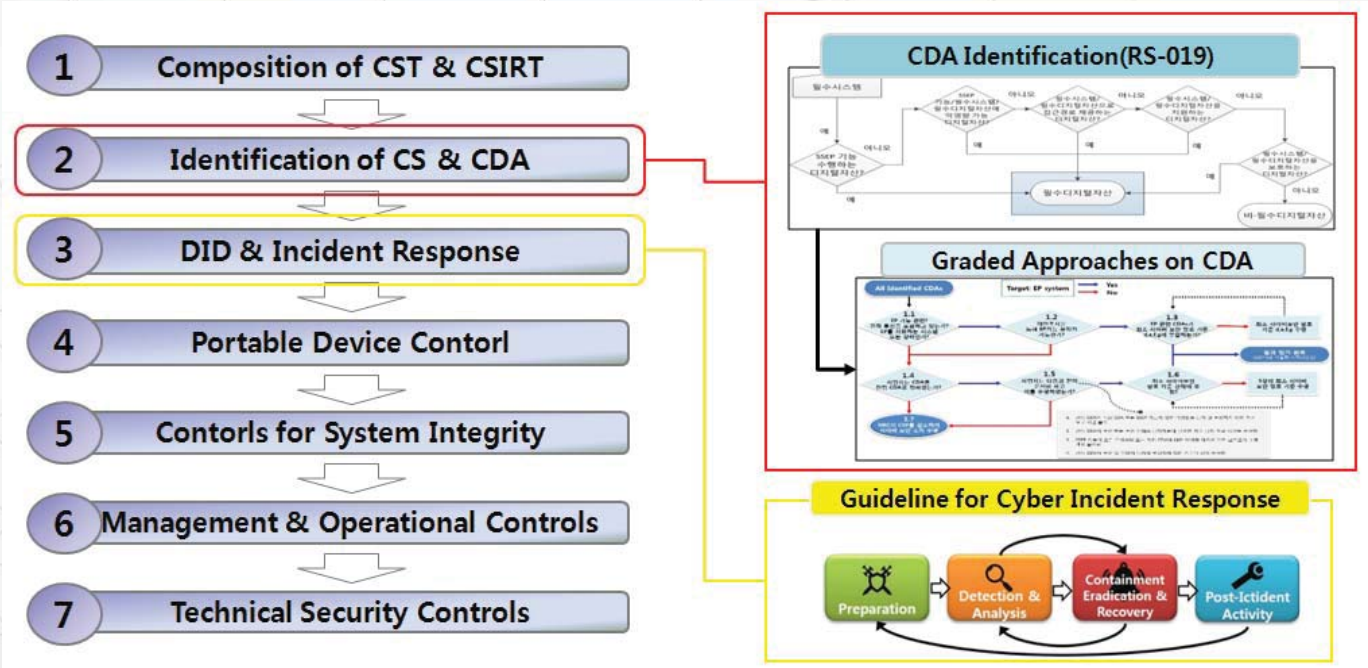
- **Main Regulatory Activities**
  - CDBT Development, Review, Inspection, Exercise Assessment
- **Other Activities**
  - Policy Support, R&D, Education & Trainiong, Cooperation, Etc



KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
KINAC

Current Regulatory Activites

- **7 Step Special Inspection by 2018**



Current Regulatory Activites

- **Regulation based on the APPRE**
  - (DBT) Review the CDBT every 3 years based on threat asses.
  - (Review) Cyber Security Plan and Etc
  - (Inspection) Carry out every 2 years during overhaul period
  - (Exercise) Assess Licensee's Implementation
    - One Full exercise and two Partial exercise per year
- **Inspection**
  - 5 inspectors composed of ICS, IT Security specialist carry out the 2 weeks inspection

Week	1	2	3 ~ 4	5
Phase	Preparation, Collection of licensees' self assessment	Office Review, Site Inspection Plan	Site Review, Site Inspection	Reporting

KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL

Current Regulatory Activites

- **Cyber Design Basis Threat**

Threat Assessment

Government should establish physical protection system by assessing threats on nuclear facilities on a regular basis *[APPRE Article 4]*

Development of DBT

The NSSC* should develop Design Basis Threat every 3 years or when necessary, which is the criteria for design and assessment of nuclear licensee's physical protection system *[Enforcement Decree of APPRE Article 7]*

Performance Based Regulation

Prescriptive Based Regulation

Current Regulatory Activites

▪ DBT Process

Threat Assessment Report (KINAC) [D-12M]	**Draft DBT** (KINAC) [D-10M]	**Review of Draft DBT** (Consultancy Group) [D-4M]
⇧		⇩
DBT Reassessment (NSSC, KINAC)		**NSSC's Approval** (NSSC, PP WG) [D-1M]
⇧		⇩
PPS Improvement (Licensees) [D+14M]	**Scenario-Based Assessment on PPS** (KINAC, Licensees) [D+8M]	**Application of the DBT to PPS** (Licensees) [D+1M~]

KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL

Current Regulatory Activites

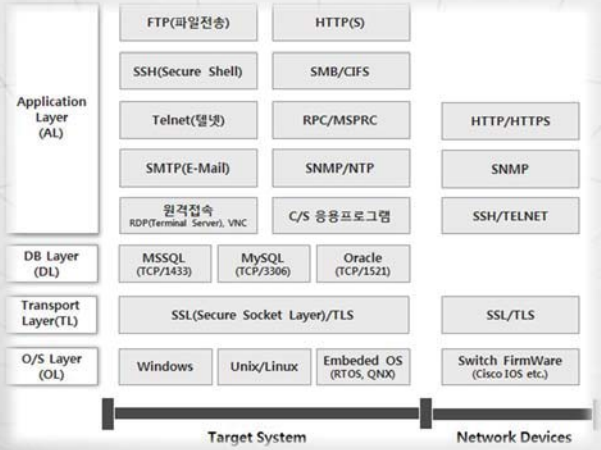
▪ Incident Response Exercise

- ◦ NSSC's Notice related with Education & Training
- ◦ Licensee should conduct Exercise every year
  - Full Exercise
  - Partical Exercise
- ◦ KINAC can conduct Assessment

KHNP				KAERI	KNF	KORAD		Greenpia	Soya
Kori	Wolsung	Hanwul	Hanbit			Center	Daejeon		
Jun	Aug	July	Mar	Aug	Sept	Oct	Oct	Dec	Dec

Other Regulatory Activites

- **Research & Development**
  - Two R&D Projects
    - One focuses on Inspection Tools
    - The other focuses on Accident Effect



DBMS Layer	MSSQL	TCP/1433	DL-SQL-01	SA계정 Null 패스워드 사용
			DL-SQL-02	MSSQL 보안 취약점 패치 점검
	MySQL	TCP/3306	DL-MySQL-01	취약한 패스워드 사용
			DL-MySQL-02	MySQL 보안 취약점 패치 점검
	ORACLE	TCP/1521	DL-ORA-01	Oracle 디폴트 패스워드 사용
			DL-ORA-02	Oracle Default SID 노출
			DL-ORA-03	TNS Listener 취약점 점검
			DL-ORA-04	Oracle 보안 취약점 패치점검
Transport Layer	SSL/TLS	TCP/443	SL-SSL-01	SSL 취약한 암호화 알고리즘 점검
			SL-SSL-02	SSL 보안 취약점 점검
Operation System Layer	Windows	N/A	OSL-SEC-01	불필요한 서비스 점검
			OSL-SEC-02	최신 보안 취약점 패치 점검
	Unix/Linux		OSL-SEC-03	불필요한 서비스 점검
			OSL-SEC-04	최신 보안 취약점 패치 점검
	Embeded O/S(RTOS)		OSL-SEC-05	불필요한 서비스 점검
	Network Device		OSL-SEC-06	IOS 보안 취약점 패치 점검

KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL

Other Regulatory Activites

- **International Cooperation**
  - IAEA , NRC SCM, PCG(DOE-NNSA, INL), UAE FANR
  - U.S HLBC, Jordan EMRC,

- **Domestic Cooperation**
  - KINS, KAERI, NSRI, University, Etc

Other Regulatory Activites

- **Education & Training**
  - NNSA Notice : Cyber Security Staff need to be trained
  - Areas to be trained
    - Cyber Security
    - ICS Structure vs IT Environment
    - I&C Filed : its function and operation

KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL

Future Plan

- **Whole Life-Cycle Regulation**
  - Currently Operation NFs is subject to KINAC's inspection
  - Construction NFs is out of regulation scope
  - Need to require licesee to include CS requirements
    - when submitting CP & OL applications

Life-Cycle	Design → Production → Construction → Operation → Maintenance → Decommission
Safety	⟷
Security	⟷

Future Plan

- **Records Retention**
  - Admendment of APPRE's Enforcement Regulation
  - Date : June 2, 2016 / Enter into Force : Jan. 1, 2016

Records	Record Time
Access Log on the CDA (Person & Device)	Whenever Accessed
Installation, Maintenance, Test Log	Whenever conducted
Periodic self security inspection to check compromisation	Whenever conducted
Cyber Incident and response record	Whenever happened

KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
KINAC

Future Plan_Graded Approach

- **Too many CDAs in NPP**
  - about 2/3 of all systems are critical system*
  - more than 60 % of the total critical systems are digital system*

  * APR1400 based (Shin-Kori NPP 3&4, Barakah NPP 1~4)

- **Addressing the 101 security controls for each CDA needs**
  - too much effort for both licensee and inspector

- **Need to focus on more significant CDA**
  - Addressing the security controls by its grade

  → Consequence-based graded approach is necessary

Conclusions

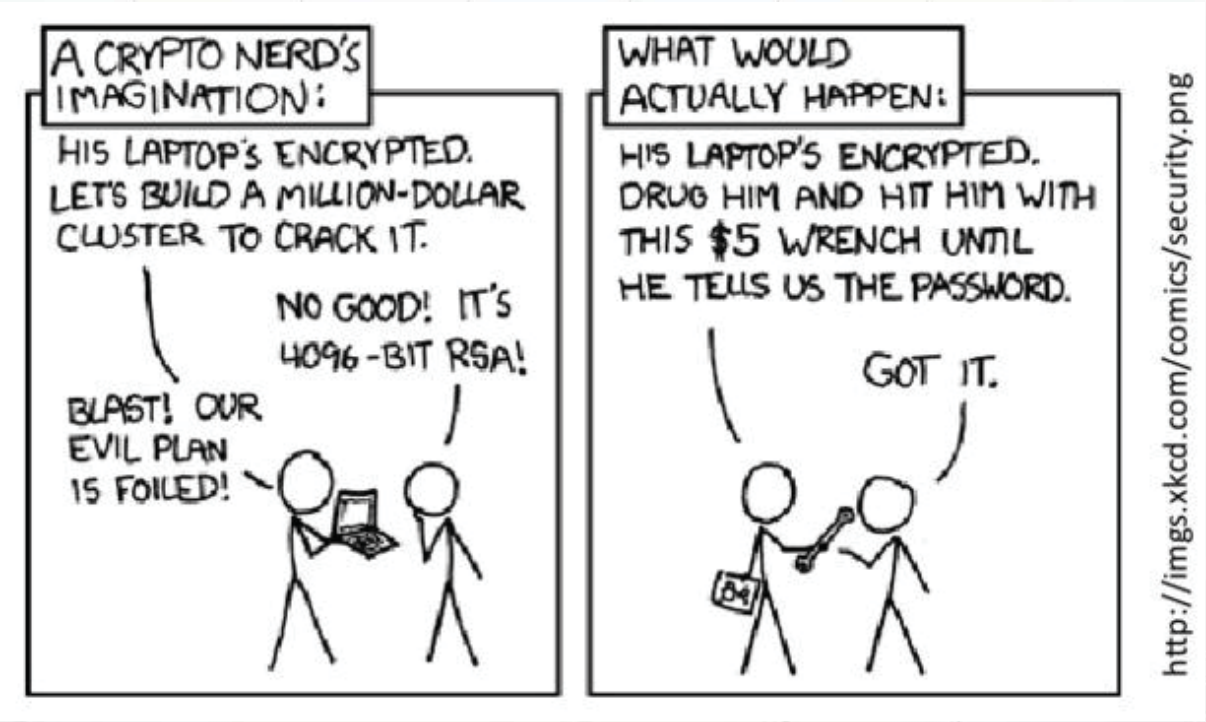
- **Talking with Expers in I&C field**
  - Safety system is both subject to
    - Cyber security regulation
    - Safety regulation
  - Some Areas of Conficts
    - Transparency vs Confidentiality
    - Authentication vs Human Factor Engineering
  - Some Areas in common
    - Defence-in-Depth, Integrity, Redundancy, etc
  - Important to understand each view points through
    - Regular meetings
    - Experts exchange

KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
KINAC

Conclusions

- **Build Competency for Facility's Operators**
  - Performance base regulation provides
    - what to comply
    - DBT
  - Operators need to
    - figure out how to implement the "what" requirements
    - show that their system can be protected from cyber attack up to DBT
  - To do so, Operators need to
    - learn and study
    - carefully select security measures which does not adversly affect the safe operation and its function

Q&A



KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
KINAC

Thank you

감사합니다