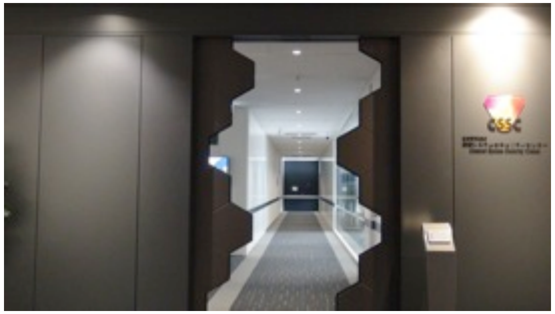
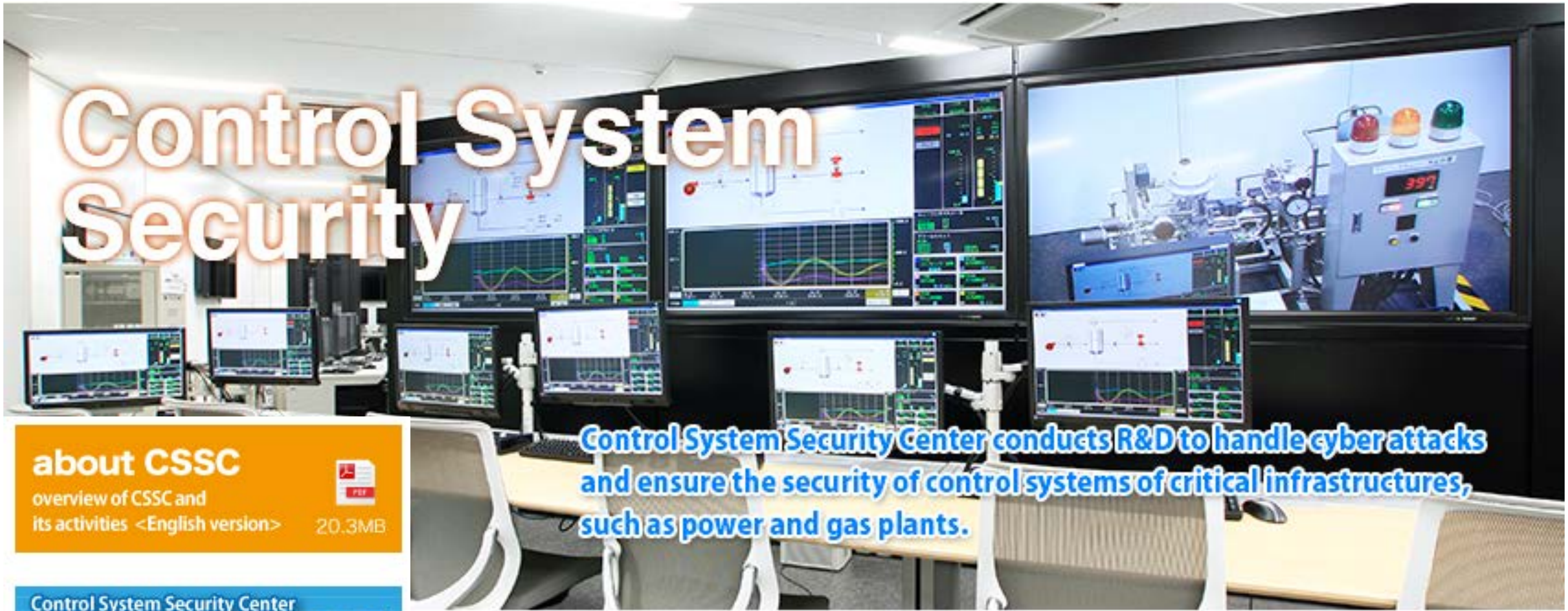
INTRODUCING THE ACTIVITIES OF CONTROL SYSTEM SECURITY CENTER(CSSC)

CSSC
制御システムセキュリティセンター
Control System Security Center
6



1. Background
2. Overviews of CSSC
3. Activities of CSSC



Control System Security

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

about CSSC
overview of CSSC and its activities <English version> 20.3MB

Control System Security Center Tohoku Tagaho 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

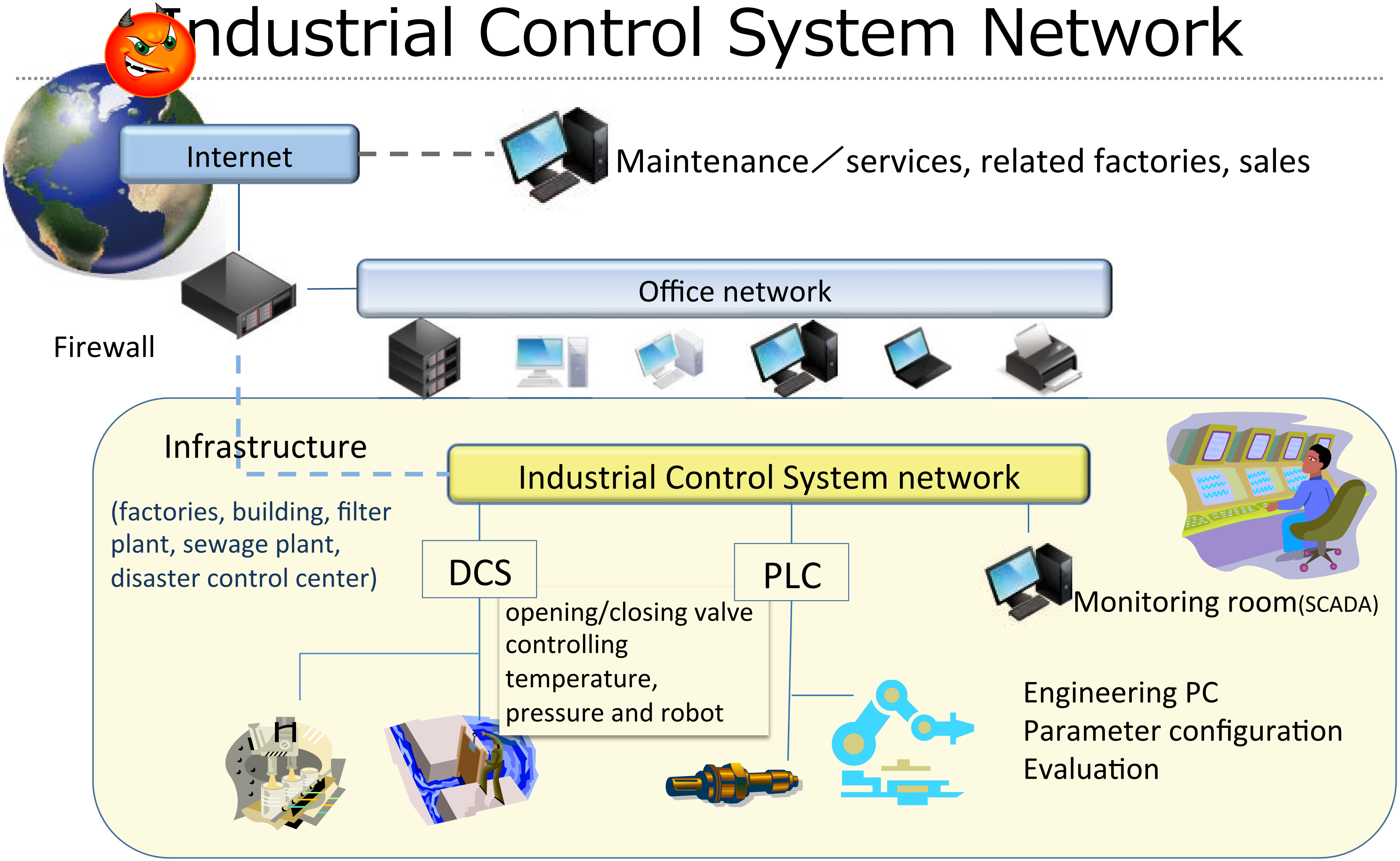
http://www.css-center.or.jp/en/index.html

CSSC Promotion Video About 8 Minutes

If Tokyo city falls into wide-area blackout, ・・・・・・・・

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

Industrial Control System Network

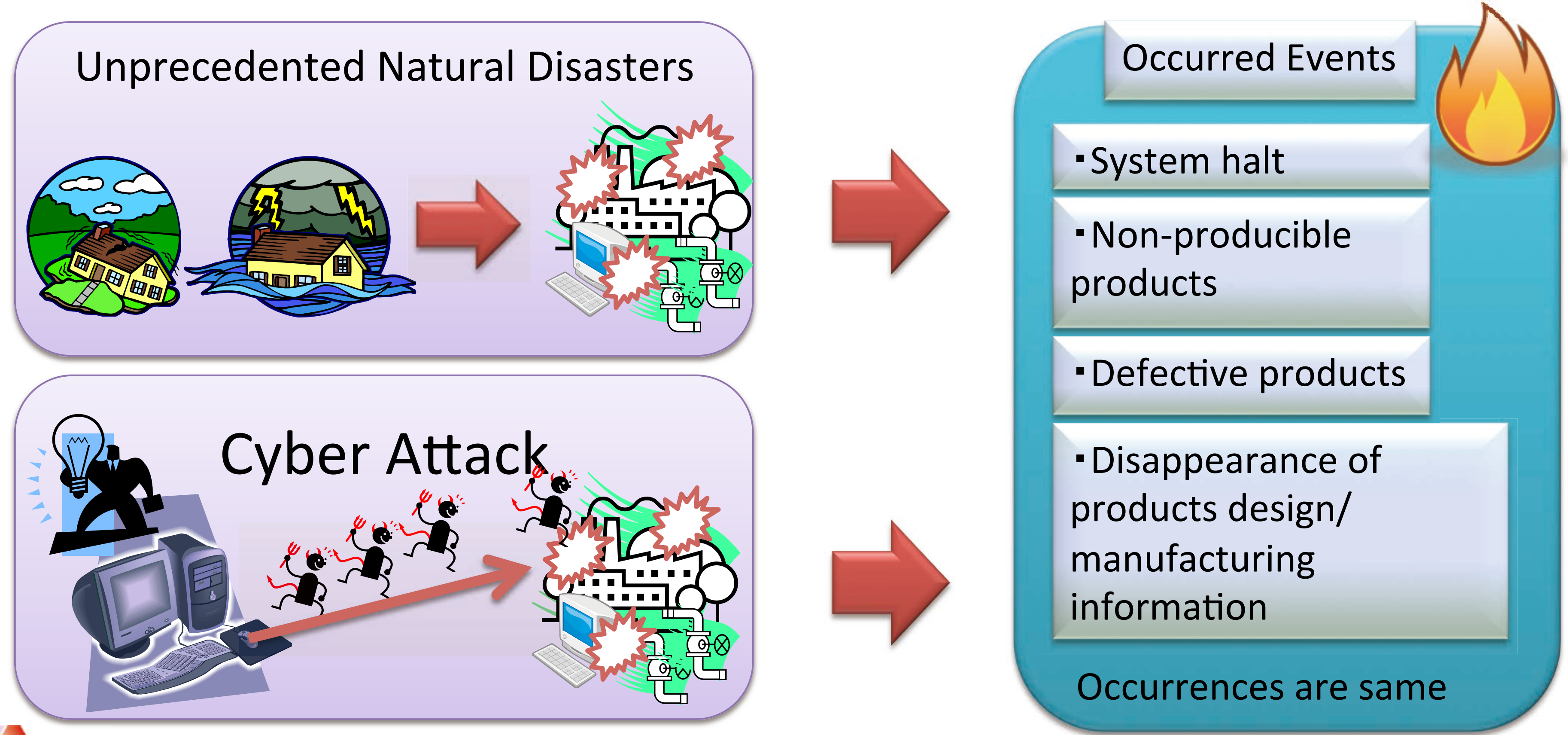

Internet
Maintenance／services, related factories, sales
Office network
Firewall
Infrastructure
(factories, building, filter plant, sewage plant, disaster control center)
Industrial Control System network
DCS
PLC
opening/closing valve controlling temperature, pressure and robot
Monitoring room(SCADA)
Engineering PC
Parameter configuration
Evaluation

DCS: Distributed Control System
PLC: Programmable Logic Controller

SCADA: Supervisory Control And Data Acquisition

Threat against Industrial Control System (ICS)

- **Cyber attack targeted ICS which surveils and controls power stations and plan operation**
  - **Oversea case that plant shutdown for a week overseas**
  - **Japanese cases that infected 100 PCs of plant facility or shutdown of automation factory systems**



Unprecedented Natural Disasters

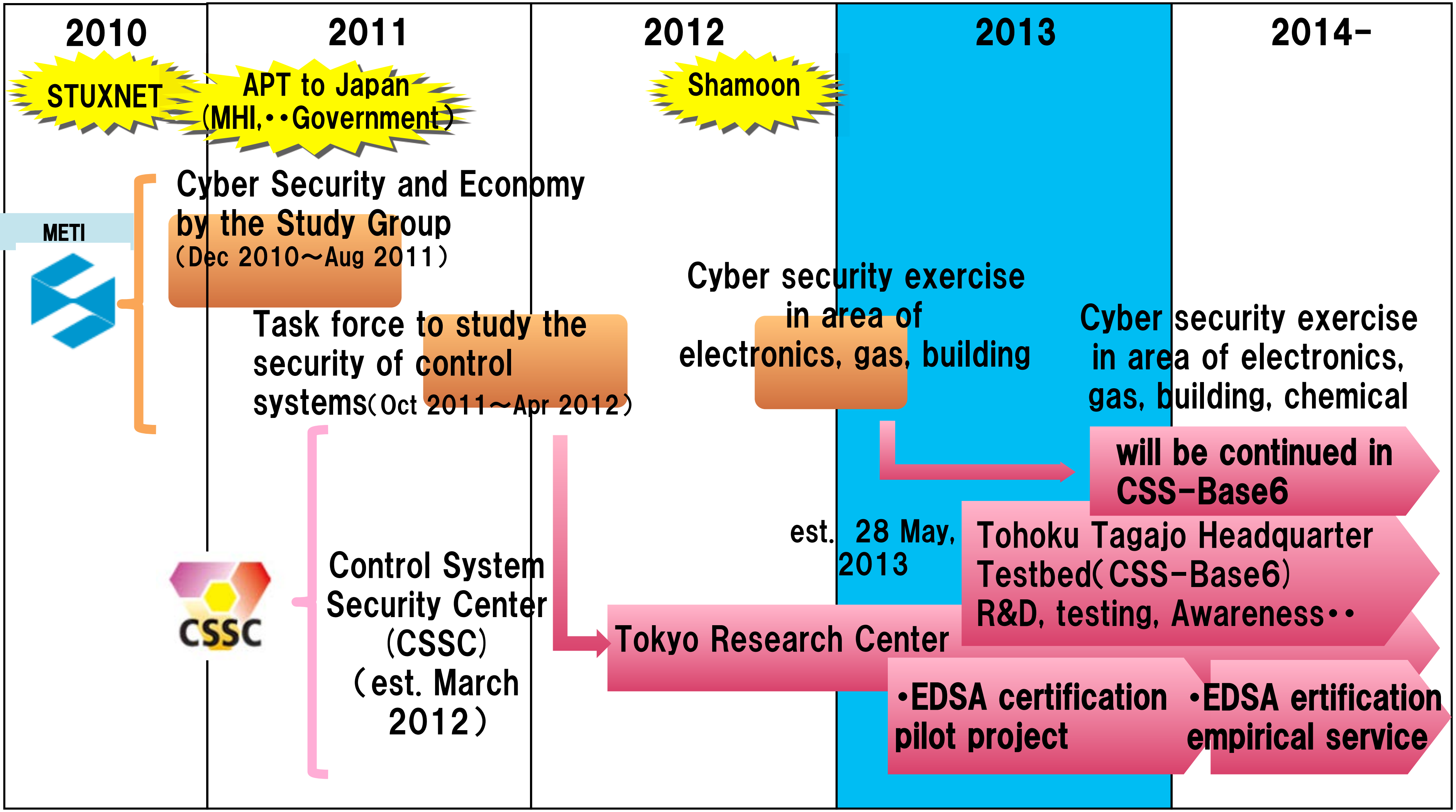
Cyber Attack

Occurred Events

- System halt
- Non-producible products
- Defective products
- Disappearance of products design/ manufacturing information

Occurrences are same

Activities on Control System Security in Japan



2010

2011

2012

2013

2014-

STUXNET

APT to Japan (MHI,••Government)

Shamoon

METI

Cyber Security and Economy by the Study Group (Dec 2010～Aug 2011)

Task force to study the security of control systems(Oct 2011～Apr 2012)

Cyber security exercise in area of electronics, gas, building

Cyber security exercise in area of electronics, gas, building, chemical

will be continued in CSS-Base6

CSSC

Control System Security Center (CSSC) (est. March 2012)

est. 28 May, 2013

Tohoku Tagajo Headquarter Testbed(CSS-Base6) R&D, testing, Awareness••

Tokyo Research Center

•EDSA certification pilot project

•EDSA ertification empirical service

◇To ensure ICS security of Japanese critical infrastructure

◇Evaluation and certification for ICS product exporters in Japan

Activities on ICS† Security in Japan

- Ministry of Economy, Trade and Industry (METI) has led continuous discussion on control system security in Japan

Cyber security and Economy study meeting (METI)

2010/12 → 2011/8

<Overview>

Recently intellectual property and life line related facilities are repeatedly targeted by cyber attackers. From the point of economic growth and nation's security, information security needs to be examined.

◇Main issues:

･Ensure ICS security

･Response to Targeted Attack

･Educate information security workforce

Control System Security **Task Force** (METI)

2011/10 → 2012/4

<Overview>

Based on the "cyber security and economy study meeting", following two issues are specified that should be examined more.

◇To ensure ICS security of Japanese critical infrastructure

◇Evaluation and certification for ICS product exporters in Japan

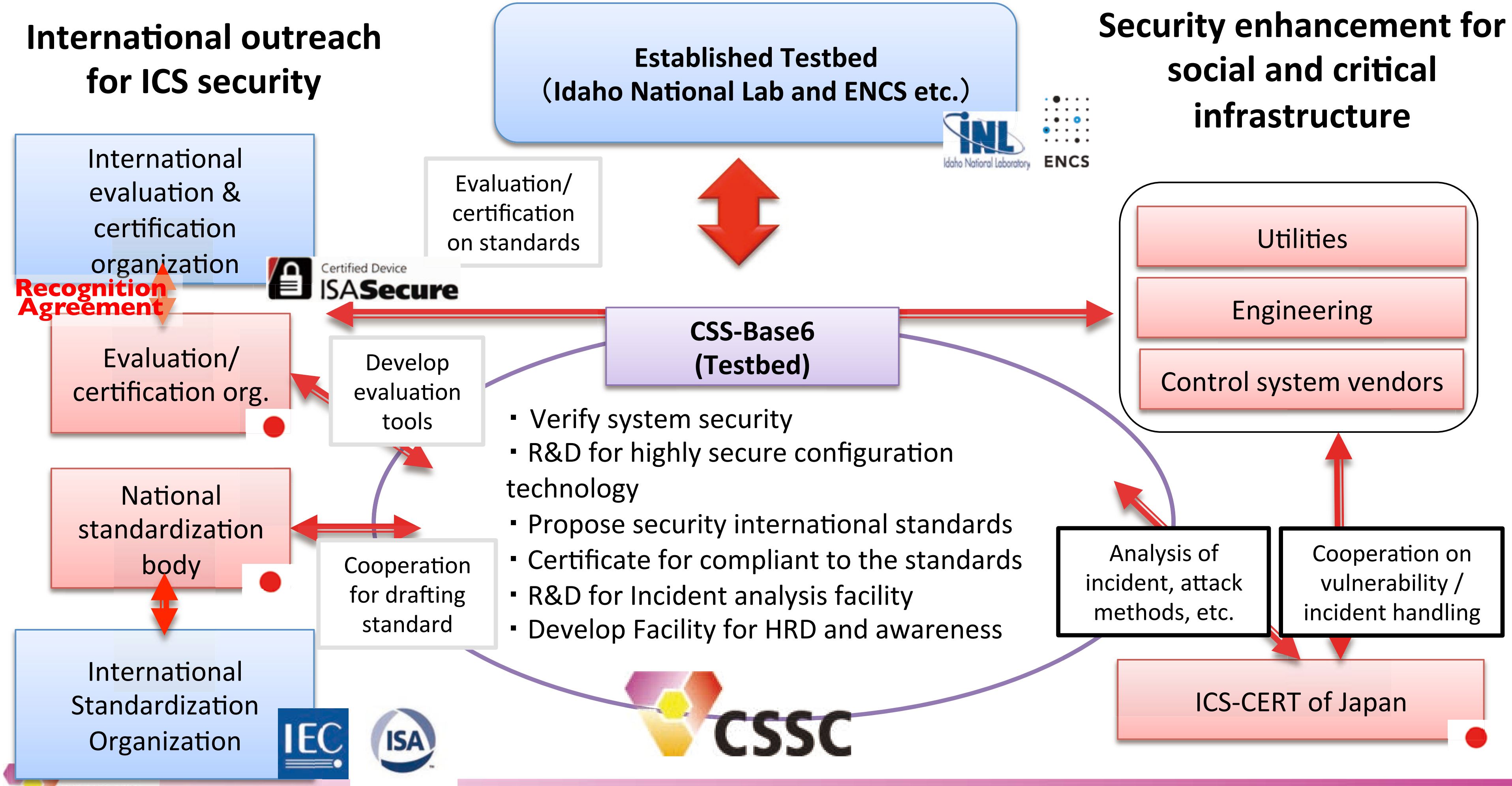
＜ Working Groups under the Task Force ＞

- Standardization WG(IPA)
- Evaluation and Certification Scheme WG (IPA)
- Incident Handling WG
- Testbed WG
- Workforce Training WG
- Promotion and education WG

†ICS : Industrial Control System that Includes smart grid devices (smart meter), plants, HEMS and BEMS) etc.

Concept of Cyber-security Testbed

- Control System Security Center (CSSC) would develop a cyber-security testbed in FY2012 funded by the Japanese Government (METI).
- Evaluation, certification and incident analysis would be conducted using the testbed.



International outreach for ICS security

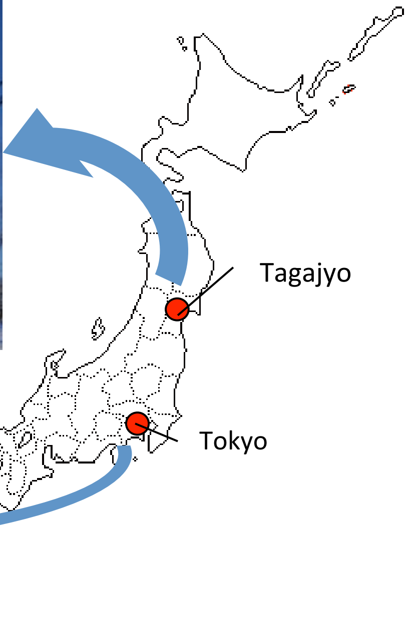
Security enhancement for social and critical infrastructure

Established Testbed
(Idaho National Lab and ENCS etc.)
INL Idaho National Laboratory
ENCS
International evaluation & certification organization
Recognition Agreement
Certified Device ISASecure
Evaluation/ certification on standards
Evaluation/ certification org.
Develop evaluation tools
National standardization body
Cooperation for drafting standard
International Standardization Organization
IEC
ISA
CSS-Base6 (Testbed)
Utilities
Engineering
Control system vendors
Analysis of incident, attack methods, etc.
Cooperation on vulnerability / incident handling
ICS-CERT of Japan
CSSC

・Verify system security
・R&D for highly secure configuration technology
・Propose security international standards
・Certificate for compliant to the standards
・R&D for Incident analysis facility
・Develop Facility for HRD and awareness

OVERVIEWS OF CONTROL SYSTEM SECURITY CENTER（CSSC)

Tohoku Tagajo Headquarters (TTHQ)



Tokyo Research Center (TRC)

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

Taga-jo?　多賀城

- Jo = 城 = 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)

多賀城南門　復元図

- 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

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

(Mayor of Tagajo)

Source: http://www.city.tagajo.miyagi.jp/

Control System Security Center (CSSC)

■Organizational overview

Name	**Control System Security Center** (Abbreviation) **CSSC** ※A corporation authorized by the Minister of Economics, Trade and Industry	**Association members** (In alphabetical order)	**Total 23 corporations (As of Dec, 2013)** *8 starting member corporations • Advanced Institute of Science and Technology* • Azbil Corporation * • Fuji Electric Co., Ltd. • FUJITSU LIMITED • Hitachi, Ltd.* • Information Technology Promotion Agency • Japan Quality Assurance Organization • LAC Co., Ltd., • McAfee Co.,Ltd. • Mitsubishi Electric Corporation • Mitsubishi Heavy Industries Ltd.* • Mitsubishi Research Institute Inc.* • Mori Building Co., Ltd.* • NEC Corporation • NRI Secure Technologies Ltd. • NTT Corporation • OMRON Corporation • The University of Electro-Communications, • Tohoku Information Systems Company, Incorporated • Toshiba Corporation* • Toyota InfoTechnology Center Co., Ltd. • Trend Micro Incorporated • Yokogawa Electric Corporation*
Established	March 6, 2012 (The registration date)		
Location	**[Tohoku Tagajo Headquarters (TTHQ)]** Tagajo City, Miyagi, Japan **[Tokyo Research Center (TRC)]** National Institute of Advanced Industrial Science and Technology Waterfront, Tokyo, Japan		

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

CSSC Association Members (As of DEC 19, 2013)

AIST
NATIONAL INSTITUTE OF ADVANCED INDUSTRIAL SCIENCE AND TECHNOLOGY (AIST)

azbil

FUJITSU

Fuji Electric

HITACHI
Inspire the Next

IPA

JQA
一般財団法人 日本品質保証機構

LAC 株式会社ラック

McAfee
An Intel Company

MITSUBISHI ELECTRIC
Changes for the Better

MITSUBISHI HEAVY INDUSTRIES, LTD.
Our Technologies, Your Tomorrow

MORI

NEC Empowered by Innovation

NRI SECURE TECHNOLOGIES

NTT Communications

OMRON

TOiNX

TOSHIBA
Leading Innovation >>>

TOYOTA
InfoTechnology Center Co., Ltd.

TREND MICRO™

YOKOGAWA

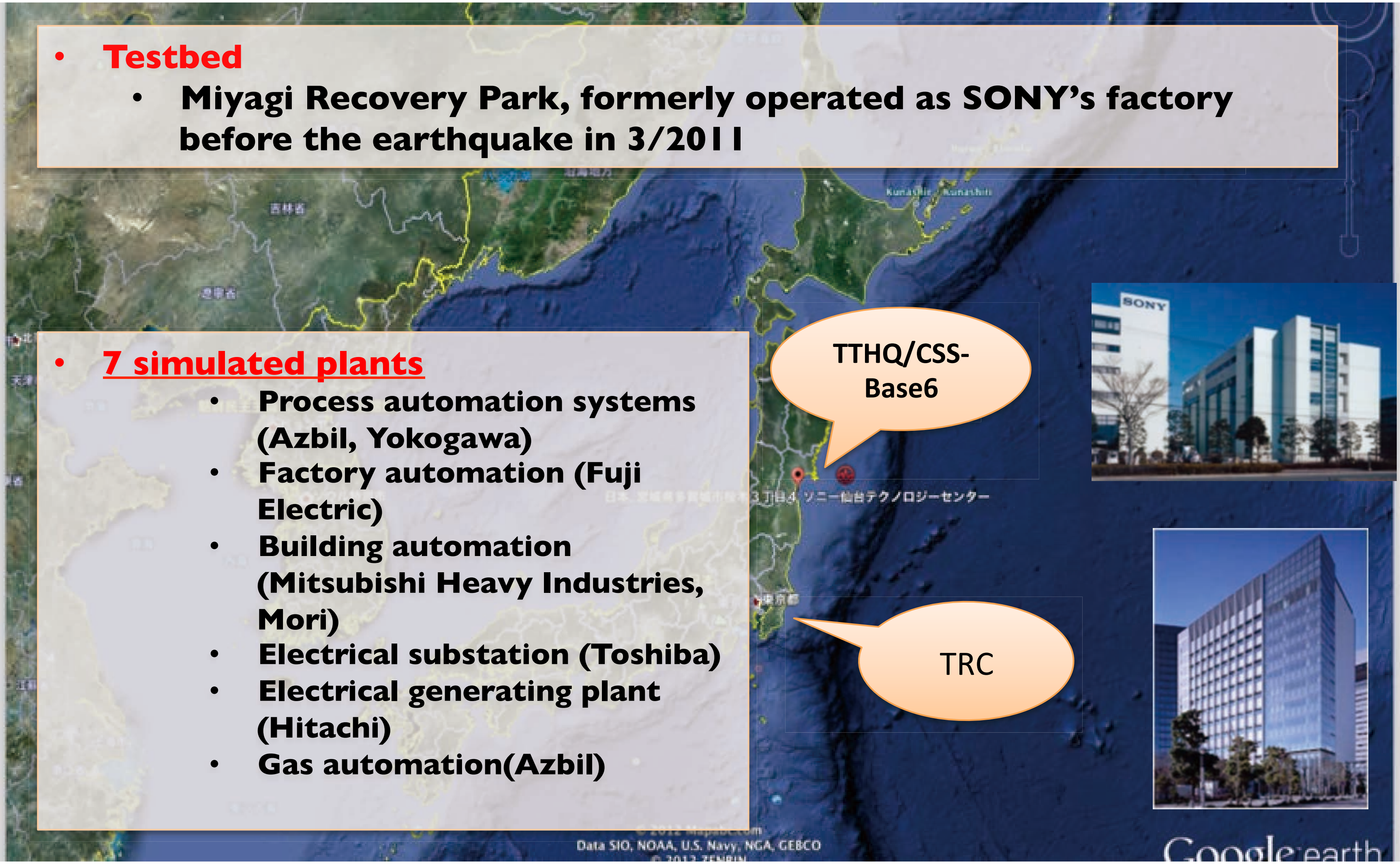
UEC TOKYO 国立大学法人 電気通信大学

Mitsubishi Research Institute, Inc.

CSS-Base6 (the testbed of CSSC)

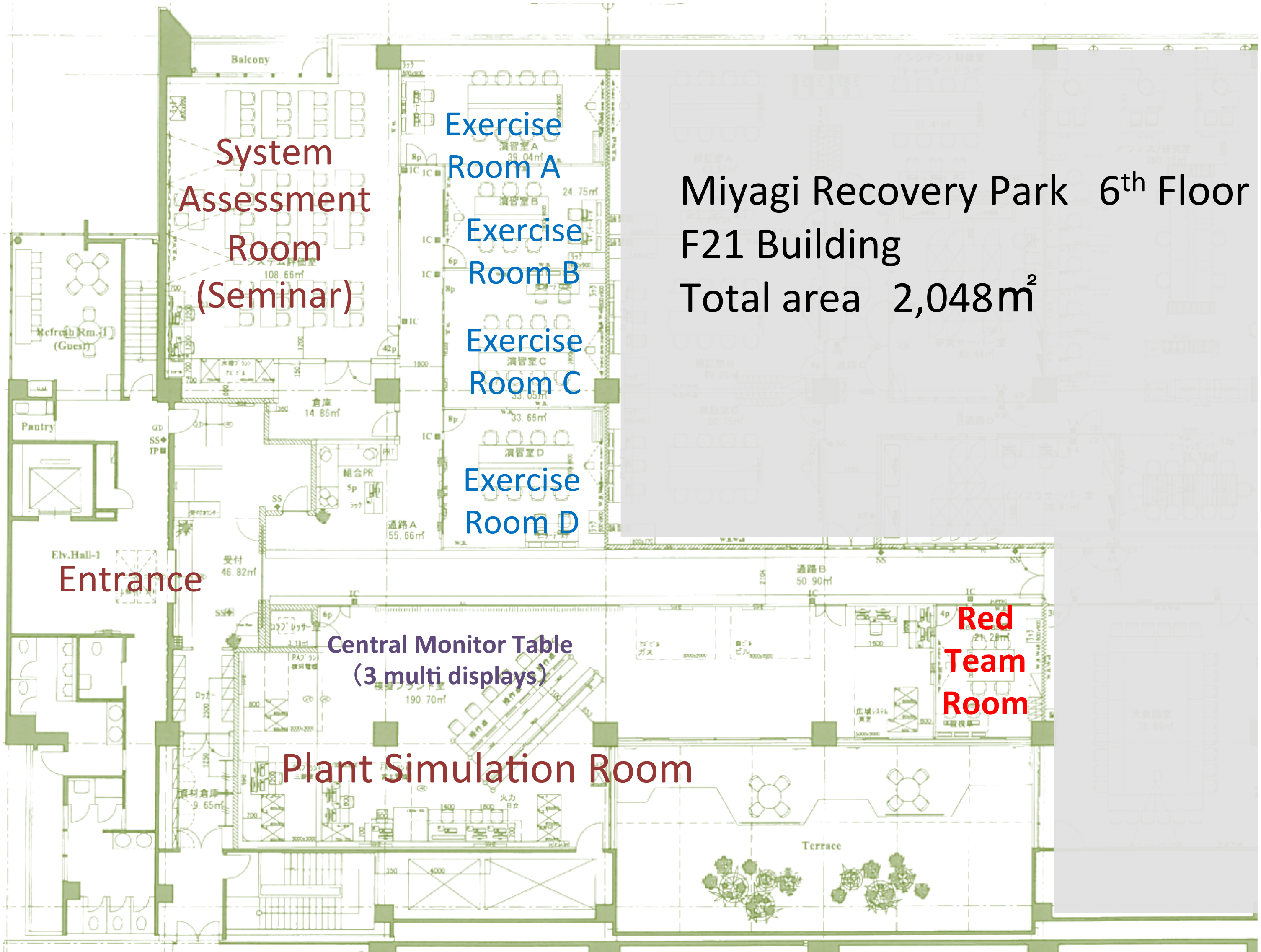
- **Testbed**
  - **Miyagi Recovery Park, formerly operated as SONY's factory before the earthquake in 3/2011**

- **7 simulated plants**
  - **Process automation systems (Azbil, Yokogawa)**
  - **Factory automation (Fuji Electric)**
  - **Building automation (Mitsubishi Heavy Industries, Mori)**
  - **Electrical substation (Toshiba)**
  - **Electrical generating plant (Hitachi)**
  - **Gas automation(Azbil)**


TTHQ/CSS-Base6
ソニー仙台テクノロジーセンター
TRC
SONY
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
Google earth

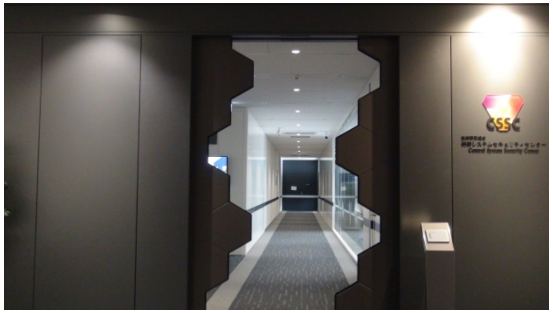
Source: Google earth

Tohoku Tagajo Headquarters （Testbed : CSS-Base6）



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

Testbed : Entrance and simulated central monitor table

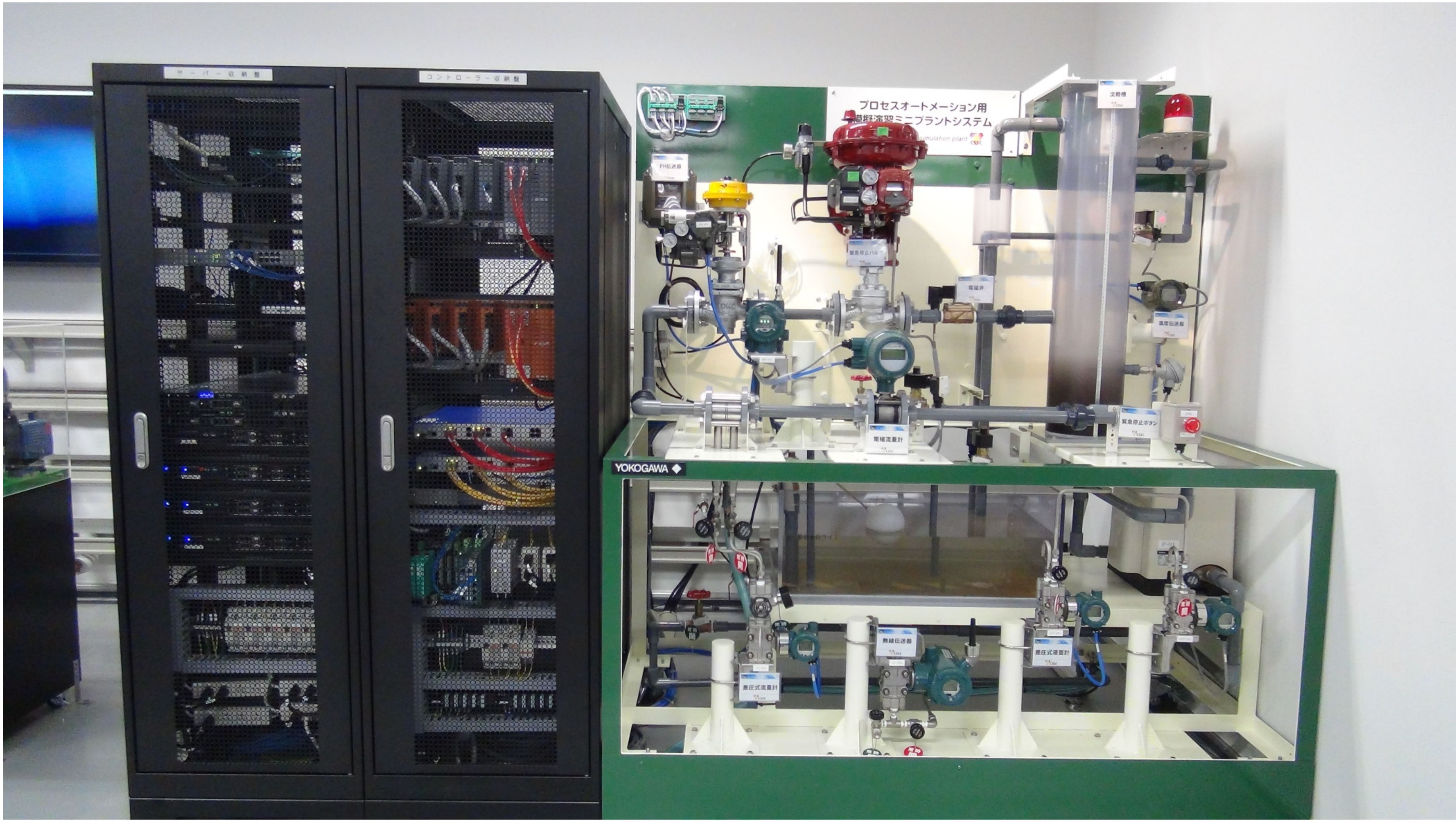


Plant simulations

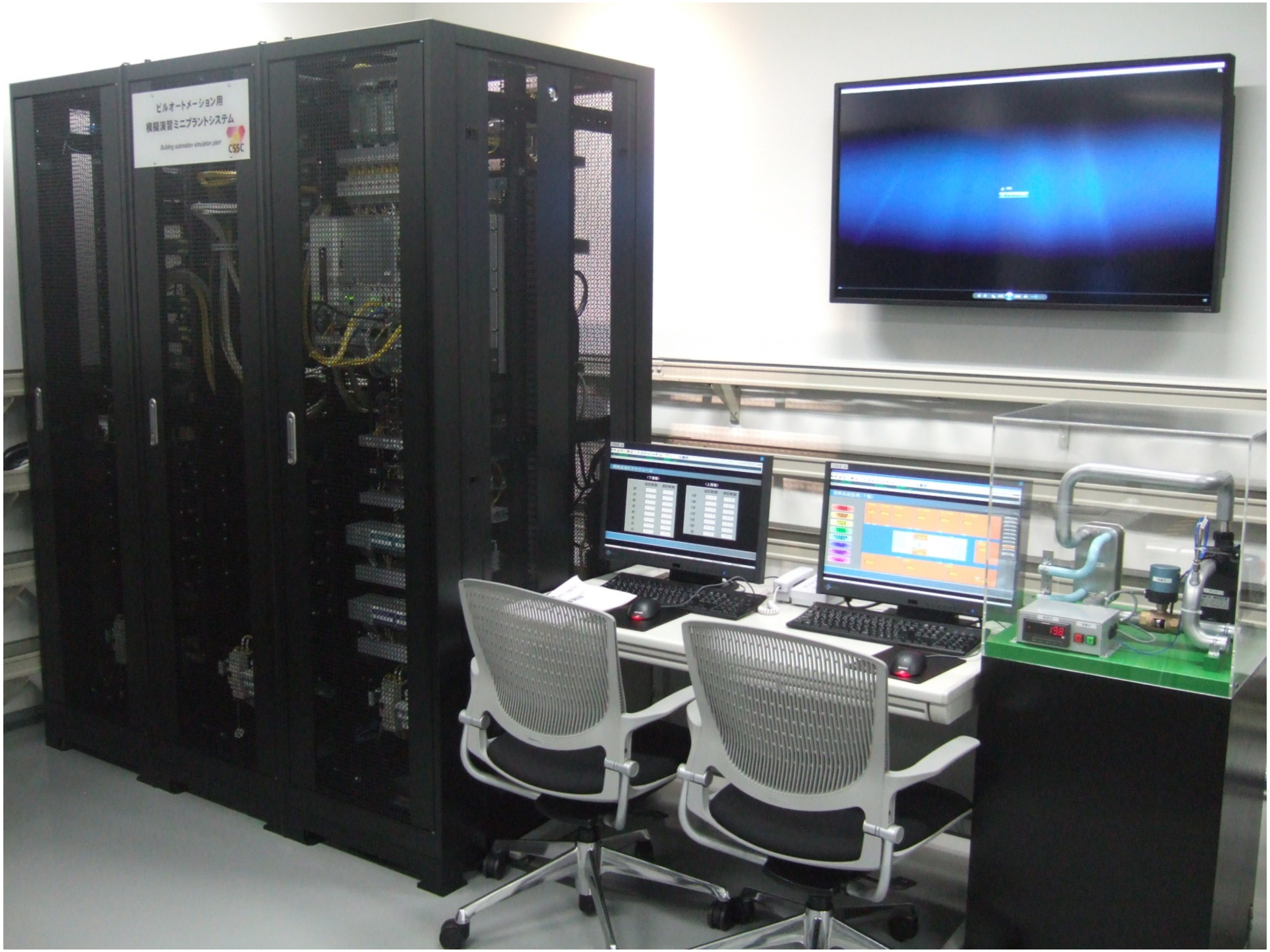
- **Extracted characteristic functions of ICS**
- **Developed plant simulations for demonstration and cyber exercises**
- **Implemented 7 kinds of plan simulations**

（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

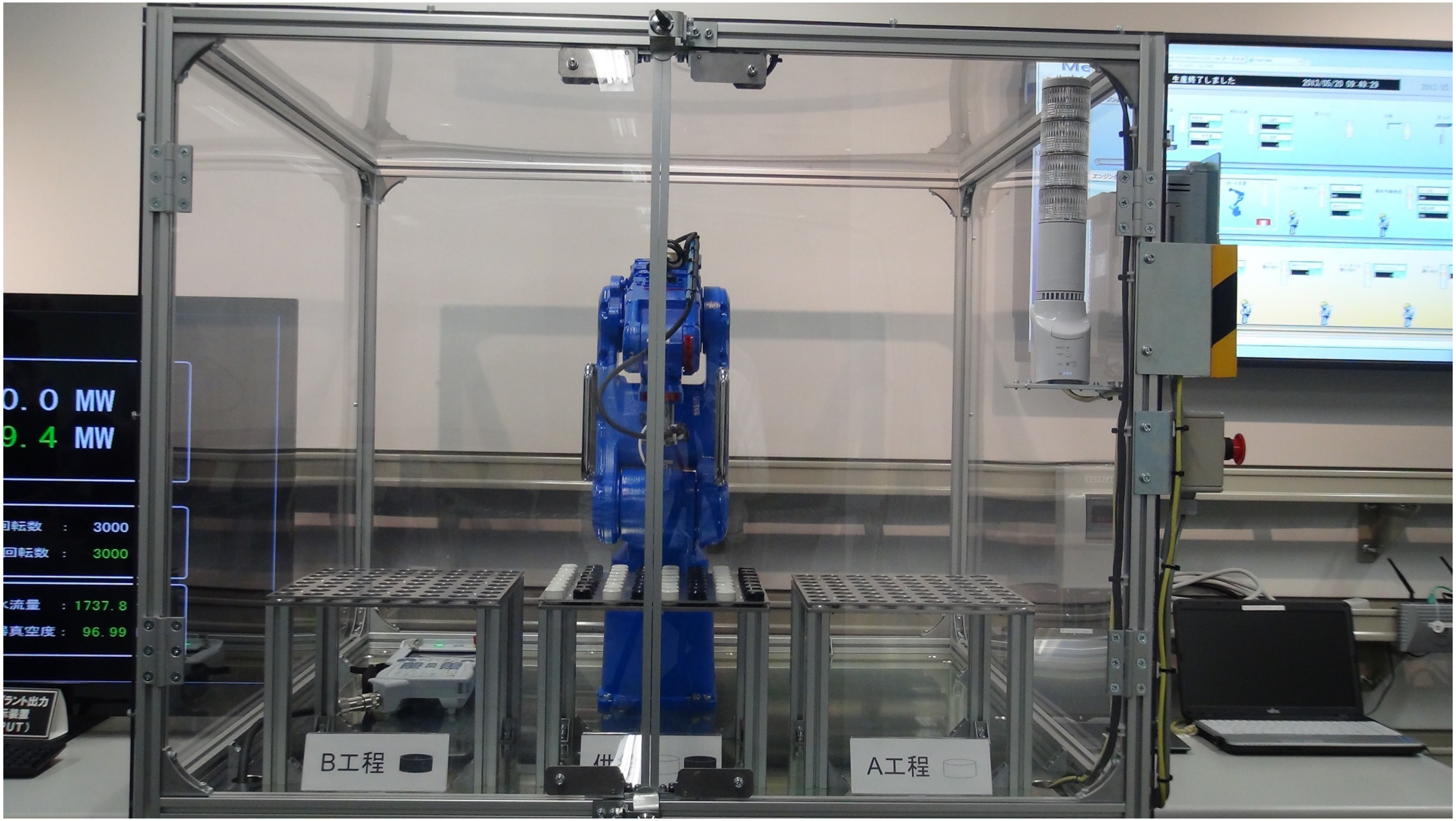
Plant simulation： （１） Sewerage and drainage process automation system



Plant simulation : （２） Building automation system

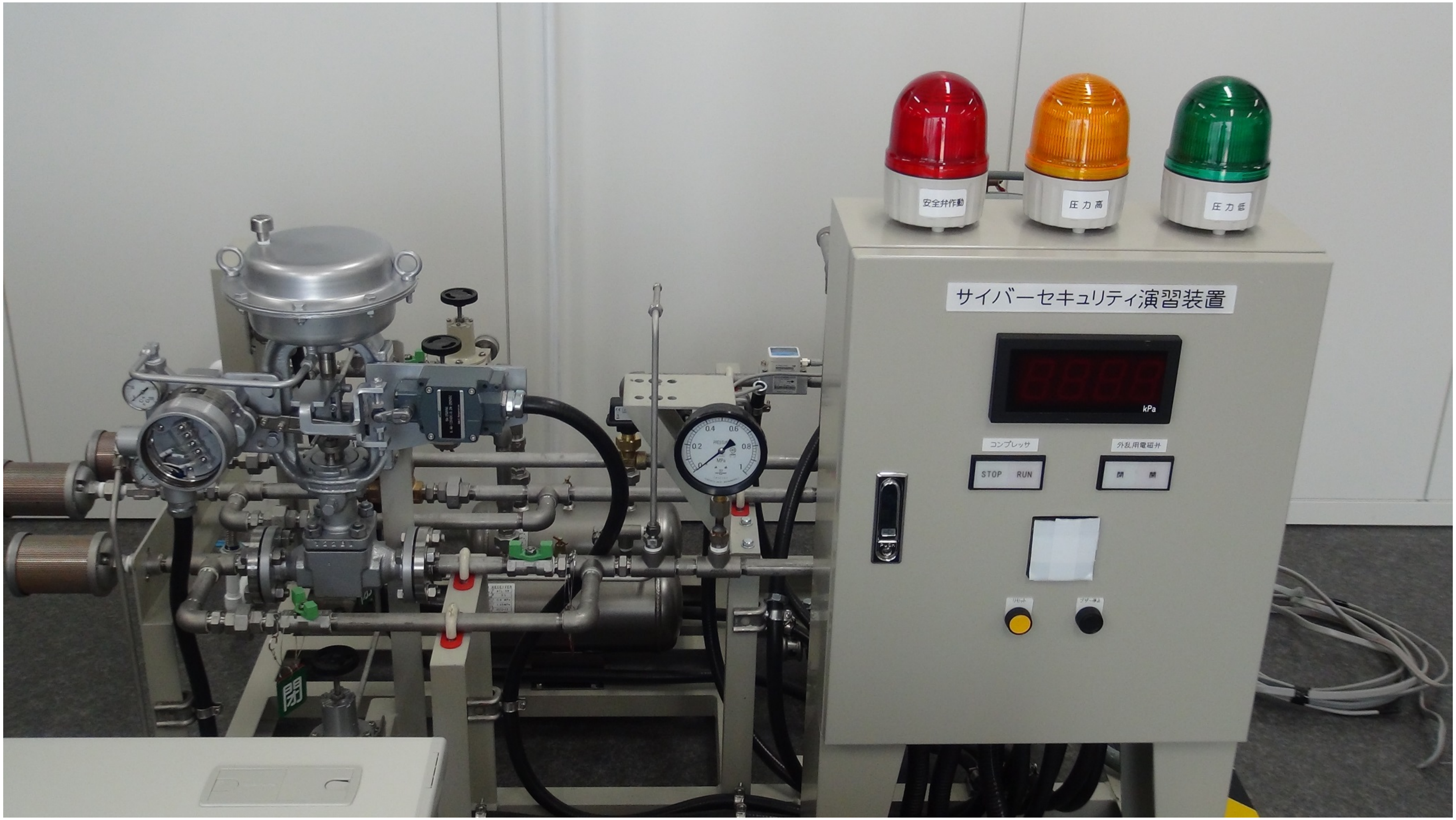

ビルオートメーション用
模擬演習ミニプラントシステム
Building automation simulation plant
CSSC

Plant simulation:(3) Factory automation plant

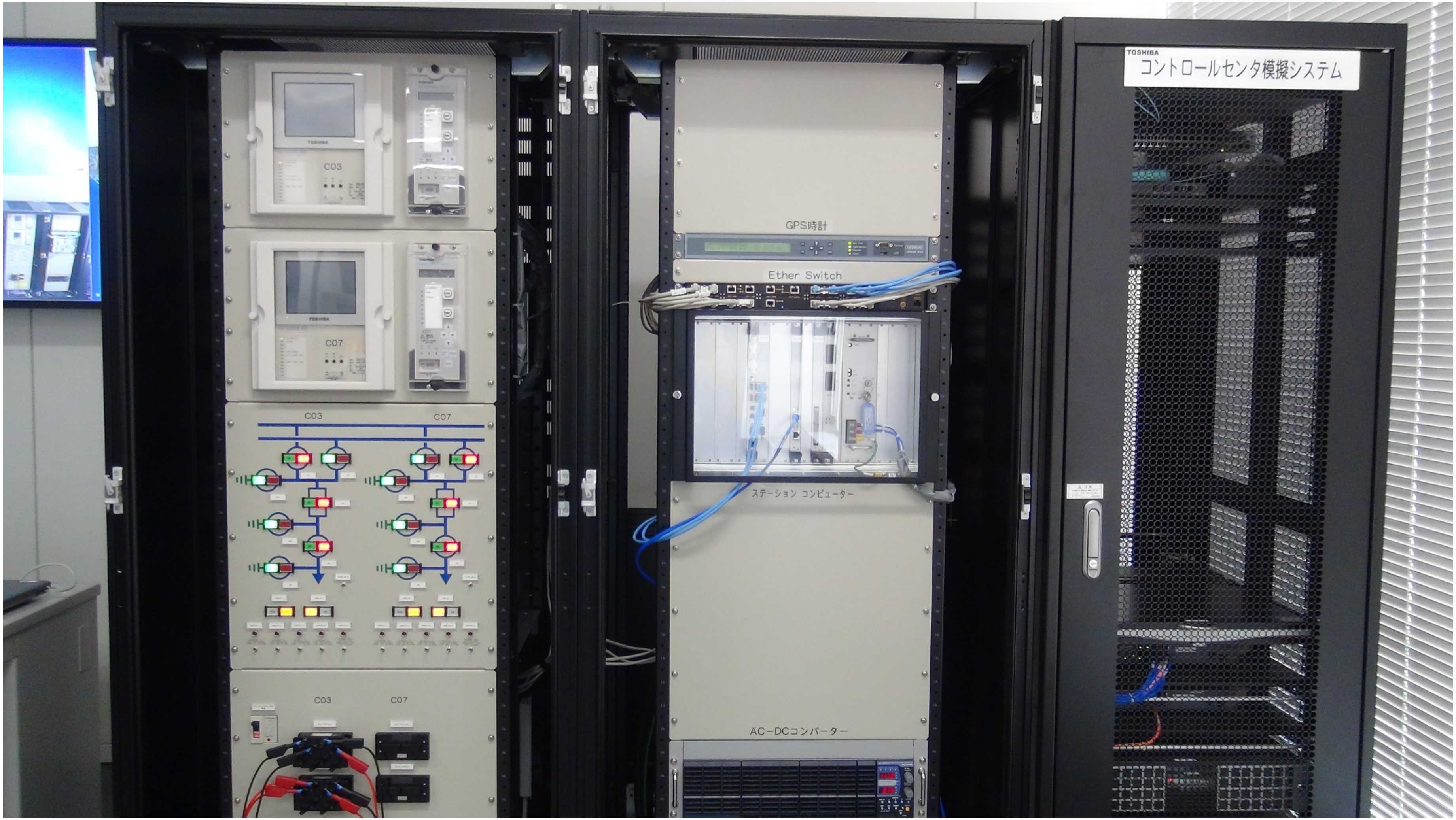


Plant simulation : （４） Thermal electrical generating plant

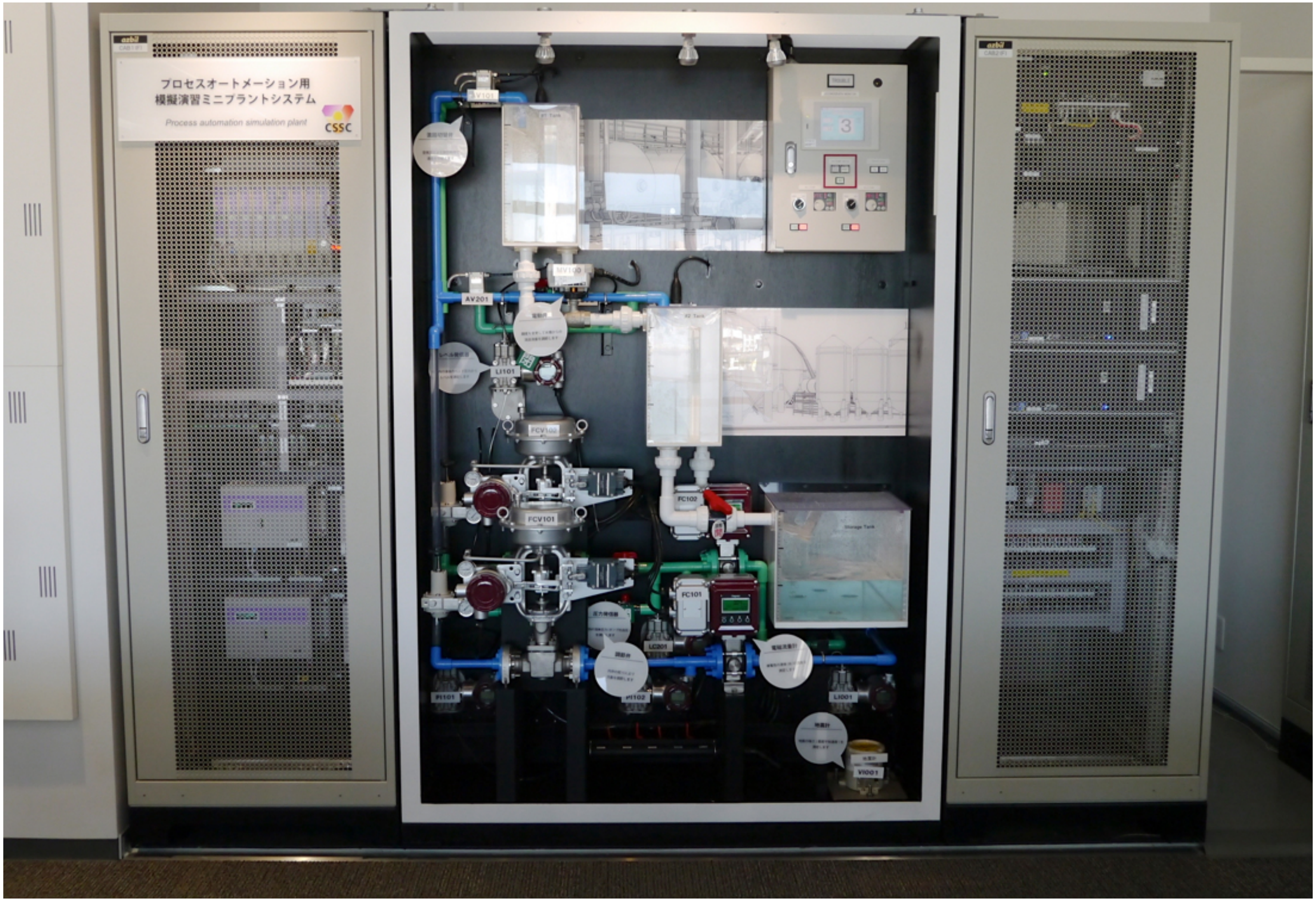
Plant simulation：（５） Gas plant



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



Plant simulation： （7）Chemical process automation system

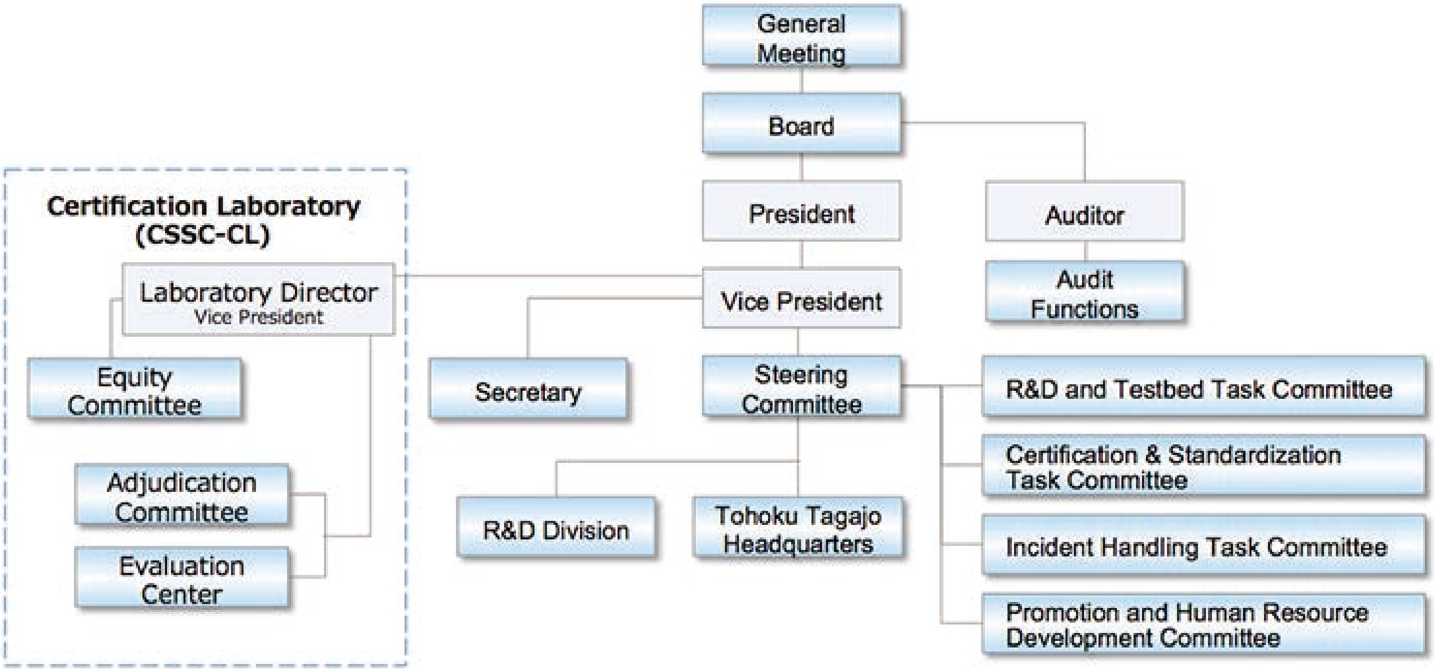

azbil
プロセスオートメーション用
模擬演習ミニプラントシステム
Process automation simulation plant
CSSC
AV201
LI101
FCV102
FCV101
FC102
FC101
LC201
PI101
PI102
LI001
VI001

Testbed: 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 testbed
- 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 Tagajyo Headquarters and Tokyo Research Center

Organization of CSSC

- Under the supervision of the Steering Committee, 4 task committees were established.
- Certification Laboratory (CSSC-CL) has also launched since 01/08/2013.


General Meeting
Board
Auditor
Audit Functions
President
Vice President
Secretary
Steering Committee
R&D Division
Tohoku Tagajo Headquarters
R&D and Testbed Task Committee
Certification & Standardization Task Committee
Incident Handling Task Committee
Promotion and Human Resource Development Committee
Certification Laboratory (CSSC-CL)
Laboratory Director
Vice President
Equity Committee
Adjudication Committee
Evaluation Center

Organization of CSSC (Cont’d)

Task Committee	Activities
R&D and Testbed Task Committee	It sets the direction of R&D regarding control system security as well as the construction of testbeds and promotes R&D and leverages the testbeds.
Certification and Standardization Task Committee	It examines evaluation certification regarding control system security and strategies and policies of standardization. It leverages the testbeds for evaluation certification and standardization.
Incident Handling Task Committee	It prepares for security incidents in control systems and examines the directions of technical development needed for incident handling including the countermeasures of security incidents.
Promotion and Human Resource Development Task Committee	It sets the direction of awareness and human resource development for control system security as a technical research association. It enhances situational awareness and promotes human resource development, making the use of the testbeds.

CL	Activities
CSSC-CL	It promotes International standard compliance certification. Especially it conducts evaluation/certification of ICS and “Communication Robustness Test” defined in EDSA.

Activities of CSSC

1. Testing & Certification
2. Training
3. Cyber-security Exercises
4. Research & Development
5. Information & Knowledge Sharing

1.Testing & Certification

- CSSC’s activities are listed below. Currently, CSSC examines IEC 62443 series.

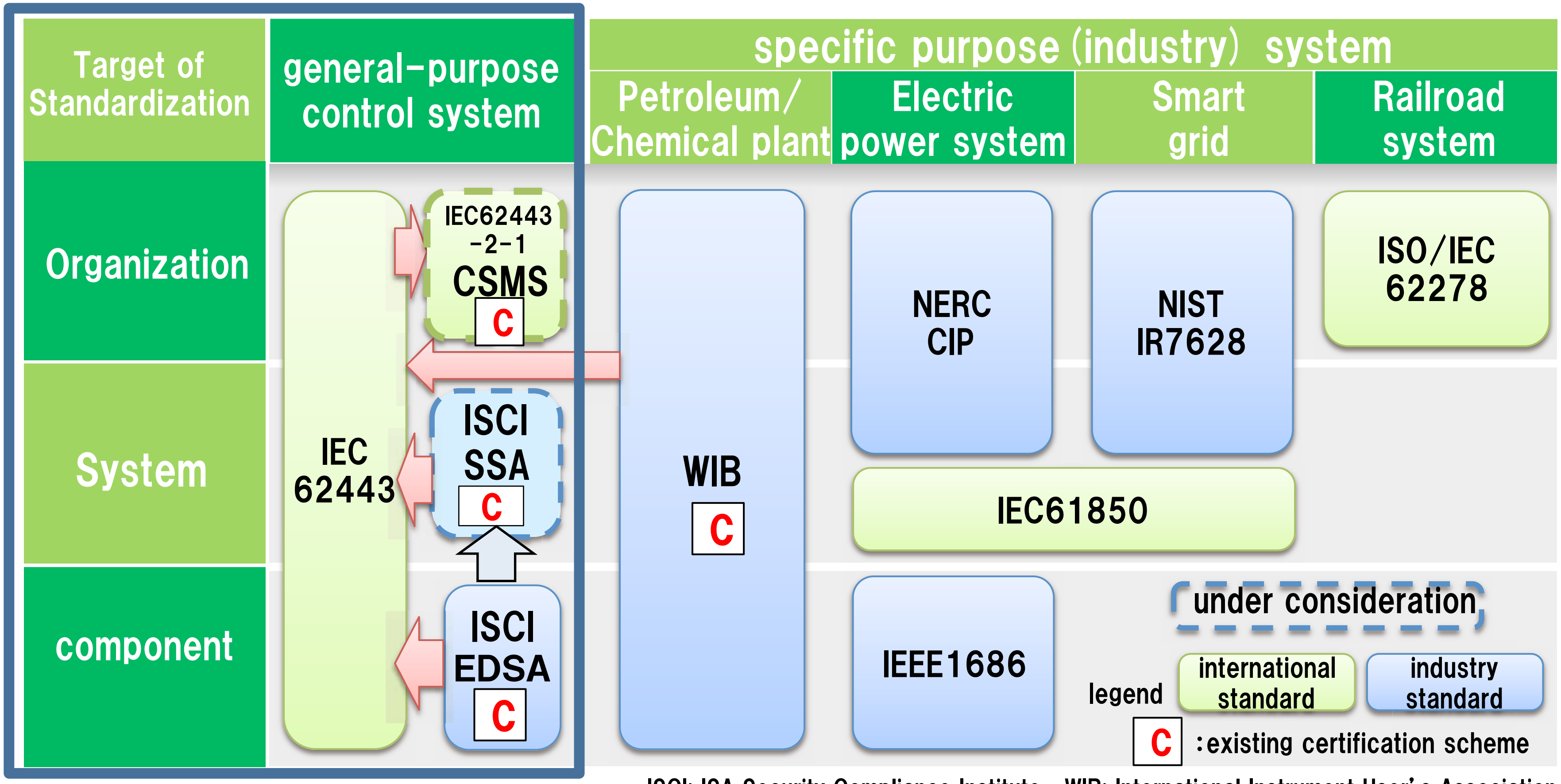
- FY2012
  - Tools CSSC purchased:
    - ◆Achilles Testing platform, BreakingPoint, IxNetwork, Codenomicon Defensics, Nessus ProfessionalFeed and Raven for ICS
  - Commissioned R&D:
    - ◆Verifying (protocol fuzzing) several PLCs and DCSs. (by two universities)
      - ▫Detailed methods and results are closed to the universities and the relevant product vendors.
    - ◆Developing a fuzzing tool prototype (CSSC original tool)
    - ◆Developing fuzzing plugins of “Raven for ICS” (domestic tool)
      - ▫BACnet/IP, FL-net, and IEC61850 MMS/ASN.1

1.Testing & Certification(Cont’d)

- FY2013 --
  - Using BreakingPoint to partially automate testing and cyber exercise
  - Continuously developing the CSSC original tool
    - ◆We’re focusing on CRT conformance in this FY.
  - Contributing to ISA99 etc.
    - ◆such as SSA and SDLA
    - ◆CSSC will be “Associate Member” of ISCI by Oct. 2013

1.Testing & Certification(Cont’d)

ISA/IEC62443 and ISA/ISCI ISASecure



Target of Standardization

general-purpose control system

specific purpose (industry) system

Petroleum/ Chemical plant

Electric power system

Smart grid

Railroad system

Organization

System

component

IEC 62443

IEC62443 -2-1 CSMS C

ISCI SSA C

ISCI EDSA C

WIB C

NERC CIP

NIST IR7628

ISO/IEC 62278

IEC61850

IEEE1686

under consideration

legend

international standard

industry standard

C :existing certification scheme

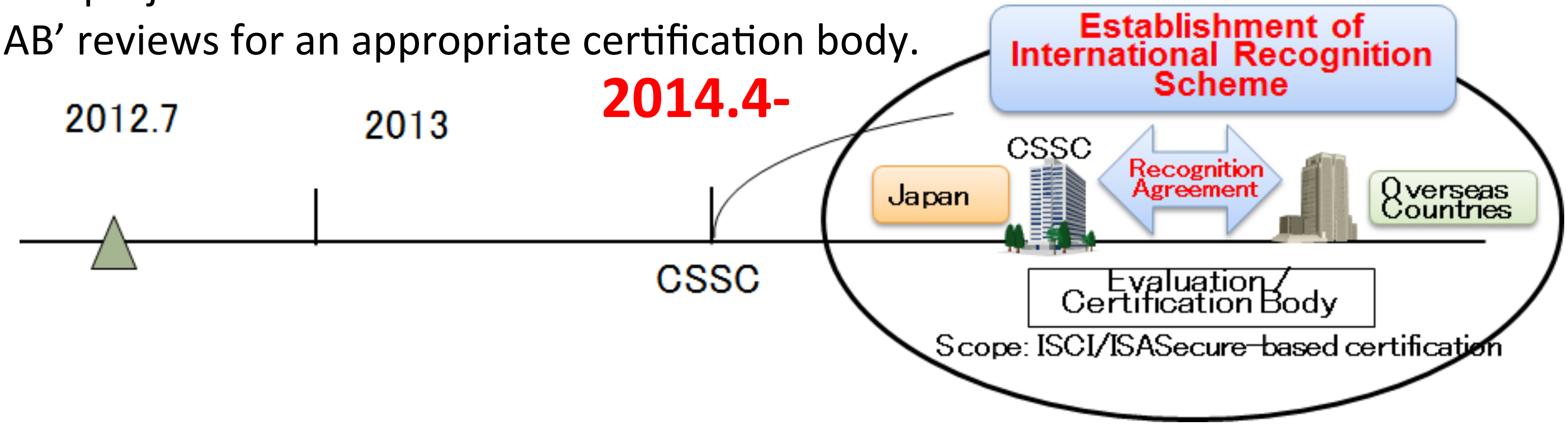
ISCI: ISA Security Compliance Institute WIB: International Instrument User’s Association

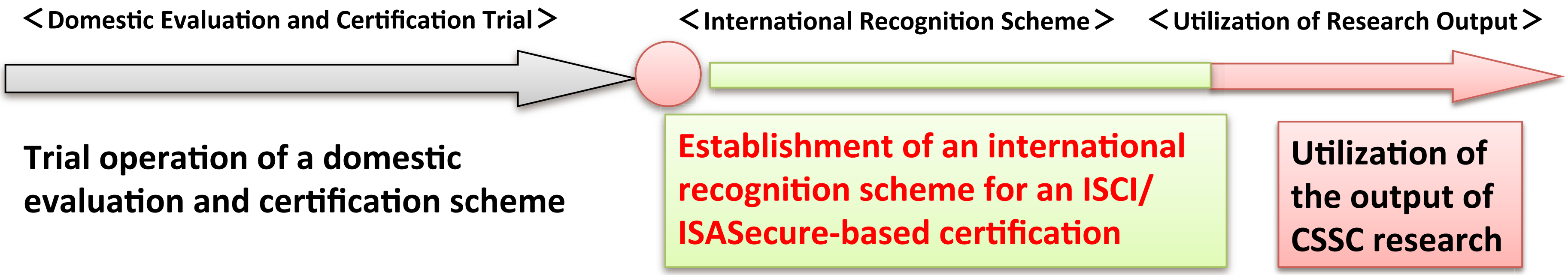
1.Testing & Certification(Cont’d)

Certification Services

Start of applying ISCI certification

-CSSC established Chartered Laboratory last August
-Apply to Japan Accreditation Board (JAB)
-ISCI associate member for ISASecure certification
-Pilot projects of EDSA certification
-JAB’ reviews for an appropriate certification body.


2012.7
2013
2014.4-
CSSC
Establishment of International Recognition Scheme
CSSC
Japan
Recognition Agreement
Overseas Countries
Evaluation/ Certification Body
Scope: ISCI/ISASecure-based certification


＜Domestic Evaluation and Certification Trial＞

＜International Recognition Scheme＞

＜Utilization of Research Output＞

Trial operation of a domestic evaluation and certification scheme

Establishment of an international recognition scheme for an ISCI/ ISASecure-based certification

Utilization of the output of CSSC research

ISCI：ISA Secure Compliance Institute

2.Training

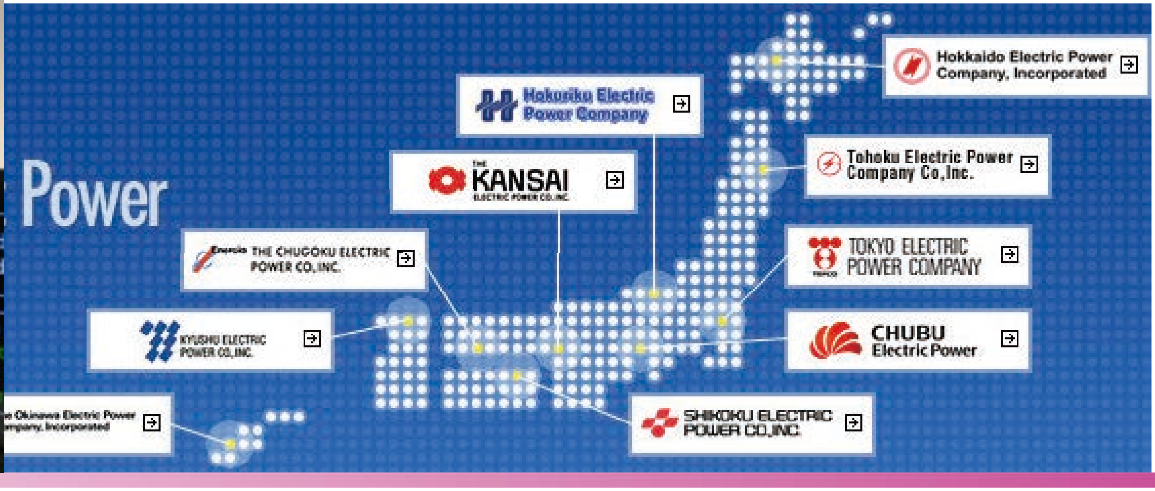
- FY2013--
  - Developing Red/Blue training materials
  - 3 days training for people interested in “functional safety” & control system security (Nov. 20-22)
    - ◆The training is funded by a government agency
    - ◆The training material is based on IEC 62443 and using CSS-Base6 to experience cyber threats and their mitigations.
    - ◆The material will be reused to promote EDSA in Japan
  - Training program on enhancing Information security for ASEAN (Jan. 20-29, 2014)
    - ◆Focusing on ISMS and ICS Security
    - ◆Managers in electric power system plans
    - ◆Heads of ASEAN Power Utilities/ Authorities (HAPUA)

3. Cyber-security Exercises

- CSSC is scheduled to host the FY2013 cyber security exercise of the government (METI)
  - Objective
    - ◆Let participants to learn how to react to incidents including cyber attacks
  - Areas
    - ◆Electricity
    - ◆Gas
    - ◆Building automation
    - ◆Chemical (From FY2013)

3.Cyber-security Exercise (1/4)

- Electricity (FY2012 -)
  - Target ICS:
    - ◆Coal-fired electricity generating plant.
  - Participants:
    - ◆Operators and engineers of the member companies of the Federation of Electric Power Companies (FEPC). Almost all the companies of


Power
Hokkaido Electric Power Company, Incorporated
Hokuriku Electric Power Company
Tohoku Electric Power Company Co,Inc.
THE KANSAI ELECTRIC POWER CO.,INC.
Energia THE CHUGOKU ELECTRIC POWER CO.,INC.
TOKYO ELECTRIC POWER COMPANY
KYUSHU ELECTRIC POWER CO.,INC.
CHUBU Electric Power
e Okinawa Electric Power mpany, Incorporated
SHIKOKU ELECTRIC POWER CO.,INC.

3.Cyber-security Exercise (2/4)

- Gas(FY2012-)
  - Target ICS:
    - ◆Gas production/supply system
  - Participants:
    - ◆Engineers of the members of the Japan Gas Association. 6 major gas companies raise their hands(2013)
  - Plants:
    - ◆Gas automation(Azbil)

3.Cyber-security Exercise (3/4)

- Building Automation(FY2012-)
  - Target ICS:
    - BA system such as light, electricity, and air conditioning management
  - Participants:
    - Instrument engineers of Mori buildings and its subcontractors.
  - Plants:
    - BA plant of MHI and Mori bldgs.
  - Red/Blue
    - Red: Experts from universities
    - Blue: Instrument engineers
    - White: N/A
  - Precondition
    - Targeted building is physically intruded by adversaries

3.Cyber-security Exercise (4/4)

- Chemical(NEW, FY2013-)
  - Target ICS:
    - ◆Chemical plant
  - Participants:
    - ◆Managers, operators and field engineers of the members of the Japan Chemical Industry Association
  - Plants:
    - ◆Process automation systems (Azbil, Yokogawa)

MITSUBISHI CHEMICAL

Mitsui Chemicals

SUMITOMO CHEMICAL

SHOWA DENKO

4. Research & Development

- Choosing theme so that the member companies (sometimes competitors) can share output.
  - Some topics require NDA with CSSC and a member company.

- Common research
  - CSSC's verification tool
    - ◆EDSA conformance
    - ◆Fuzzing functionality against frequently used protocols in domestic environment
      - ◘ (FY2012) BACnet/IP, FL-net, and EC61850 MMS/ASN.1
    - ◆Advanced penetration/fuzzing testing functionality
      - ◘ (FUTURE) Merging results of contract researches by three universities
    - ◆Vulnerability scanner using public vulnerability DB
      - ◘ (FUTURE) Using jVN

4. Research & Development (Cont’d)

- Common research (Cont’d)
  - Incident handling tools and methodologies
    - ◆Early alert system for ICS
      - ▫Reasoning the status of a plant
    - ◆Log management/mining for ICS
      - ▫ Mining and visualize logs with conforming to the standards
    - ◆Evaluating products such as McAfee SIEM, IDS, and Whitelist with the plants in CSS-Base6
  - Cyber range for both training and exercise
    - ◆Using the plants and BreakingPoint to partially automate training and exercise

4. Research & Development (Cont’d)

- Application level research
  - Threat and risk analysis for ICS
    - ◆Define virtual and typical models of PA, FA, and Smart community and analyze them
  - “Secure System Construction Guide for ICS”
    - ◆Publish guide for ICS system integrators
  - ICS modeling
    - ◆Define how to describe ICS so that, for example, IDS can be easily deployed

4. Research & Development (Cont’d)

- Innovative research
  - Conducted by AIST, The National Institute of Advanced Industrial Science and Technology (aist.go.jp)
    - ◆Around 10 researchers are listed as cooperation member
  - Hypervisor, White list, Security barrier device, Human Factor, etc.

5. Information & Knowledge Sharing

- CSSC's activities as for this topic are listed below:

- C-Level contents
  - Contents for each plant in CSS-Base6 are created/ updated in this FY
  - Contents will be arranged for each industry such as electricity, gas, etc.

- "Supporting Member": A new member category.
  - Augmented numbers of SMEs want to be involved with CSSC.
  - Member-only contents will be provided with CSSC's portal. Examples are:
    - ◆Results of activities
    - ◆CIP News (by courtesy of IPA.go.jp)
    - ◆Vulnerability. Info (by courtesy of IPA.go.jp)

5. Information & Knowledge Sharing (Cont’d)

- Identifying potential guests for CSS-Base6 (as a part of PPP)
  - A CSSC member company received another budget to develop a plan for CSSC’s “Promotion and HRD Task Committee”.
  - METI and CSSC plan to promote ICS security in global scale
- Accepting lots of guests since the opening (May 2013) to today (Approx. 6 months)
  - Guests: 612 people (Except for opening ceremony which approx. 150 people came)
  - 97 organizations including 19 from oversea

We focus on awareness raising, training and seminars this year so that more people can recognize CSSC and use our testbed facility.