

ICS SECURITY IN JAPAN

INTRODUCTION OF CONTROL SYSTEM SECURITY CENTER (CSSC)

April 26th, 2017

The 3rd French Japanese Meeting on Cybersecurity

Kenzo Yoshimatsu
R&D Division

Control System Security Center (CSSC)





about CSSC

overview of CSSC and
its activities <English version>



20.3MB

Control System Security Center
Tohoku Tagajo Headquarter (CSS-Base6)
Opening Symposium
available only in Japanese

CSSC Tohoku Tagajo Headquarter
(CSS-Base6)
Opening · Symposium Report

click to watch
CSSC PV
on YouTube



Control System Security Center conducts R&D to handle cyberattacks and ensure the security of control systems of critical infrastructures, such as power and gas plants.

<http://www.css-center.or.jp/en/index.html>

CSSC Promotion Video About 8 Minutes

If Tokyo city falls into wide-area blackout,

<http://www.youtube.com/watch?v=qgsevPqZpAg&feature=youtu.be>

Where is CSSC?

- Headquarter

- Tohoku Tagajo Headquater
- TAGAJO CITY, MIYAGI

Tohoku Tagajo HQ (TTHQ)



- Tokyo Branch

- Tokyo Research Center
- CHOFU-SHI, YOKYO

Tokyo Rsearch Center (TRC)



Where is Tagajo?

- Jo = castle; since 8th century
- Historically famous and important place in Japan
- Tsunami (2-4 m height) caused by the earthquake has covered the 33% of the city land (Mar.11.2011)
- After the earthquake, Tagajo city launched “Research Park for Disaster Reduction” plan.
 - Internationally prominent effort for achieving disaster reduction
 - Development of distinct technologies and products
 - Policies for disaster reduction



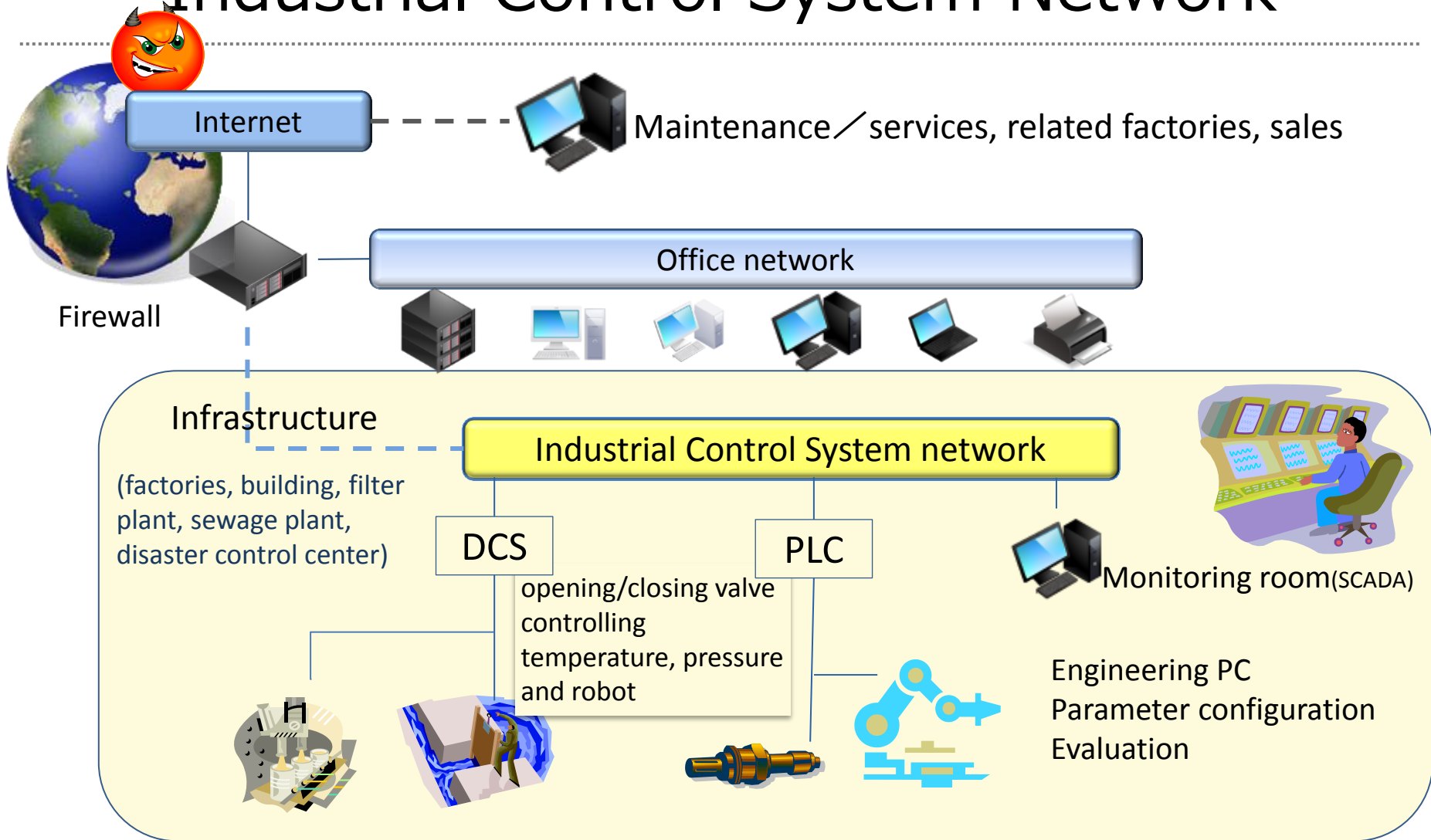
多賀城南門 復元図



“The testbed of CSSC truly suits the concept of Research park for disaster reduction.”

(Mayor of Tagajo)

Industrial Control System Network



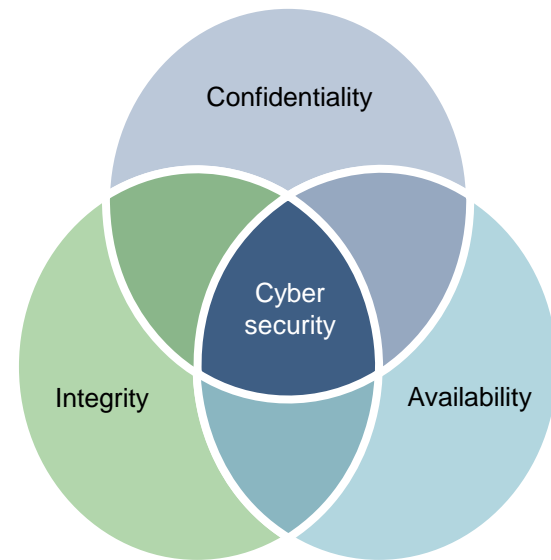
DCS: Distributed Control System

PLC: Programmable Logic Controller

SCADA: Supervisory Control And Data Acquisition

Control Security and Information Security

- The term “cyber security” means maintaining the confidentiality, integrity, and availability of information assets. These are the three requirements of cyber security and are referred to by the acronym “CIA” formed from the first letters of each. It is important to maintain all three elements with balance.
 - Confidentiality
 - The term “confidentiality” refers to the ability of authorized persons to properly access information only by authorized methods. In other words, confidentiality ensures that users without access privileges cannot access information.
 - Integrity
 - The term “integrity” refers to the safeguarding of the accuracy and integrity of assets.
 - Availability
 - The term “availability” refers to the ability of authorized persons to access assets in a timely fashion when necessary and the maintenance of assets in a state in which they can be used without a problem.



- **Control Security**
Availability > Integrity > Confidentiality
- ↕
- **Information Security**
Confidentiality > Integrity > Availability

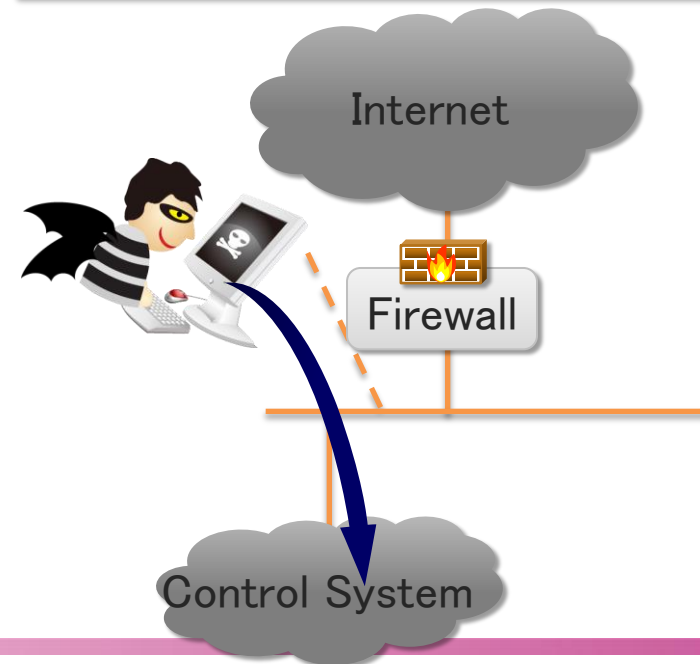
Security Incidents in Water Sector

- A wastewater treatment plant system in Australia was hacked in 2001, and released raw sewage into local rivers and parks. In the result, there was significant damage to the ocean system.
- That incident was committed by a former employee of a SCADA software vendor. *He was arrested eventually.
- He used the remote access account and route, and illegally operated the control system.



Chesapeake Bay Program/CC BY 2.0 this is a referencing image

A resignee hacked into a control system through remote access route



Security Incidents in Railway Field

- Train signaling systems were shut down by a malware (sobig) infected the internal computer system, in the United States in 2003.
- It took 6 hours to recover, and the train operation was disrupted all the while.

CSX Train



Flowizm .../CC BY 2.0

Sobig

The sobig worm is a trojan-type malware. It appears as an email attachment, and replicates by itself to spread infection. Sobig searches out stored email addresses from Windows address books and files (that extensions are: txt, eml, html, htm, dbx, wab) on victims' computers, then mails out messages containing attached files infected with copies of the virus.

Security Incidents in Petrochemical Field

- Turkish oil pipeline was exploded in 2008. The attackers hacked the operational control system, super-pressurized the crude oil in the line, and caused the explosion.
- Hackers had shut down all the alarm devices (including cameras and sensors), and cut off communications.

Oil pipeline



Will Russell/CC BY 2.0 this is a referencing image

Oil pipeline (overall view)



Source: Bloomberg research

Bloomberg Graphics

Example of Incident with BA System

Hacking into an HVAC system at a hospital by a security officer



W.B. Carrell Memorial Clinic

Date	April – June, 2009
Target of Attack	W.B. Carrell Memorial Clinic in Dallas, Texas (America)
Path of Entry	Illegal access to the hospital's HVAC system, patient information computer, etc.
Damage	System intrusion, online disclosure of system screens. A DDoS attack was also planned, but failed.

<i>Timeline</i>	<i>Background and Outline</i>
<i>Background</i>	A contracted security officer at the hospital in question (25 years old at the time) also acted as leader of a group of hackers called "Elektronik Tribulation Army" under the pseudonym "Ghost Exodus."
<i>Attack</i> <i>April – June, 2009</i>	The security officer in question penetrated the hospital's HVAC system and customer information computer and disclosed screenshots of HMI screens from the HVAC system online. Menus of the various functions of the hospital including pumps and cooling devices in operating theaters could be checked from the screens disclosed (see the next page). Moreover, motion images of scenes depicting acts such as installing malware in PCs in the hospital (apparently, botnetting of PCs in preparation for the DDoS attack detailed later) were also disclosed online.
–	Meanwhile, although hospital staff thought it strange that the HVAC system alarm was not functioning as programmed because the alarm settings had been stopped, nothing amiss was discovered in the hospital.
<i>Discovery and Arrest</i> <i>June, 2009</i>	The attack was discovered when a SCADA security expert examined information he had obtained from a hacker acquaintance and reported it to the FBI and the Texas Attorney General's Office, leading to the arrest of the security officer in question on June 26, 2009. (He was sentenced to serve 9 years in a federal penitentiary.)
<i>Attack Plan (Failed)</i> <i>July, 2009</i>	Although the attack failed with the arrest of the security officer concerned, he had planned to launch a large-scale DDoS attack using the infected hospital system on July 4, 2009 (Independence Day) and was recruiting hackers who wished to help on the Internet. He had already reported his intent to resign to the security company to which he belonged on the day before the scheduled attack date.

Source: DOJ Press release (http://www.justice.gov/usao/txn/PressRel09/mcgraw_cyber_compl_arrest_pr.html)

Threats to Control Systems in Japan

USB Ports

- Viral infections from USB memories are a common occurrence.



Remote Maintenance Lines

- A company connects terminals (e.g. turbines) to a central monitoring room (e.g. of the US headquarters) via remote maintenance lines in order to monitor devices in real time. That causes illegal access and cross-contamination by malware from the terminals.

Replacement of Operating Terminals

- (An Actual Case) In an automotive company: A terminal replaced by a vendor was infected by virus.

An infected terminal brought by a vendor



Physical Intrusion

- No password settled for monitoring terminals
- Using common passwords or IDs, or posting them on walls



Other Past Incidents:

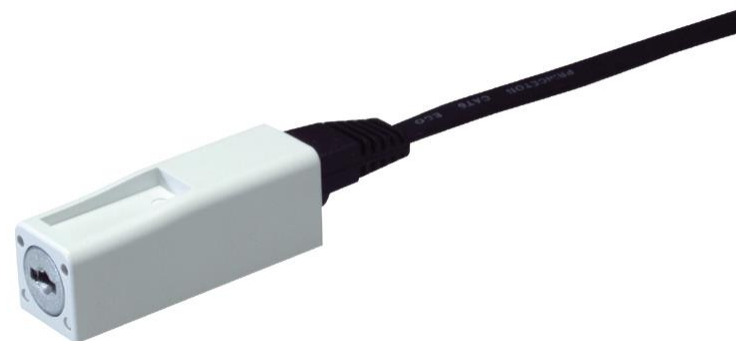
- A Japanese infrastructure company was infected by a virus when an operator connected his terminal to the Internet to play a game.

Measures of Security Control of Connection Devices

- Disabling unused USB ports



- Disabling unused LAN cables



- Disabling unused ports on a HUB



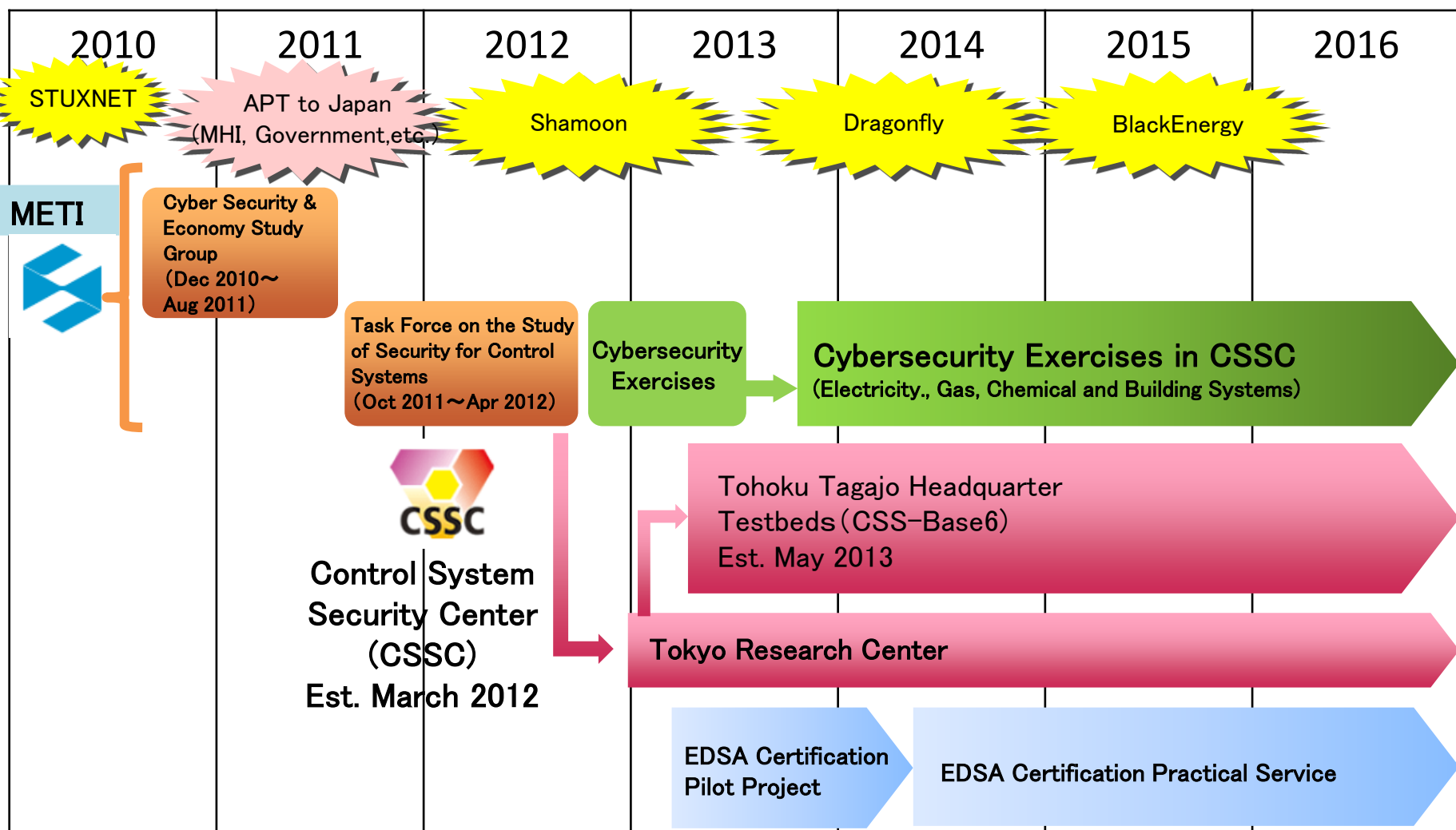
- LAN cables with security lock preventing omission



Directionality of Other Measures

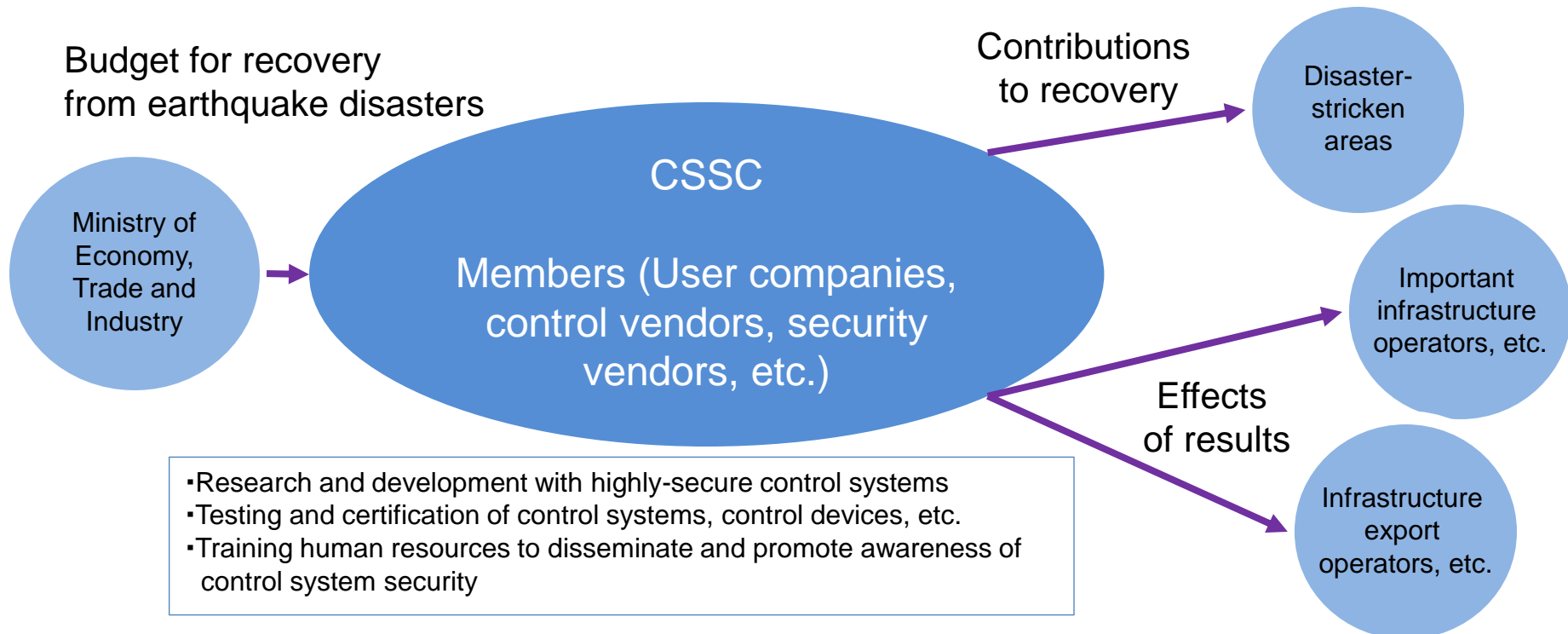
No.	Threads in Japan	Trends and Measures
1	Remote Maintenance Lines	<ul style="list-style-type: none">▪ Authenticate terminals connected to remote maintenance lines (e.g. issue certificates)▪ Conduct security inspection
2	Terminal Replacement	<ul style="list-style-type: none">▪ Run a standalone malware scan when a terminal is replaced
3	Others	<ul style="list-style-type: none">▪ Fully enforce physical security measures (e.g. managing keys and entrance and exit lists, introducing biometric identification, installing security cameras, checking personal belongings and body weight)

Activities on Control System Security in Japan



Purpose of CSSC Activities and Activities Scheme

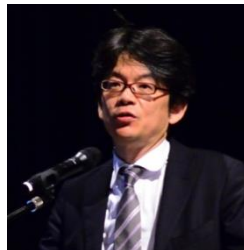
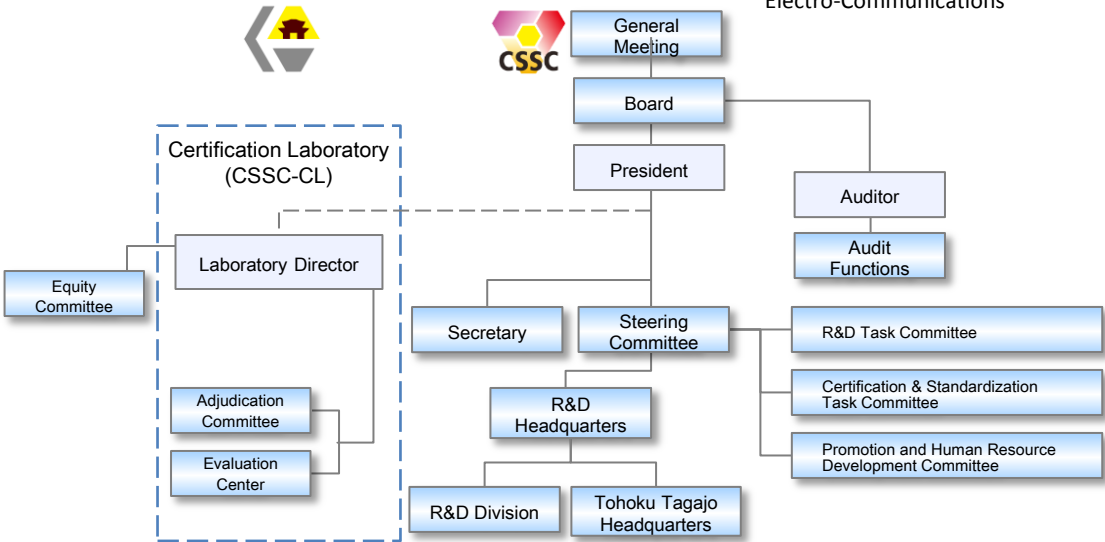
- 1 Ensuring the security of control systems with the focus on important infrastructures
- 2 Strengthening export competitiveness concomitant with ensuring control system security
- 3 Contributions to recovery in disaster-stricken areas



Organization Chart



Dr. Seichi Shin, President of CSSC
Professor, The University of Electro-Communications



Dr. Makoto Takahashi,
TTHQ Executive Director
Professor, Tohoku University

Position	Name	Business Title
President	Seiichi Shin	Professor, The University of Electro-Communications
Board member	Tadayoshi Ito	Executive Officer & General Manager of Solution & Service Business Advanced Automation Company, Azbil Corporation
Board member	Souichi Watanabe	Director eHills Corporation
Board member	Satoshi Sekiguchi	Director General, Department of Information Technology and Human Factors, National Institute of Advanced Industrial Science and Technology
Board member	Hideaki Ishii	Toshiba Corporation Social Infrastructure Systems Company
Board member	Jun Abe	Corporate Officer & Senior General Manager Control System Platform Division
Board member	Masaya Nakagawa	Senior Vice President Head of ICT Solution Headquarters, Mitsubishi Heavy Industries, Ltd.
Board member	Kenji Kondo	Executive Officer, Corporate Research and Development, Mitsubishi Electric Corporation
Board member	Hiroo Mori	Director and Executive Vice President, Mori Building Co.,Ltd.
Board member	Naoki Ura	Head PA Systems Business CenterIA Platform Business Headquarters Yokogawa Electric Corporation
TTHQ Executive Director	Makoto Takahashi	Advisor Professor, Tohoku University
Advisor	Kenji Watanabe	Professor, Nagoya Institute of Technology
Advisor	Kenji Sawada	Associate Professor, The University of Electro-Communications
Advisor	Kazumasa Kobayashi	President and CEO, Fatware ,Inc.
Auditor	Ryuichi Inagaki	Attorney
Secretary-General	Ichiro Murase	Control System Security Center

Outline (As of April 1, 2017)

Name	Control System Security Center (Abbreviation) CSSC <small>※A corporation authorized by the Minister of Economics, Trade and Industry</small>	31 Association members <small>(In alphabetical order)</small>	The National Institute of Advanced Industrial Science and Technology*, ALAXALA Networks Corporation, Azbil Corporation*, Cisco Systems G.K., Fuji Electric Co., Ltd. , Fujitsu Limited, Hitachi, Ltd.*, Hitachi Systems Power Services, Ltd., IHI Corporation, Information Technology Promotion Agency, Japan Audit and Certification Organization for Environment and Quality, Japan Quality Assurance Organization, Macnica, Inc. and Fuji Electronics Co., Ltd., McAfee Co., Ltd., Meidensha Corporation, Mitsubishi Electric Corporation, Mitsubishi Heavy Industries Ltd.*, Mitsubishi Research Institute Inc.*, Mori Building Co., Ltd.*, NEC Corporation, NRI Secure Technologies Ltd. , NTT Communications Corporation, OMRON Corporation, Panasonic Corporation, SOHGO SECURITY SERVICES CO.,LTD., The University of Electro-Communications, Tohoku Information Systems Company, Incorporated, Toshiba Corporation*, Tohoku University, Trend Micro Incorporated , and Yokogawa Electric Corporation* (*8 founding members)
Established	March 6, 2012 (The registration date)		
Location	[Tohoku Tagajo Headquarters (TTHQ)] Miyagi Reconstruction Park F21 6F, 3-4-1 Sakuragi, Tagajo City, Miyagi, 985-0842, Japan	Special Supporting members	Miyagi Prefecture, Tagajo City, Check Point Software Technologies (Japan) Ltd., Cyber Solutions Inc., Eri, Inc., ICS Co.,Ltd., System Road Co., Ltd., Fukushima Information Processing Center, Techno mind Corporation, Toho C-tech Corporation, Tosaki Communication Industry Ltd., TripodWorks CO.,LTD., Tsuken Electric Ind Co., Ltd. , East Japan Accounting Center Co.,Ltd.
		Supporting members	Aiuto, Artiza Networks, Inc., Check Point Software Technologies Ltd., Chiyoda-keiso Co., Ltd., Fortinet Japan K.K., Infosec Corporation, Interface Corporation, Ixia Communications K.K., Japan Nuclear Security System Co.,Ltd., JAPAN DIREX CORPORATION, KPMG Consulting Co., Ltd., Mitsubishi Space Software Co.,Ltd., NUCLEAR ENGINEERING, Ltd., OTSL Inc., The Japan Gas Association, TOYO Corporation

CSSC Association Members (As of April 1, 2017)



Alaxala



azbil



FUJITSU

FE Fuji Electric

HITACHI
Inspire the Next

株式会社 日立システムズパワーサービス

IHI IPA



JQA
一般財団法人 日本品質保証機構

mF Macnica Fuji Electronics



明電舎



NEC Empowered by Innovation

NRI SECURE TECHNOLOGIES



OMRON Panasonic



TOINX

TOSHIBA
Leading Innovation >>>



YOKOGAWA

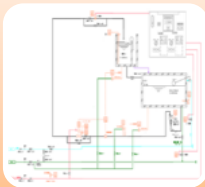


MITSUBISHI RESEARCH INSTITUTE, INC.

Overview of CSSC's R & D 2

1**[Products]**

Checks and measures of current products (controllers, etc.) and research and development of creating secure products

2**[Systems]**

Checks and measures of current systems (mostly IT systems) and research and development of creating secure systems

3**[Plants]**

Checks and measures of current plants and research and development of creating secure plants

4**[Testbeds]**

Research and development of environments where simulation plants can be used for checks and measures of products, systems, and plants

Research and Development in CSSC

1. [Products]

1



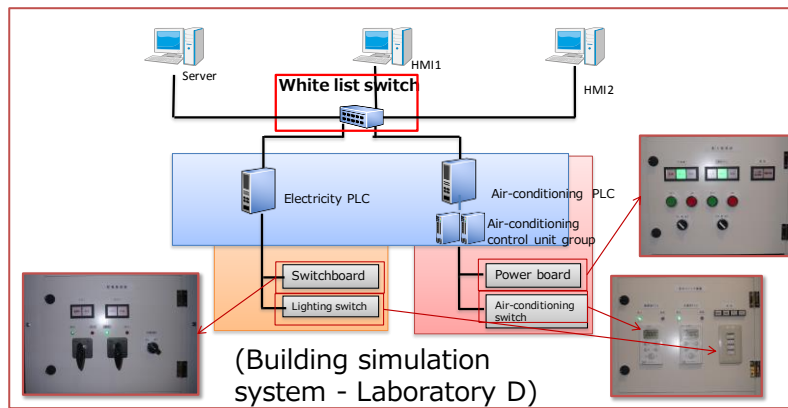
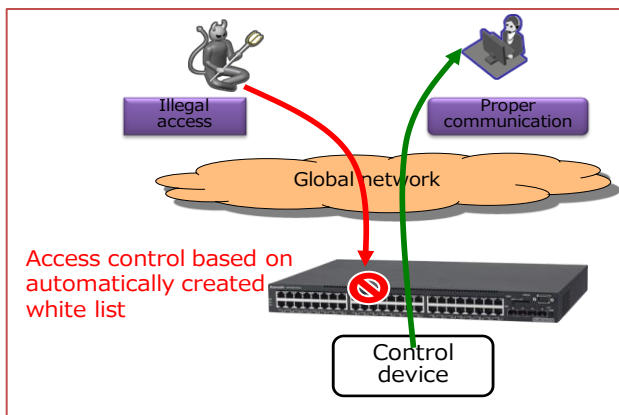
[Products] Checks and measures of current products (controllers, etc.) and research and development of creating secure products

Technology to verify current products

- Verification technology in conformity with ISCI/EDSA
- Establishment of CSSC specific verification items

Technology development for secure products

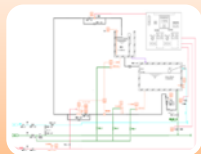
- White list switch
- White list (for terminals and servers)
- Security barrier device (SBD)



Research and Development in CSSC

2. [Systems]

2



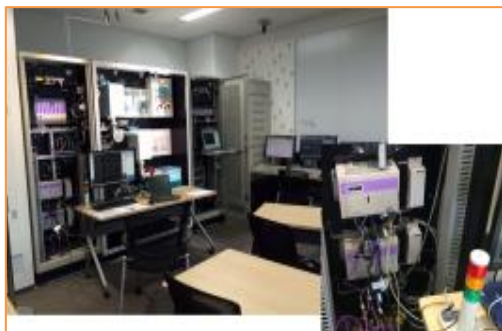
[Systems] Checks and measures of current systems (mostly IT systems) and research and development of creating secure systems

Technology to verify current systems

- Verification technology in conformity with ISCI/SSA
- Establishment of CSSC specific verification items

Technology development for secure systems

- Guide to build secure control systems (IEC 62443)
- Secure log collection technology in control systems
- Cross-sectional log analysis technology in control systems
- Technology to standardize control system asset management (SCAP)
- CSSC specific verification tool



(Chemistry simulation plant
- System evaluation room)



(FA simulation
plant -
Simulation
plant room)

Research and Development in CSSC

3. [Plants]

3



[Plants] Checks and measures of current plants and research and development of creating secure plants



Online information (1)

Online information (2)

Offline information



Narrow down abnormality hypotheses including cyber attacks

- Online information (1): Information always monitored at real-time
- Online information (2): Information obtained online as needed
- Offline information: Information obtained at sites and input to systems manually by humans

Technology to verify current plant operations

- Evaluation of the maturity level of system risk management based on the capability model
- CSMS exercise contents

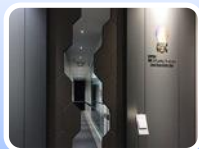
Technology development for secure plants

- Technology to recognize cyber attacks at early stages
- Security technology based on the model-based control
- Measures for human factors

Research and Development in CSSC

4. [Testbeds]

4



[Testbeds] Research and development of environments where simulation plants can be used for checks and measures of products, systems, and plants



All simulation plants and connected devices are the target

Establishment of testbeds

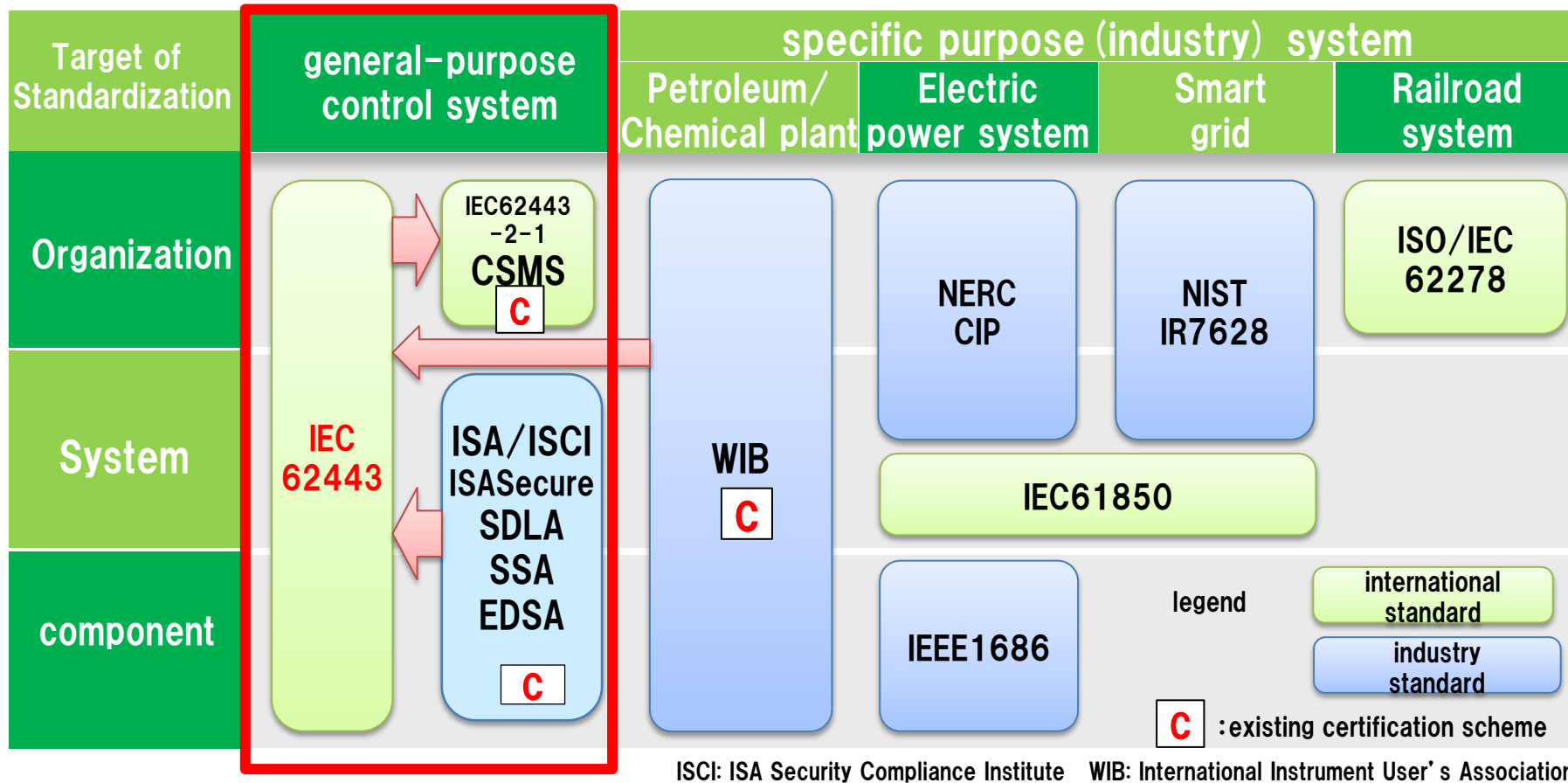
- Establishment of nine simulation plants
- Establishment of an interconnection environment using OPC
- Establishment of a function reproducing malware behaviors
- Establishment of countermeasures

Establishment of verification environments for testbeds

- Establishment of a remote verification environment
- Establishment of a pseudo attack environment

ISA/IEC62443 and ISA/ISCI ISASecure

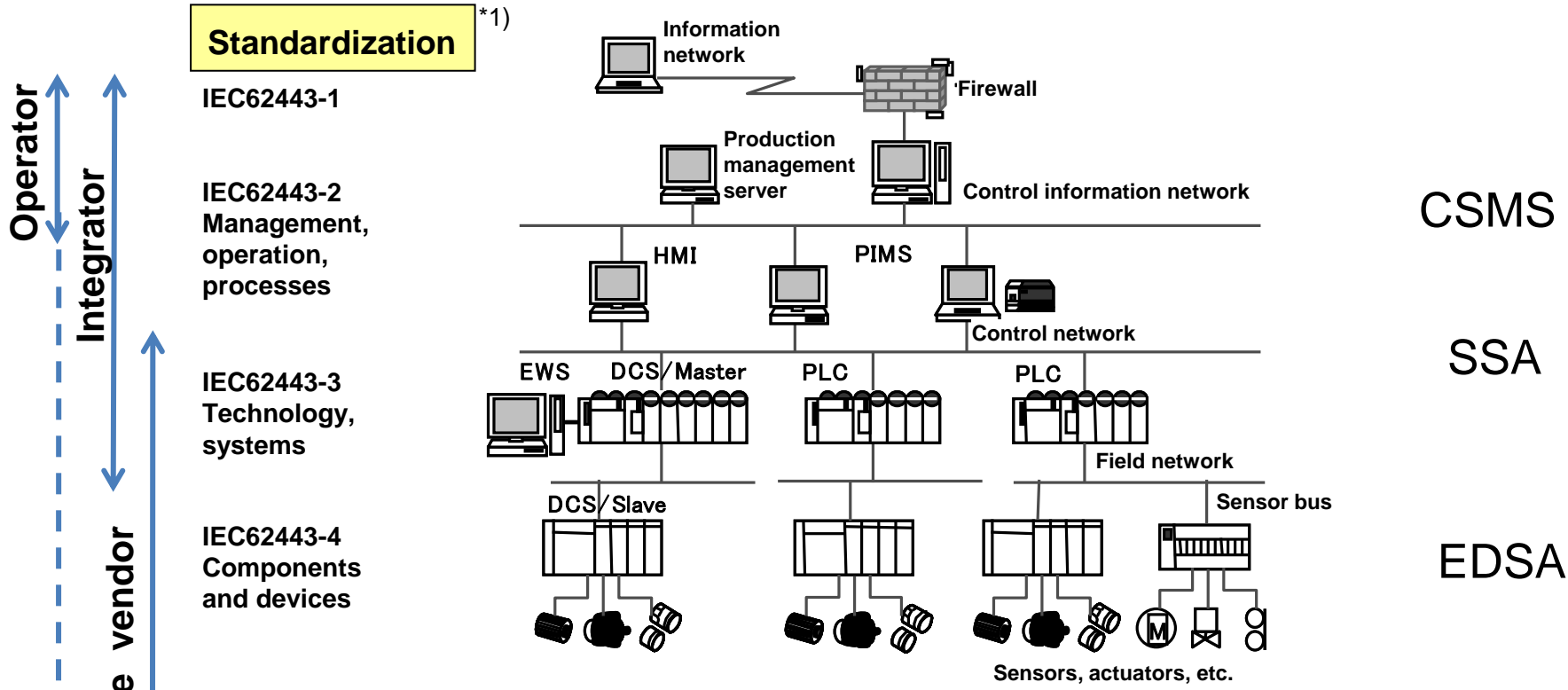
METI and CSSC promote ISA/IEC62443 as ICS security standard and also ISA/ISCI ISASecure as ICS security certification standard.



3)-1 Testing & Certification

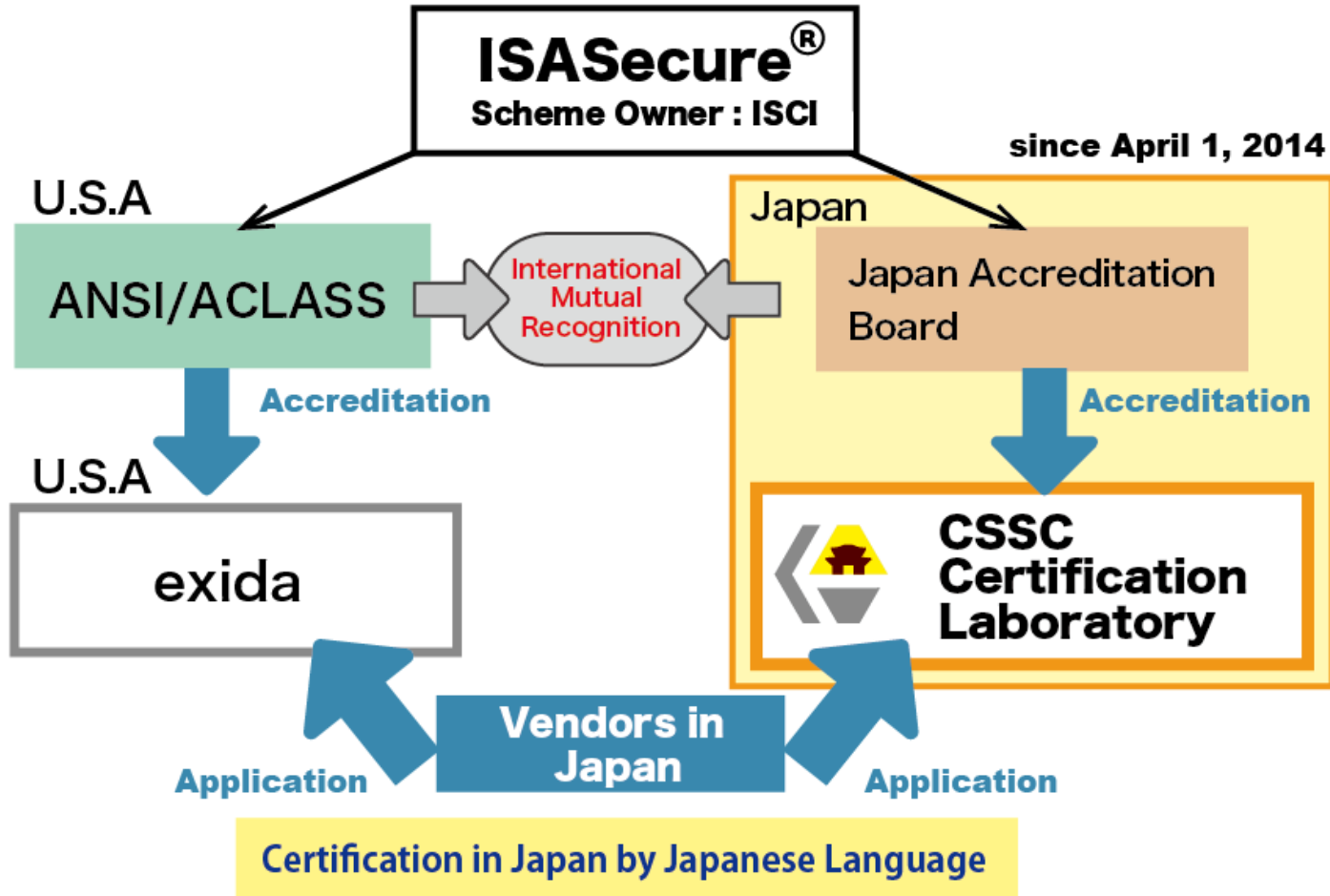
EDSA Certification

- IEC62443 is a standard that covers all control system security layers and players.
- The antecedent standards issued for testing and certification (e.g. EDSA and WIB certification) are to be used for IEC62443.



*1) IEC/TC65/WG10 oversees the task of standardization of IEC62443 cyber security (JEMIMA handles the Japan office).
 *2) EDSA: Embedded Device Security Assurance: Control device (component) certification program → Proposed to IEC62443-4.
 *3) WIB: International Instrument User's Association program → Proposed to IEC62443-2-4.
 DCS: Distributed Control System PLC: Programmable Logic Controller PIMS: Process Information Management System

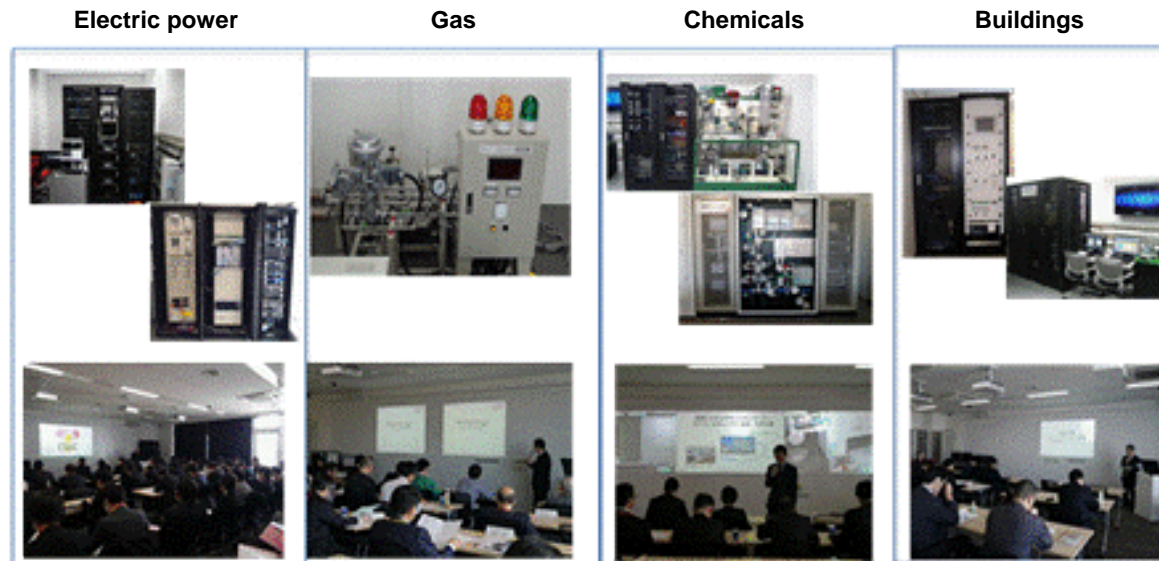
3)-2 Testing & Certification(Cont'd)



Outcome of R&D: Based on pilot certification service in 2013, CSSC-CL started operating an impartial and fair certification service from 2014.

4) Development of Human Resources Training Program: Cyber Security Practice

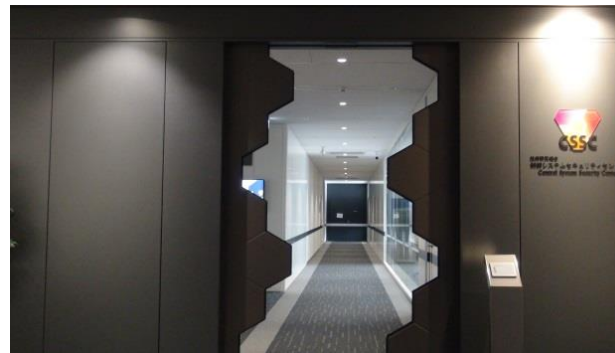
Purpose	Persons such as site supervisors, engineers, and related vendors in the fields of electric power, gas, buildings, and chemicals use a mock CSS-Base6 plant to develop awareness of security threats to control systems and practice cyber security with the purpose of verifying the validity of elements such as procedures for detecting the occurrence of security incidents and coping with resulting damage to promote the acquisition of knowledge with the focus on control system security measures in their respective fields.
Dates and Venues	4 sessions implemented in four fields using CSS-Base6 from December 2014 through February 2015
Participants	Cumulative total 216 people (including observers) participated in the exercises in FY 2014. Participation by entities and persons including industrial groups, operators, well-informed persons, and competent authorities.



Outcome of R&D: Growing awareness of the existence of security threats in each field and the need for countermeasures.

OVERVIEWS OF CONTROL SYSTEM SECURITY CENTER (CSSC)

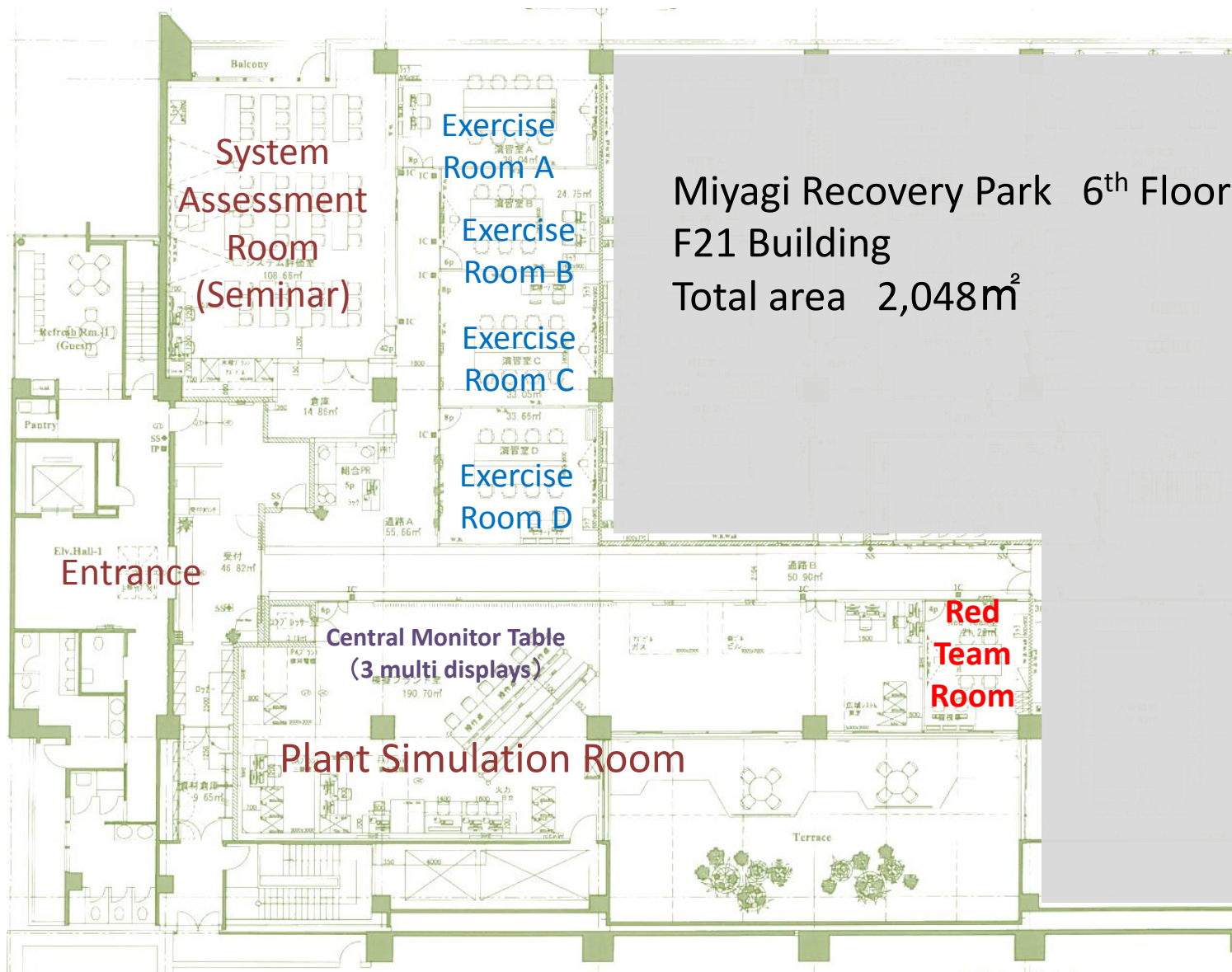
Tohoku Tagajo Headquarters (TTHQ)



Tagajo

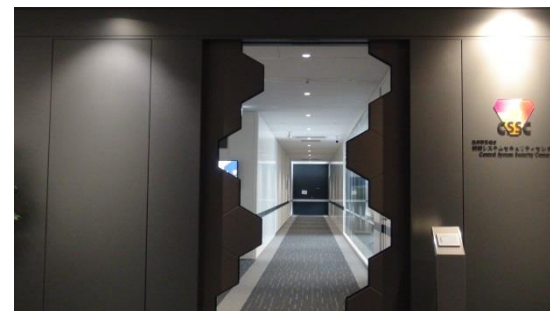
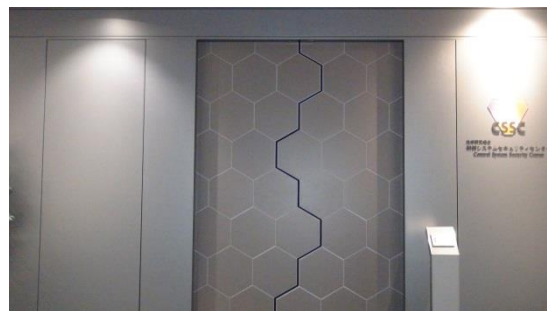
<http://www.css-center.or.jp/en/index.html>

Tohoku Tagajo Headquarters (Testbed : CSS-Base6)



Miyagi Recovery Park 6th Floor
 F21 Building
 Total area 2,048m²

Testbeds : Entrance and simulated central monitor room

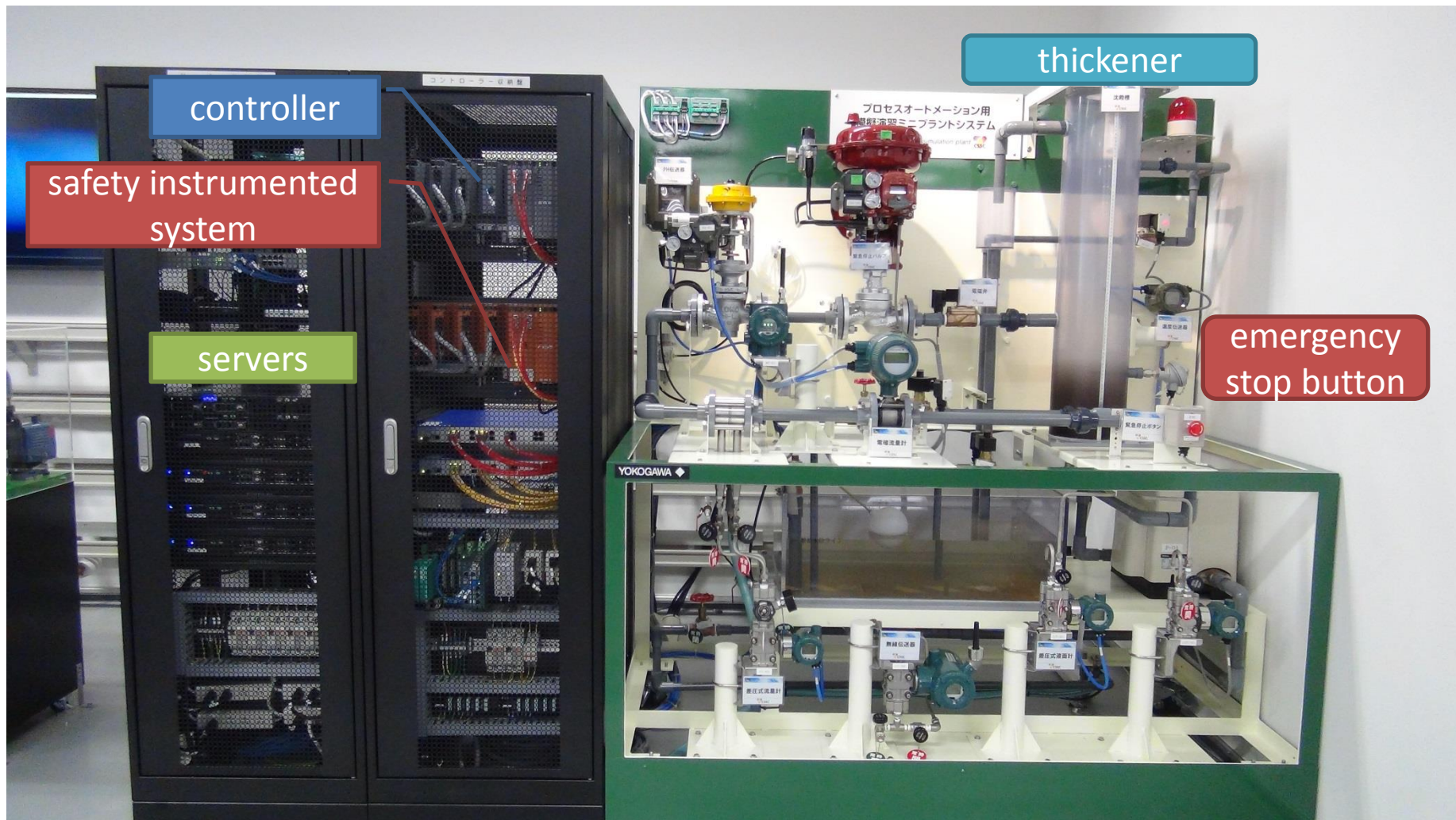


Plant simulations

- **Extracted characteristic functions of ICS**
- **Developed plant simulations for demonstration and cyber exercises**
- **Implemented 9 kinds of plant simulations**

- (1) Sewerage and drainage process automation system
- (2) Building automation system
- (3) Factory automation plant
- (4) Thermal electrical generating plant
- (5) Gas plant
- (6) Electrical substation for broad area (smart city)
- (7) Chemical process automation system
- (8) Factory automation plant 2
- (9) Building automation system 2

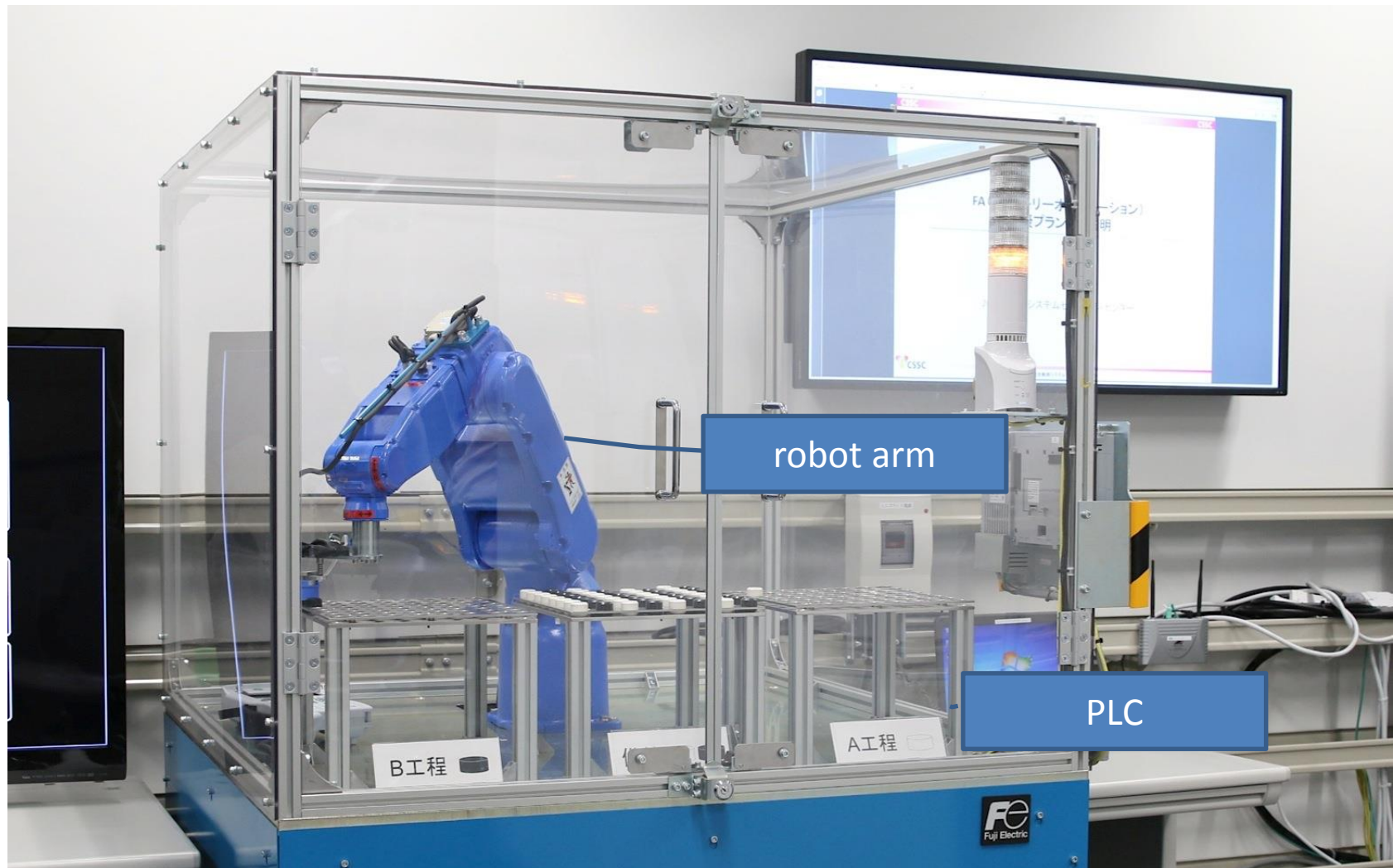
Plant simulation : (1) Sewerage and drainage process automation system



Plant simulation : (2) Building automation system



Plant simulation:(3) Factory automation plant



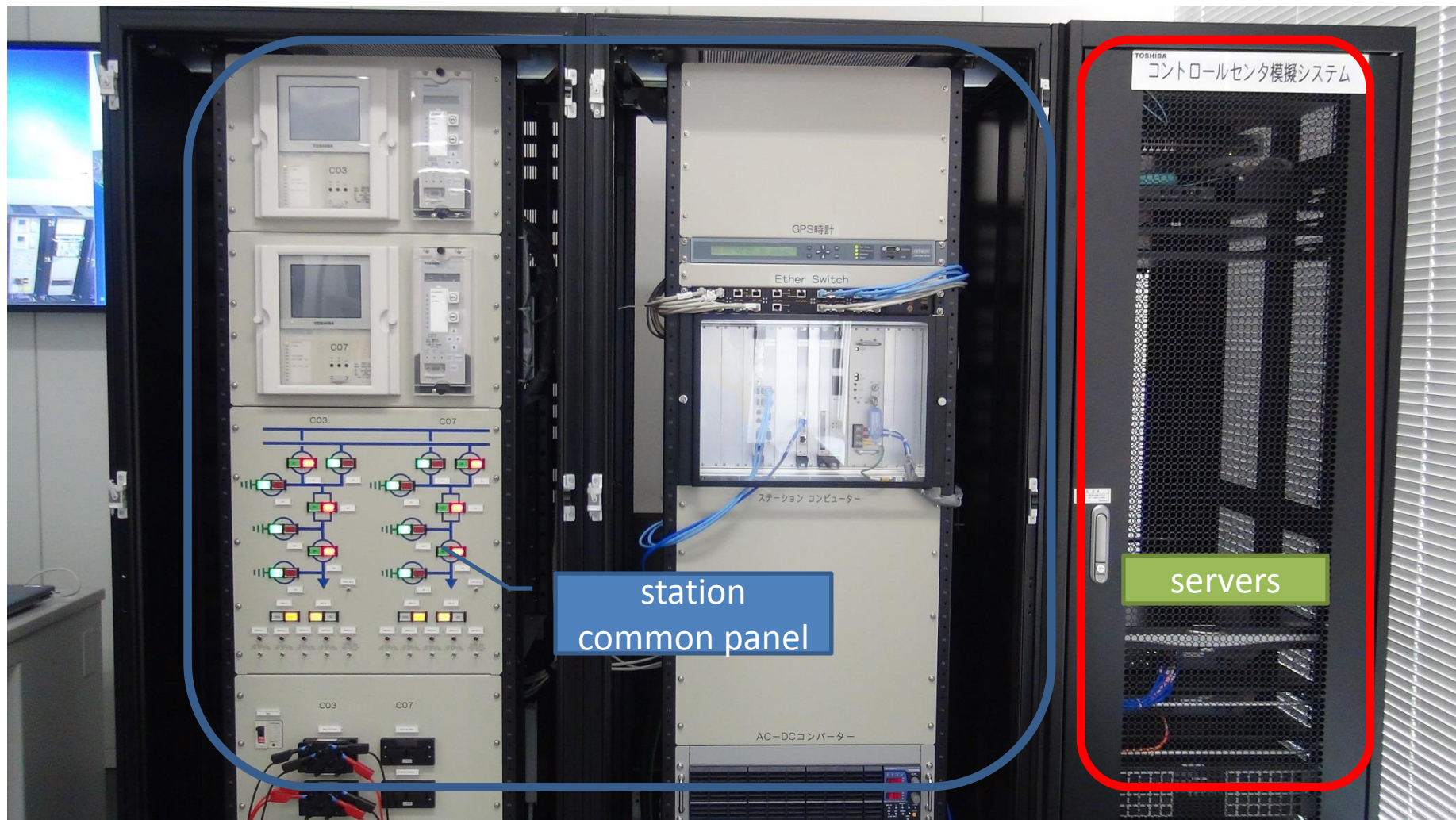
Plant simulation : (4) Thermal electrical generating plant



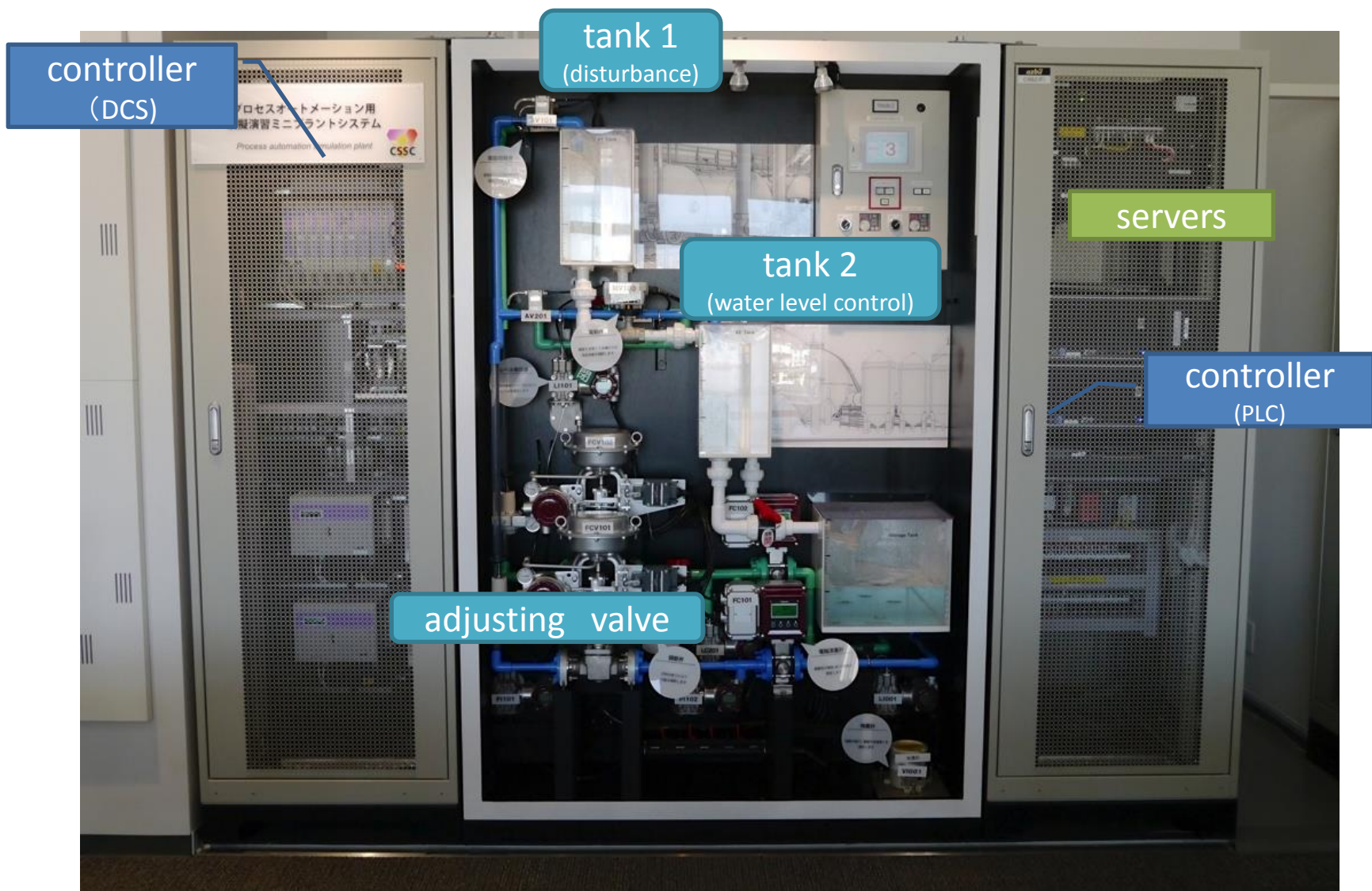
Plant simulation : (5) Gas plant



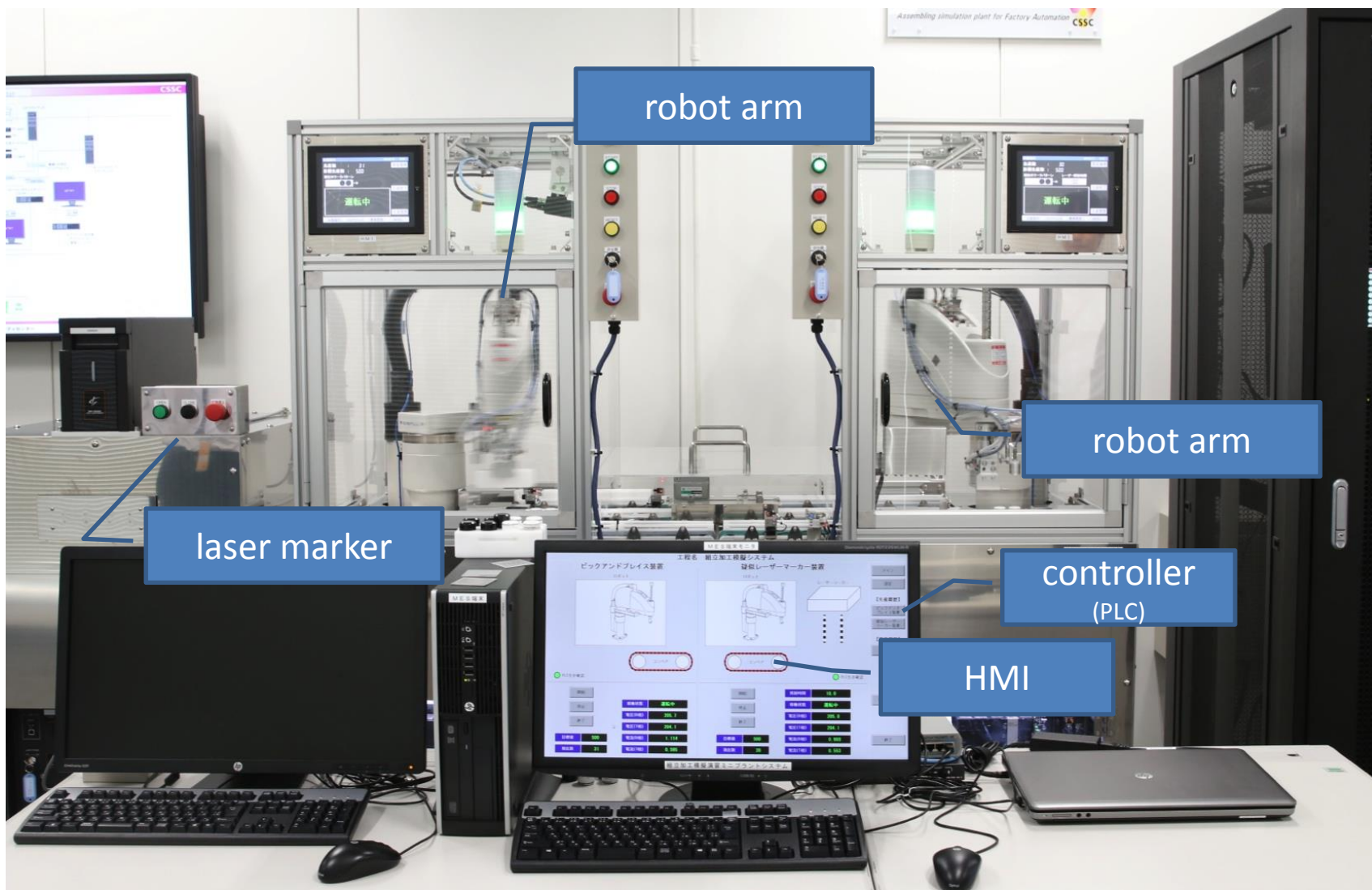
Plant simulation : (6) Electrical substation for broad area (smart city)



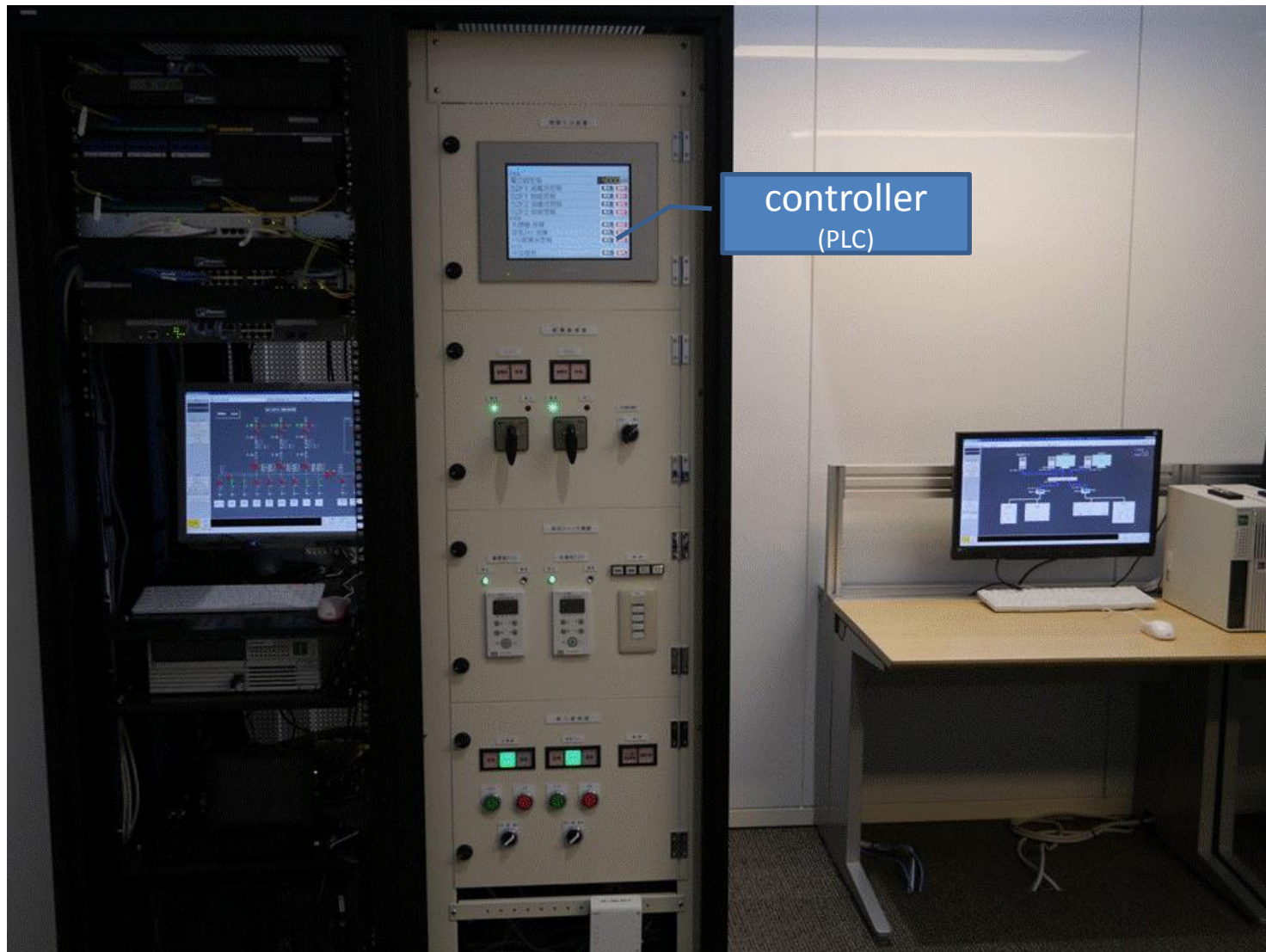
Plant simulation : (7) Chemical process automation system



Plant simulation : (8) Factory automation plant 2



Plant simulation : (9) Building automation system 2



Testbeds: other main features

- Tools for cyber attacks and fuzzing tools for testing and verifying ICS mainly of CSSC members
- Virtual network for R&D and verification environment in testbeds
- Rooms for verification activities
- System Assessment Room (full sitting numbers about 40) for seminars and awareness raising
- Blue team and red team cyber exercise
- JGN-X (research gigabit network provided by NICT) between Tohoku Tagajo Headquarters and Tokyo Research Center

Events and guests(1)

Year/Month	Events
2012.03	Established CSSC
2013.05	TTHQ opening ceremony
2013.09	Welcomed the senior vice minister for reconstruction
2013.09	Signed MOC with DHS in coordination with METI, AIST,IPA, JP
2013.12	Signed MOU with ENCS in Netherland
2014.01	Conducted Training Programs to Support Enhancement of Information Security in the ASEAN Region
2014.01	Welcomed the vice ministers of Defense and the vice minister of Education, Culture, Sports, Science and Technology
2014.01~03	Conducted Cyber security exercise FY2013
2014.02	Welcomed Cyber security researchers from England
2014.03	Welcomed the 1st Tagajo city Disaster risk reduction technology tour
2014.04	Started EDSA certification service and joined ISCI
2014.04	Signed MOU with CCI in Spain
2014.04	Welcomed ELECTRONIC TRANSACTIONS DEVELOPMENT AGENCY from Thailand
2014.04	Welcomed DENSEK(Distributed ENergy SEcurity Knowledge)
2014.04	Welcomed 12 mayors around CSS-Base6
2014.06	Welcomed senior vice minister of the cabinet office
2014.07	Welcomed the president of Japan Business Federation
2014.10	Signed a letter of intent (LoI) with ENCS
2014.11	Welcomed Meridian conference (security conference from 40 countries)
2014.11	Welcomed Deputy Secretary-General of Thai Industrial Standards Institute(TISI) and participants of "The Training Program on the Standards for Industrial-Process Measurement, Control and Automation[ENTS]"



Events and guests(2)

Year/Month	Events
2014.12~ 2015.02	Conducted Cyber security exercise FY2014
2015.01	Welcomed Chair of Special Mission Committee on IT Strategy, Liberal Democratic Party of Japan
2015.01	Conducted debrief session for CSSC special supporting member
2015.01	Welcomed the 2nd Tagajo city Disaster risk reduction technology tour
2015.03	Welcomed State Minister of Economy, Trade and Industry
2015.03	Welcomed the 3rd Tagajo city Disaster risk reduction technology tour
2015.04	Welcomed new employees of Tagajo city
2015.04	Welcomed ENCS
2015.05	Welcomed President of the Sendai Chamber of Commerce and Industry
2015.05	Conducted TTHQ site tour and annual debrief session for CSSC members
2015.06	Welcomed observation team of "Royal College of Defence Studies"
2015.07	Welcomed Professional Staff Member, Senate Armed Services Committee (SASC)
2015.07	Welcomed TOMODACHI - Mitsui & Co. Leadership Program observation team
2015.07	Welcomed the 4th Tagajo city Disaster risk reduction technology tour
2015.07	Welcomed United States Forces Japan
2015.08	Conducted CSSC tour for CSSC special supporting member
2015.09	Welcomed the House Administration Committee
2015.10	The organization for restructuring businesses after the Great East Japan Earthquake
2015.10	Welcomed National Conference of State Legislatures, The Council of State Governments



Events and guests(3)

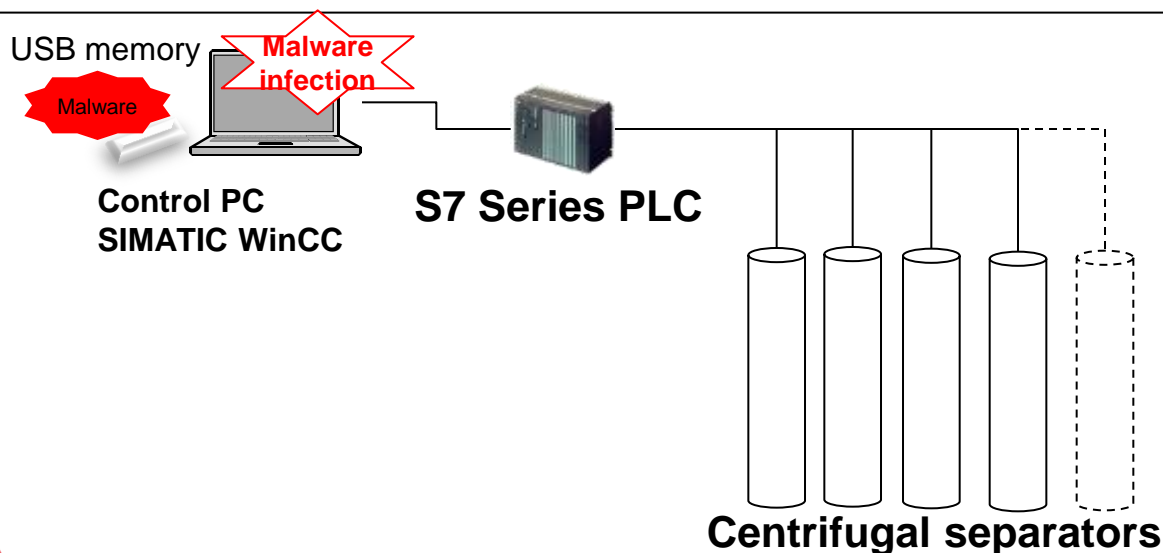
年月日	イベント等の内容
2015.10	Welcomed Qatar Science Campus Factory tour
2015.11	Welcomed Dutch Cyber Security Delegation
2015.11	Welcomed Italy - Japan Business Group
2015.12	Welcomed IECEE PSCWG3 Cyber Security TF
2015.12	Welcomed Estonian delegation
2015.12	Welcomed the 5th Tagajo city Disaster risk reduction technology tour
2016.02	Welcomed trainees from ASEAN countries
2016.05	Welcomed the House of Representatives' Committee on the Cabinet
2016.07	Welcomed the 7th Tagajo city Disaster risk reduction technology tour
2016.09	Welcomed U.S. Ambassador to Japan Caroline Kennedy



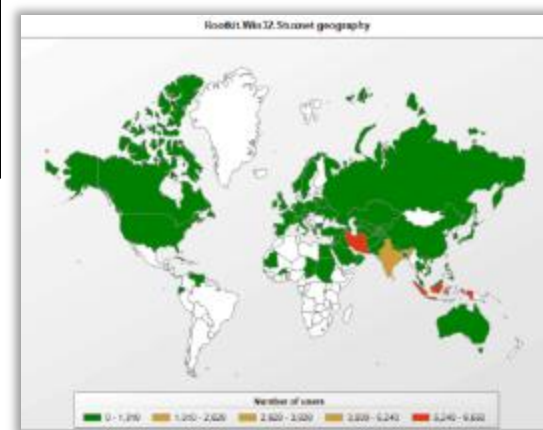
Our guests since the opening
Over 6,100 people / 1,200 times of plant demo
more than 400 oversea guests
 (as of April 1, 2017)

Appendix: Overview of Stuxnet

- In September 2010, a cyber attack was launched targeting **uranium-enriching centrifugal separators** at a nuclear fuel facility in Iran.
- The attack exploited four unknown vulnerabilities in Windows so that infection would occur when PC users displayed USB memory content using Windows Explorer.
- It was reported that the centrifugal separators were overloaded, resulting in destruction of 20%.
- It is also rumored that Stuxnet has caused a major setback (approximately three years) in Iran's nuclear development program.



Country-specific infection counts confirmed by Symantec



Source: <http://ebiquity.umbc.edu/blogger/2010/09/23/is-stuxnet-a-cyber-weapon-aimed-at-an-iranian-nuclear-site/>