Asia Pacific ICS Security Summit 2013

The State of Control System Security in Japan

NRI SecureTechnologies, Ltd.

Technical Consulting Services Department

Diasuke　Noguchi

My Profile

DAISUKE NOGUCHI

NRI SecureTechnologies, Ltd. (NRIST)
Technical Consulting Services Department

●Security Consultant(Control System)

● Penetration Tester

■**Customers**：

- ➢Critical infrastructure(Oil, Gas, Electronic)
- ➢Manufacturing
- ➢Government
- ➢IT

etc.

Company Information

NRI SecureTechnologies, Ltd.

- **Founded：August 1, 2000**

- **Office**
  - ➢Headquarters：Tokyo, Japan
  - ➢North America Branch：2102 Business Center Drive, Suite 130 Irvine, CA 92612 Number of Employees (as of April 1, 2013)：250

- **Certificate Holders (as of March 31, 2013)**
  - ➢CISA(Information System Auditor) : 55
  - ➢CISM(Information Security Manager) : 33
  - ➢CISSP(Certified Information Systems Security Professionals)：31
  - ➢GIAC(Global Information Assurance Certification)：96 in total

- **The others :**
  - ➢**NRIST is the SANS Partner in Japan**
  - ➢NRIST has NCSIRT(CSIRT) and NRIST is **the member of FIRST**
  - ➢NRIST is certified as **PCI DSS ASV and QSA.**

Agenda

壱 ***The State of Control System Security in Japan***

弐 ***Control System Security Center (CSSC)***

参 ***Wrap-Up***

Agenda

壱 ***The State of Control System Security in Japan***

弐 ***Control System Security Center (CSSC)***

参 ***Wrap-Up***

Objectives

- In this session, I would like to share…
  - The State of Control System Security in Japan, based on our report **“Organizations Information Security Status Investigation 2013”**

Organizations Information Security Status Investigation 2013

企業における
情報セキュリティ実態調査 2013
Information Security - Report 2013
NRI SecureTechnologies

Research Overview

Date : 2013 August –October

Method : Questionnaire

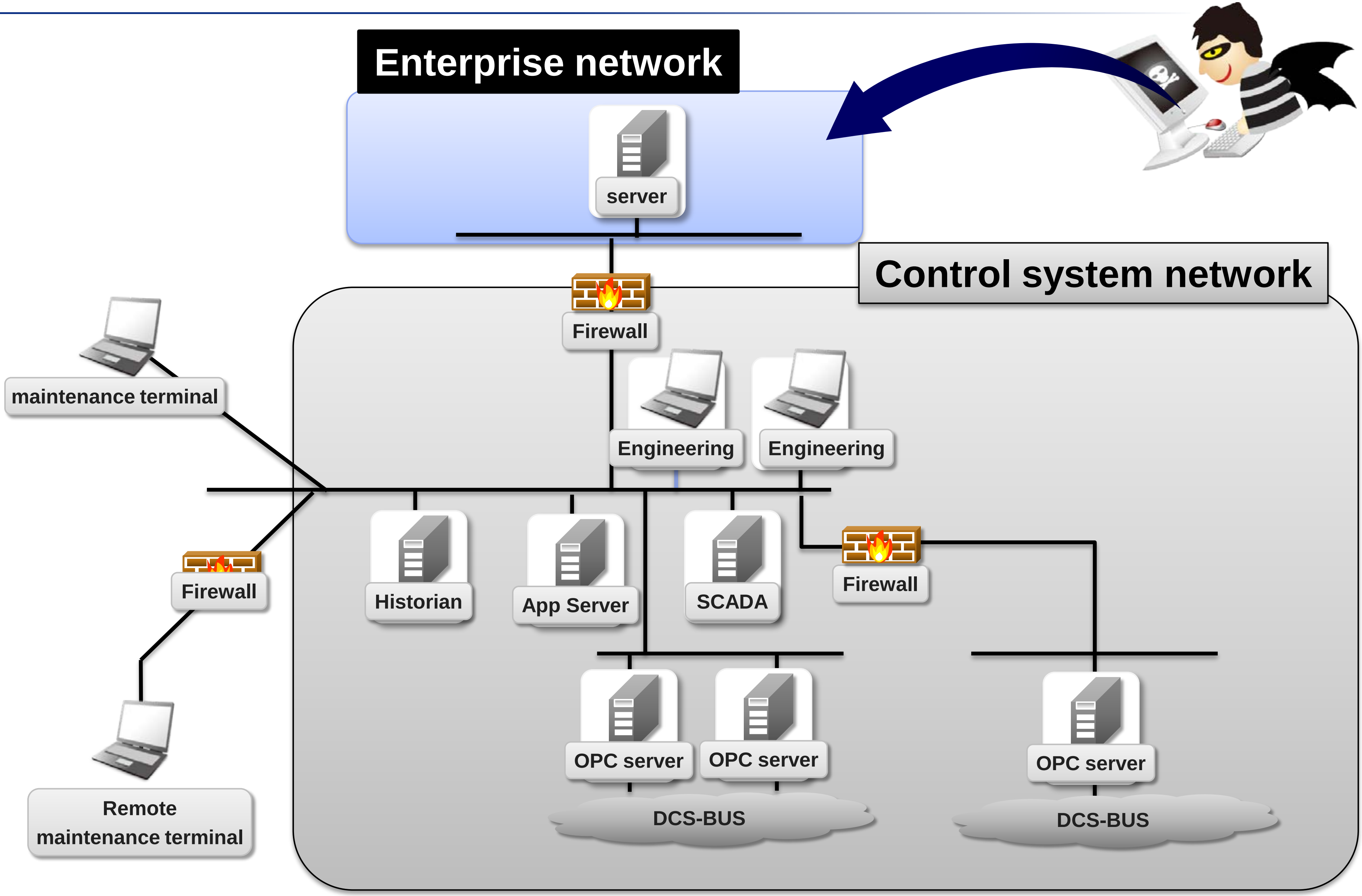
Target :

3000 companies (especially listed company of 1st & 2nd section of TSE, and of OSE)

Valid Response :685

Control system User Response:161

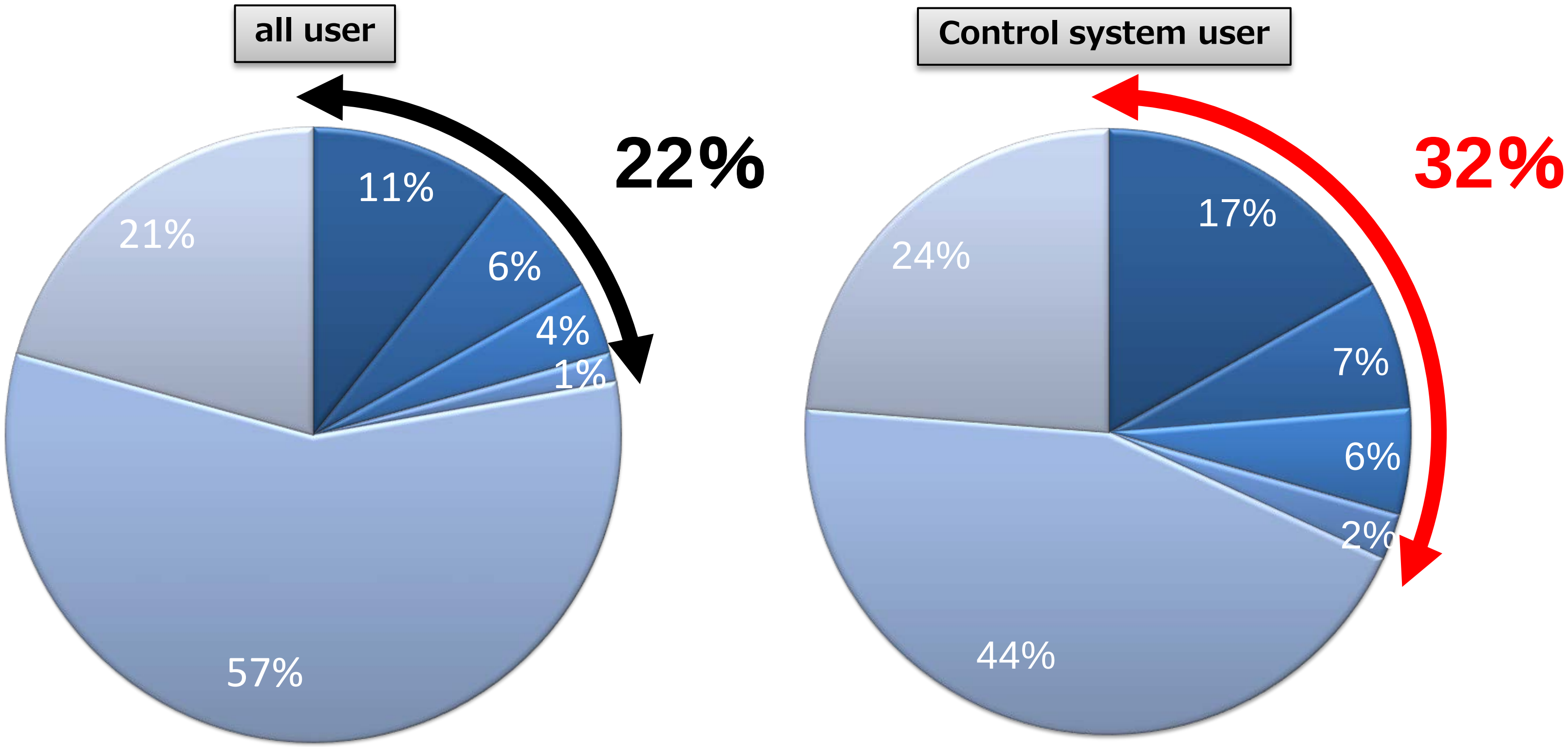
Attack to Enterprise network



Attack to Enterprise network

Q. What kind of attack have you ever had?

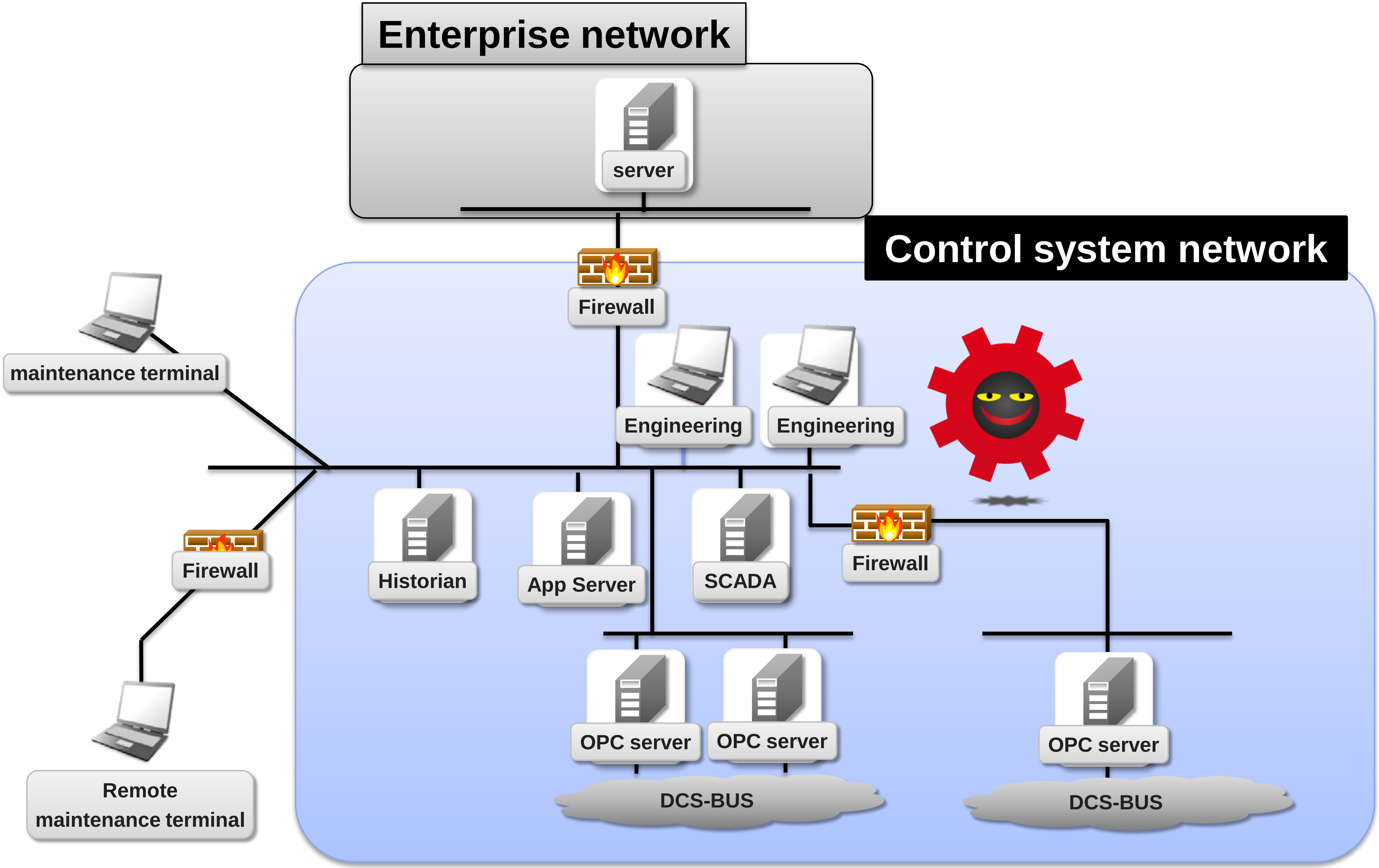
■ Targeted E-mail Attack
■ Persisted attack to published server
■ Attack both of the above
■ Other attacks (other than the above)
■ Never been attacked so far
■ No grasp


all user

Control system user

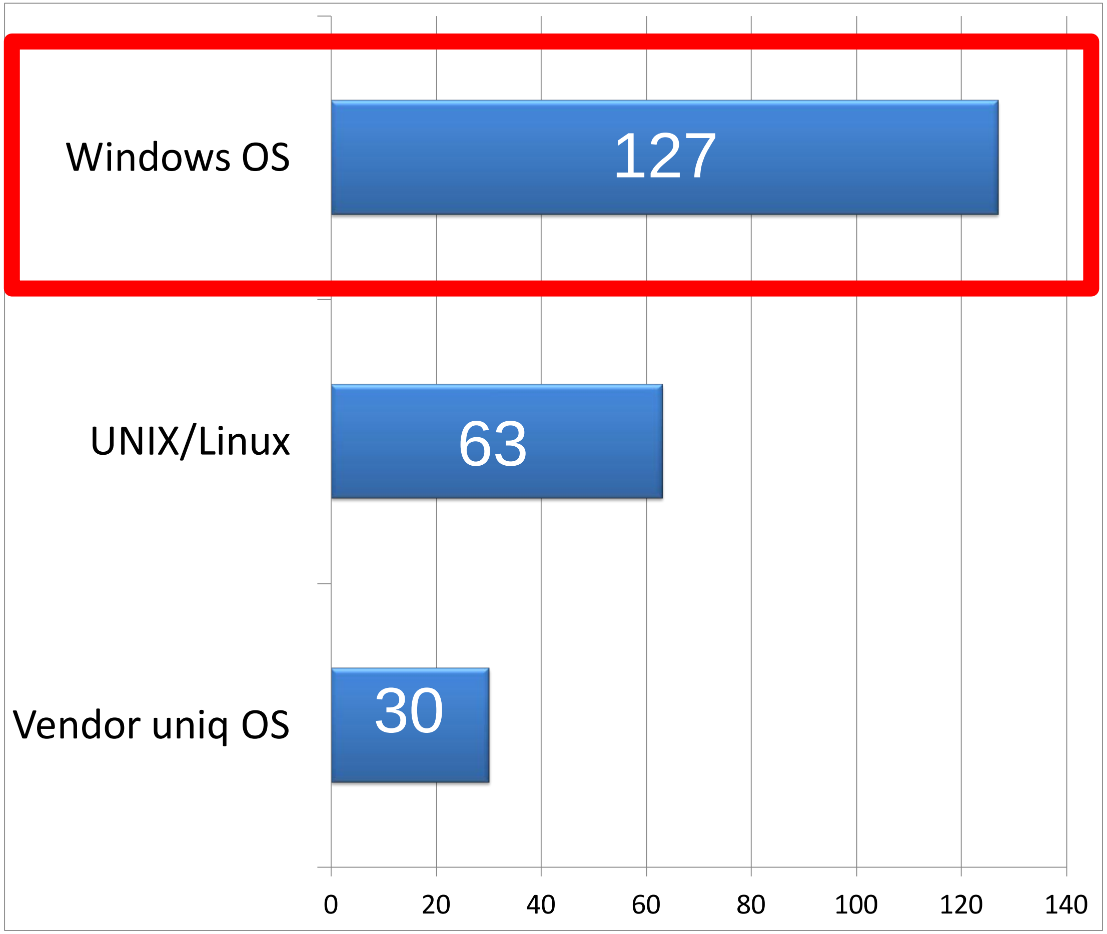
Control system users have had more attacks than non-control system users.

Abstract architecture of Control System



Operating System in Control System

Q. What kind of operating system do you use in your control system? (Select all that apply)

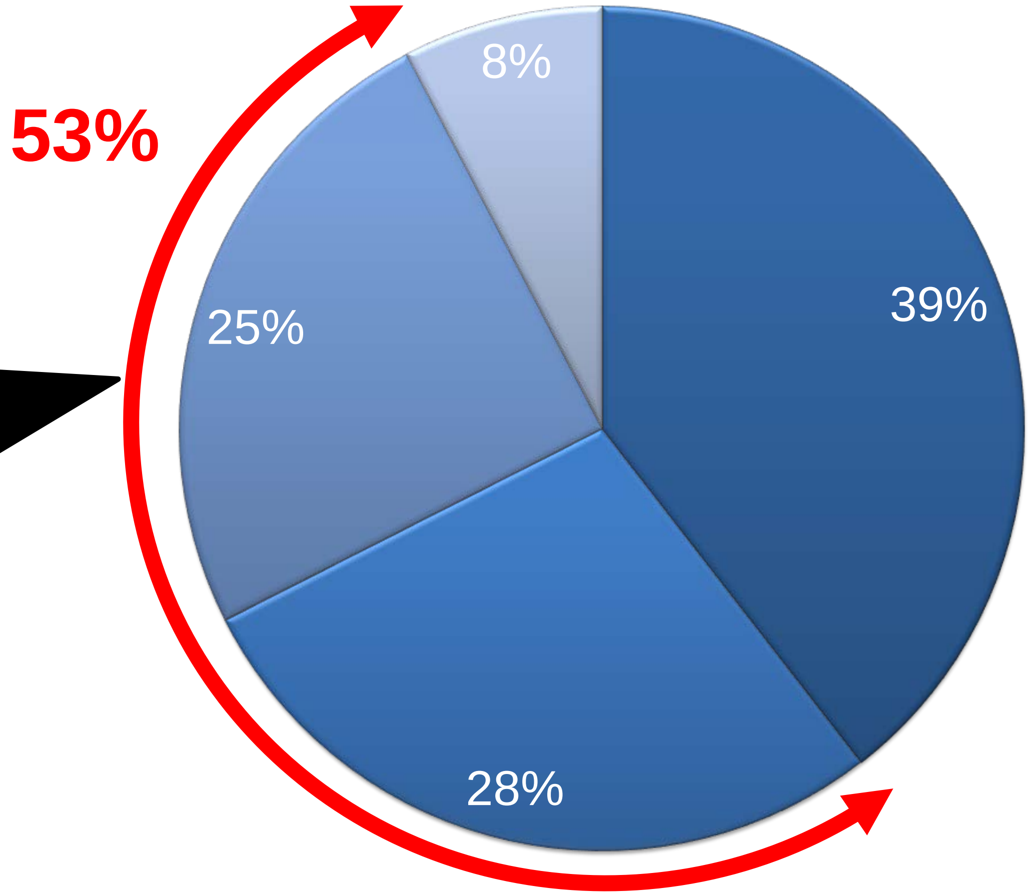


127 companies（about 79% of the control system users）are using Windows OS in their Control system.

Segmentation between Enterprise and SCADA

Q. What kind of architecture do you take for dividing between Enterprise network and SCADA network?

■ Physical segmentation ■ Logical segmentation by firewall ■ Without segmentation ■ No grasp



The SCADA network of 53% control system companies is connecting to corporate network.

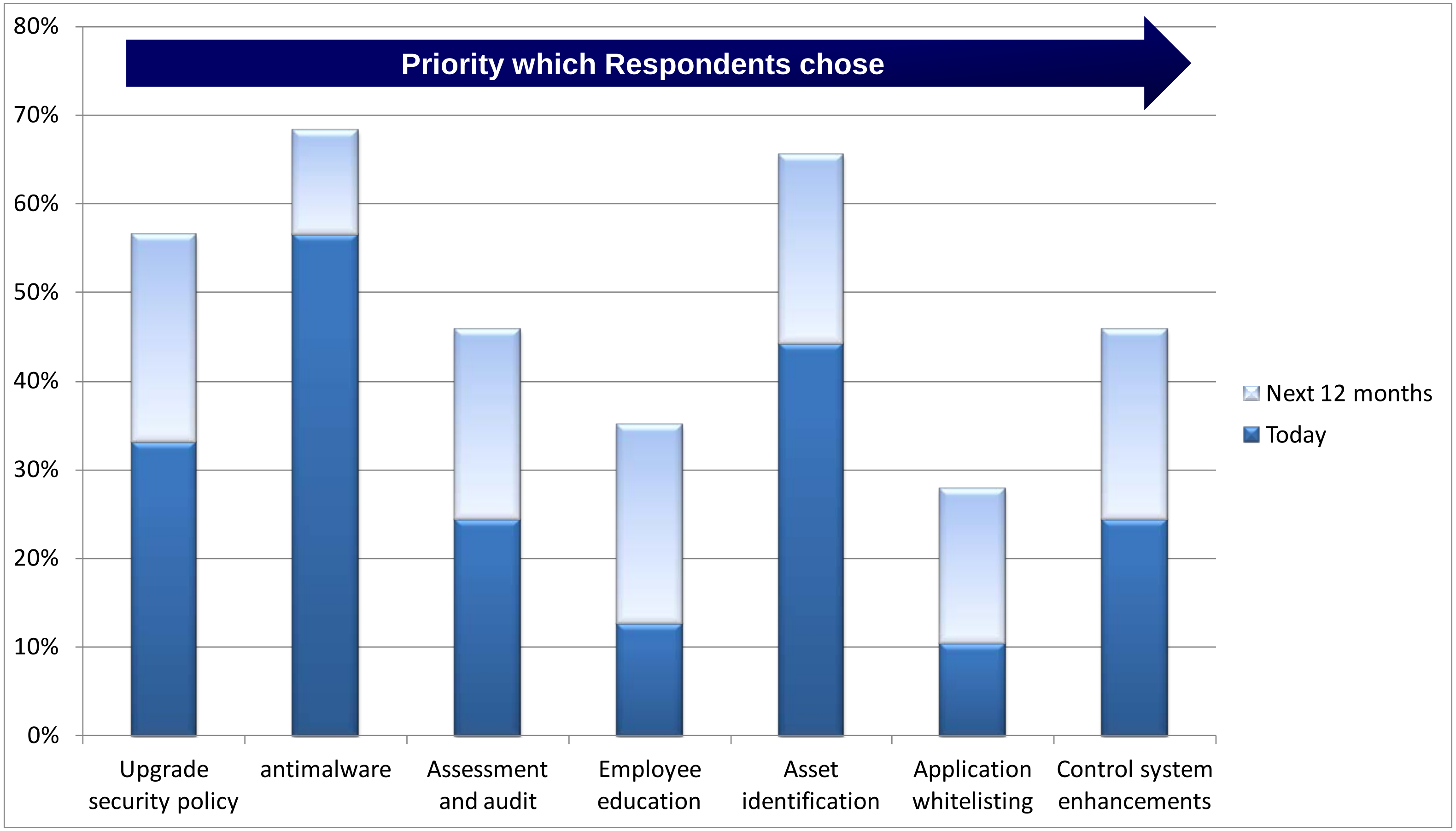
According to other research, they use TCP/IP network in their control system.

According to previous described, Control systems are opening multiple connections to external networks, using Windows OS and TCP/IP, that are similar to Information system.

That is thought to be similar to other countries.

Security Control(Tools and Processes)

Q. What do you use for control system security today? What do you plan to implement in the next 12 months? (Select all that apply.)



Our services

We have services described below. In addition to the services below, we will provide customized services according to customer request.

Assessment

- Device
- Web Application
- Platform
- Database
- Smartphone application
- Source code audit

etc.

Consulting

- IEC62443 Consulting
- Customized Guideline
- Operation audit
- Action plan
- Support for self-assessment
- Monthly Report

etc.

Review

- Application Design Review
- Architecture Review
- FW Policy Inspection

etc.

Forensic

- log investigation
- Hard drive salvage
- Malware analysis

etc.

Guideline

- Web application Security
- Operating System Security
- Database Security
- Smartphone Application Security

etc.

Incident Response

- Incident Response Support
- Annual contract
- IR for Information leakage
- IR for Malware Infection

etc.

Agenda

- 壱 ***The State of Control System Security in Japan***
- 弐 ***Control System Security Center (CSSC)***
- 参 ***Wrap-Up***

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:

- to ensure ICS security
- Response to Targeted Attack
- Education of information security workforce

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

Control System Security Task Force (METI)

2011/10 <Overview> 2012/4

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

Control System Security Center (CSSC)

Objectives

- ■Promote developing security verification facilities (testbeds) and launching evaluation & verification organizations
- ■Enforce the security of critical infrastructures, plants and factories
- ■Strengthen exports of infrastructure systems

From METI presentation

Control System Security Center (CSSC)

Name	**Control System Security Center** (CSSC) ※A corporation authorized by the Minister of Economics, Trade and Industry
Established	March 6, 2012 (The registration date)

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

azbil

FUJITSU

Fuji Electric

HITACHI Inspire the Next

IPA

McAfee An Intel Company

MITSUBISHI ELECTRIC Changes for the Better

MITSUBISHI HEAVY INDUSTRIES, LTD. Our Technologies, Your Tomorrow

M O R I

MITSUBISHI RESEARCH INSTITUTE, INC.

NEC

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

Control System Security Center (CSSC)

7 simulated plants

①Process automation systems (Azbil)

②Process automation systems(Yokogawa)

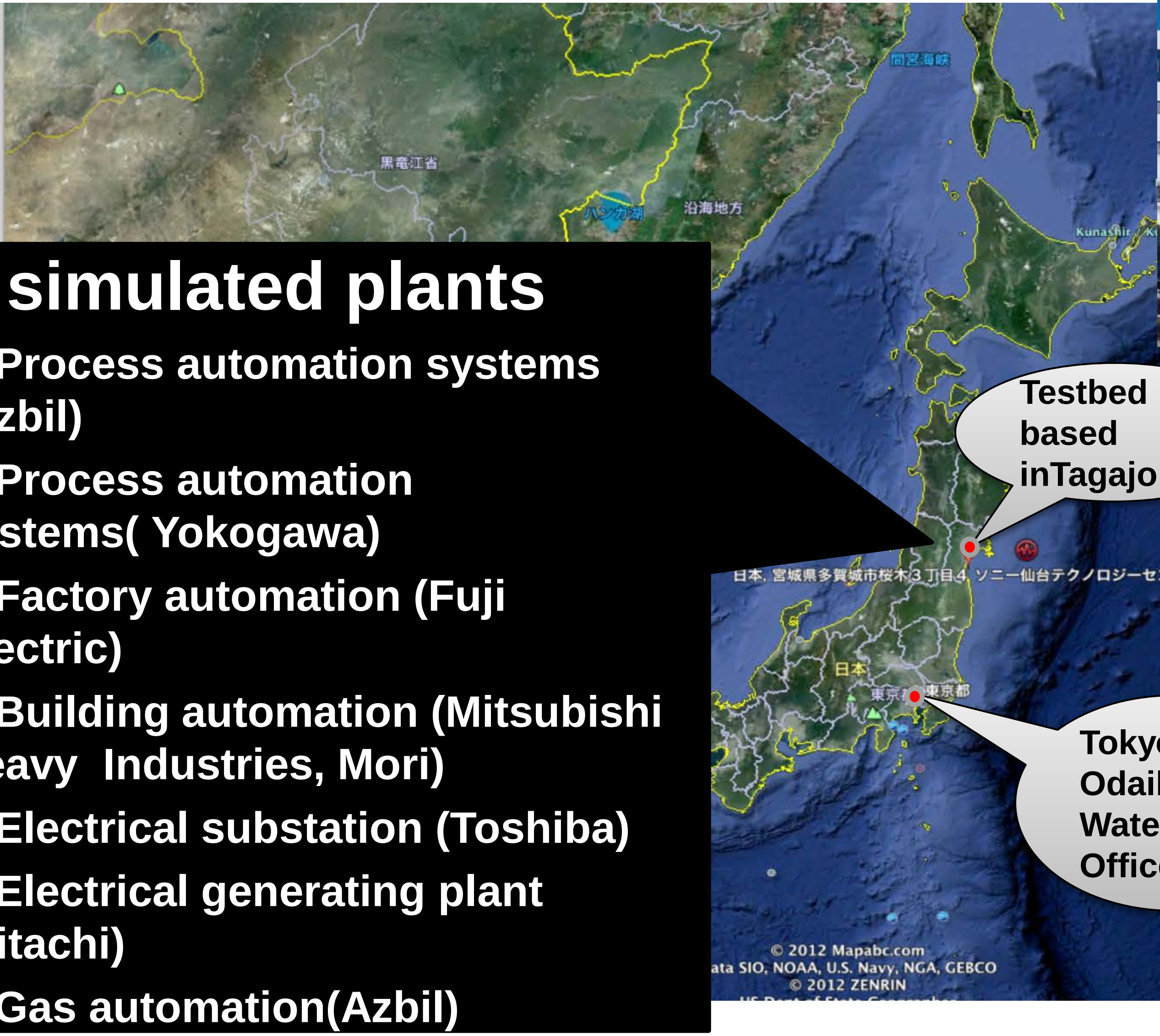
③Factory automation (Fuji Electric)

④Building automation (Mitsubishi Heavy Industries, Mori)

⑤Electrical substation (Toshiba)

⑥Electrical generating plant (Hitachi)

⑦Gas automation(Azbil)

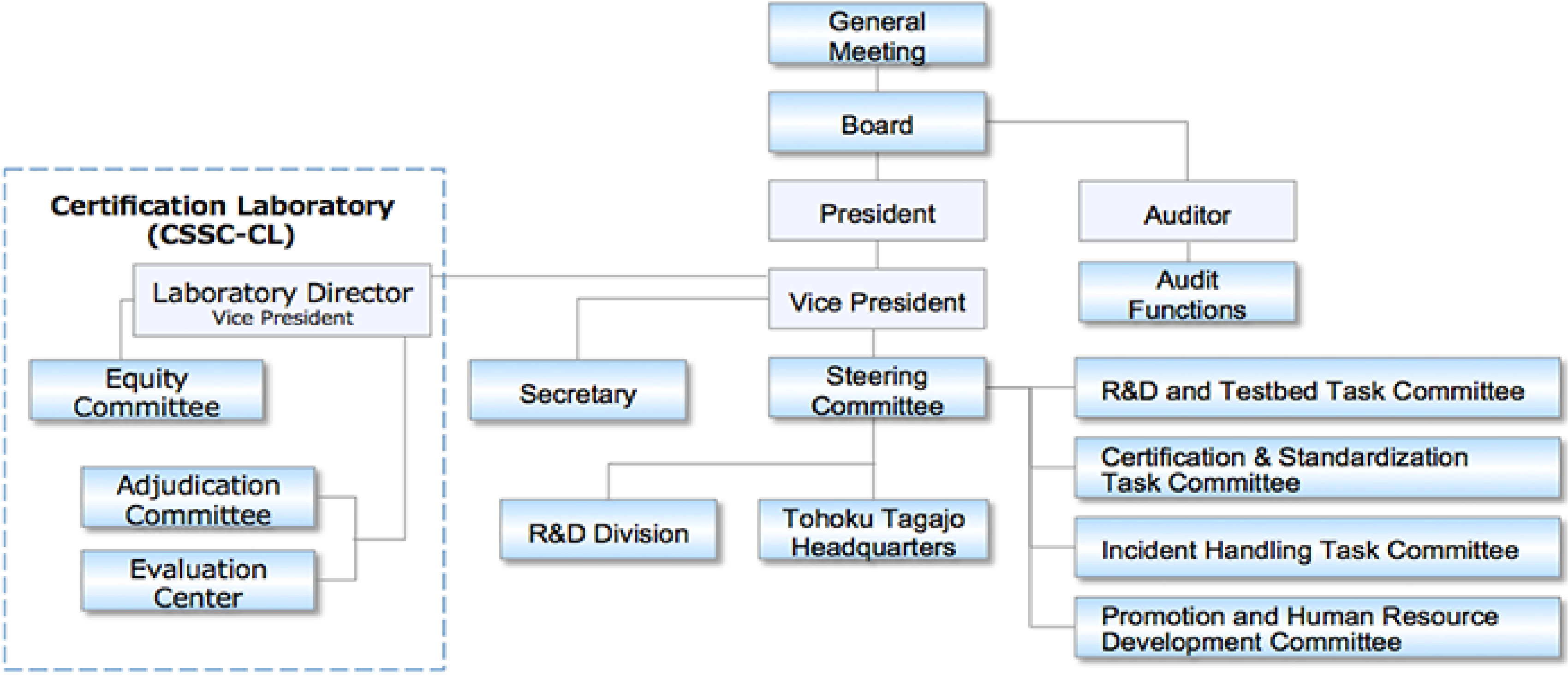

間宮海峡
黒竜江省
ハンカ湖
沿海地方
Kunashir
日本, 宮城県多賀城市桜木3丁目4, ソニー仙台テクノロジーセンター
日本
東京都
© 2012 Mapabc.com
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2012 ZENRIN

Testbed based inTagajo

Tokyo Odaiba Waterfront Office

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
President
Auditor
Audit Functions
Vice President
Certification Laboratory (CSSC-CL)
Laboratory Director
Vice President
Equity Committee
Adjudication Committee
Evaluation Center
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

4 task committees

Task Committee	Activities
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.
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.
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.
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.

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

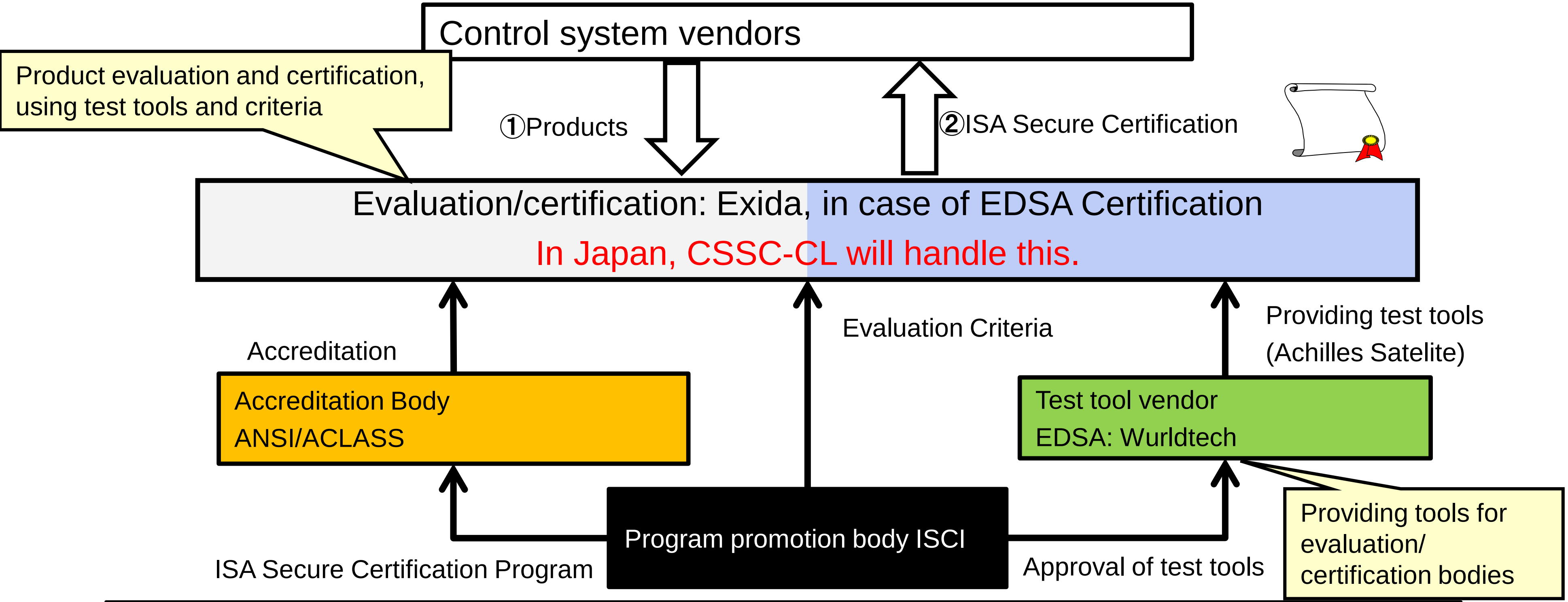
Certification and Standardization Task Committee

- **Objectives**
  - **Develop strategies and policies for CSSC such as certification with existing international standard and standardizing related to control system security**
  - **Shorten the time to acquire international certificates based on the evaluation criteria by third parties**
  - **Establish an international recognition scheme for ICS security evaluation and certification, promoting standardization, and contributing to the enhancement of ICS security at the global level**

- **Topics**
  - **Direction for certification and standardization as CSSC**
  - **Effective use of test bed for certification and standardization.**
  - **Issues for certification and standardization in control system security**

CSSC-CL: Certification Activities

Focus on Participating in EDSA/SSA Scheme



Control system vendors

Product evaluation and certification, using test tools and criteria

①Products

②ISA Secure Certification

Evaluation/certification: Exida, in case of EDSA Certification

In Japan, CSSC-CL will handle this.

Accreditation

Evaluation Criteria

Providing test tools (Achilles Satelite)

Accreditation Body
ANSI/ACLASS

Test tool vendor
EDSA: Wurldtech

Providing tools for evaluation/ certification bodies

Program promotion body ISCI

ISA Secure Certification Program

Approval of test tools

🟦Evaluation/certification body: a body who evaluates products and issue ISASecure certificates

🟧 Accreditation body: a body who examines and certifies an evaluation/certification body

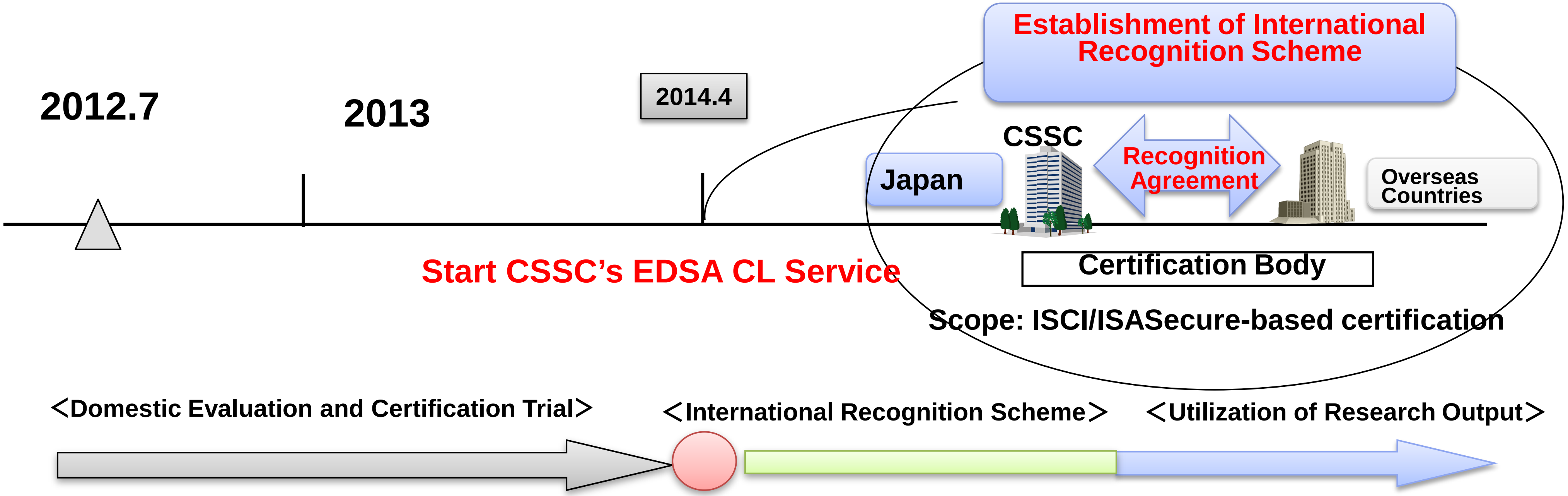
🟩Test tool vendor: a company who provides tools for evaluation/certification bodies

ANSI : American National Standards Institute）

ACLASS : ANSI-ASQ National Accreditation Board）

CSSC-CL: Certification Services

- **Timeline for Committee Activities**



Establishment of International Recognition Scheme

2012.7

2013

2014.4

CSSC

Japan

Recognition Agreement

Overseas Countries

Certification Body

Start CSSC's EDSA CL Service

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 using criteria equivalent to that used by ISCI/ISASecure certification

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

Utilization of the output of CSSC research

ISCI：ISA Secure Compliance Institute

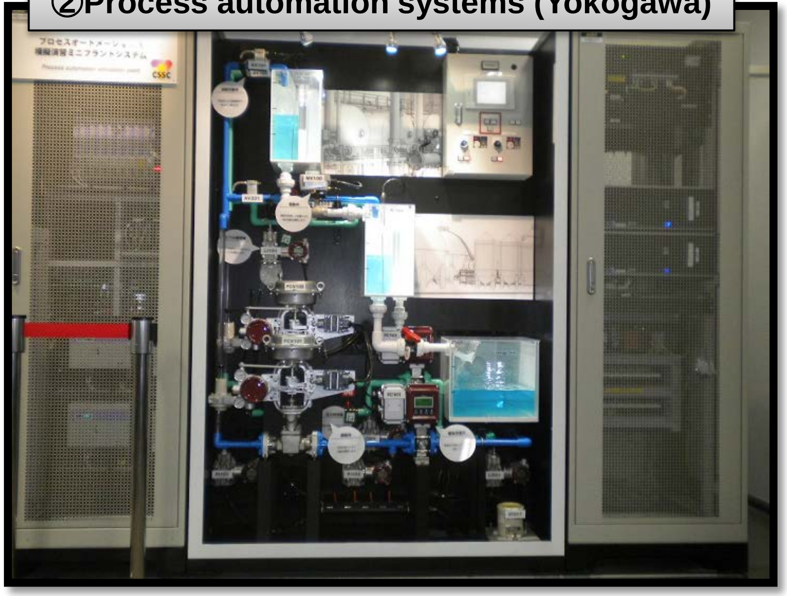
Promotion and Human Resource Development Task Committee

- Objectives
  - Promote R&D for pubic awareness and the desirable situation for HRD in CSSC.
- Topics
  - Direction for public awareness and HRD for control system security
  - Effective use of testbed for public awareness and HRD

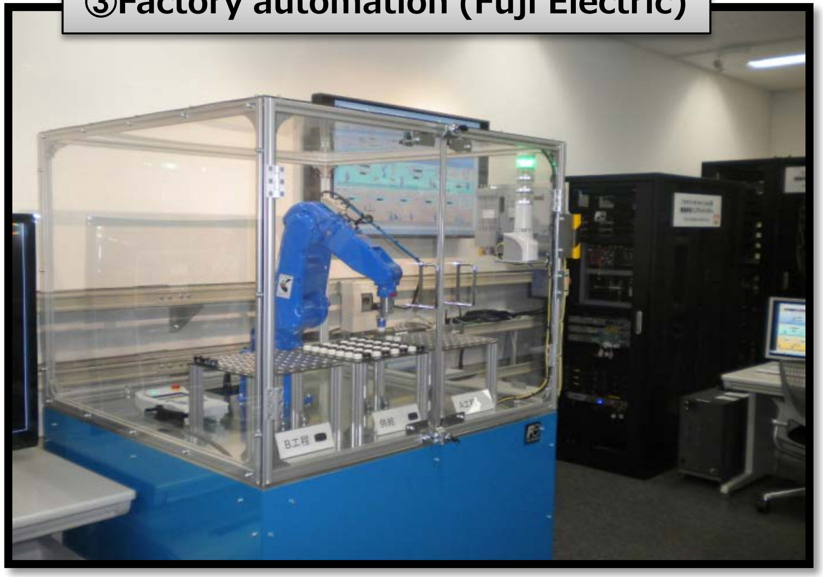
Testbed(7 simulated plants are developed)

①Process automation systems (Azbil)

②Process automation systems (Yokogawa)



③Factory automation (Fuji Electric)

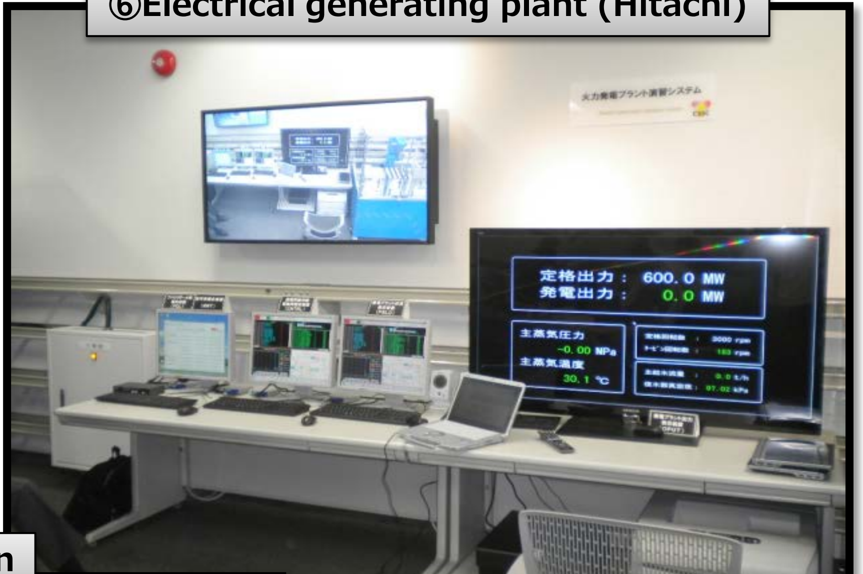


④Building automation

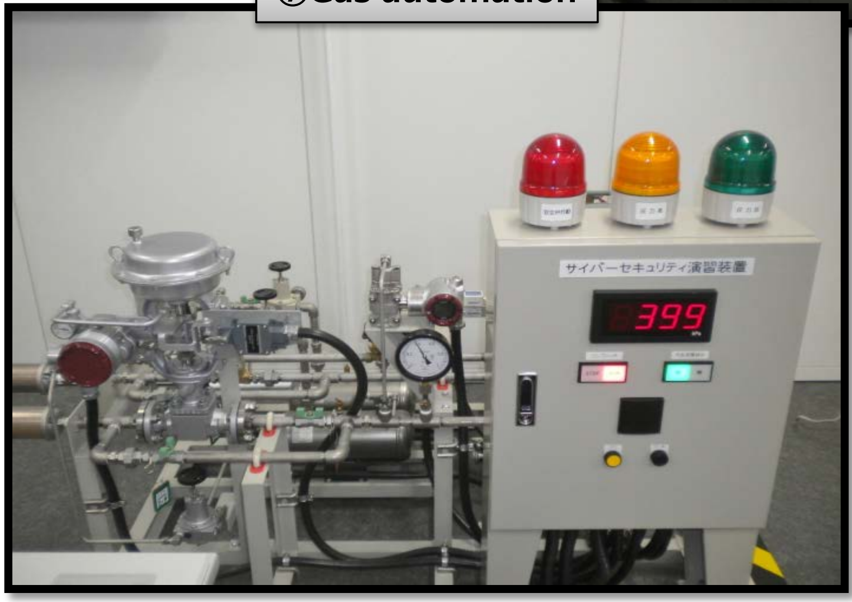
Testbed(7 simulated plants are developed)

⑤Electrical substation (Toshiba)

⑥Electrical generating plant (Hitachi)



⑦Gas automation



Simulated Plants for cyber security training

Overview

- Users will use this in order to enhance situational awareness and skill
- The system simulates a process that is actually used in real settings.
- The system consists of DCS that controls the plant.

Function/Components

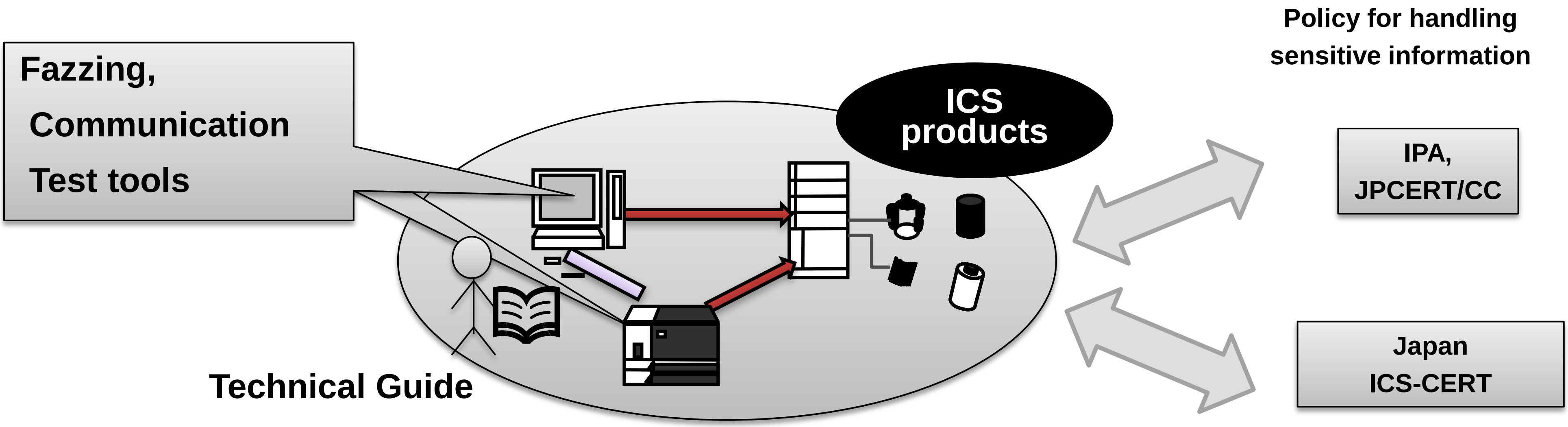
- Proven process in PA industry
- DCS that operates, monitors and controls the plant
- Safety shutdown

Security Incidents

- HMI goes out of control
- Control logic and/or parameters are over-written

Incident Handling Task Committee

- Objectives
  - Set up the guidelines to handle cyber attacks against control systems in CSSC.
- Topics
  - Policy for handling sensitive information, for example vulnerability information on evaluating equipment
  - Effective use of testbed for incident handling



R&D and Testbed Task Committee

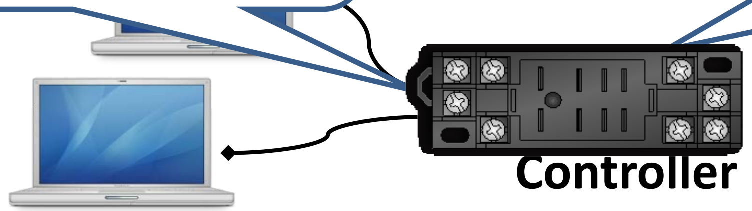
- **Objectives**
  - **Promote R&D related to control system security through discussions about how R&D and testbed should be in CSSC.**
- **Topics**
  - **Direction of R&D**
  - **Design, develop, and manage the testbed**
  - **R&D progress review**

With Highly Protected Configuration against Targeted Attack

Highly Secure Framework

· for Urgent Countermeasure

· for Fundamental Countermeasure



Agenda

壱 ***The State of Control System Security in Japan***

弐 ***Control System Security Center (CSSC)***

参 ***Wrap-Up***

Wrap-Up(Our Control)

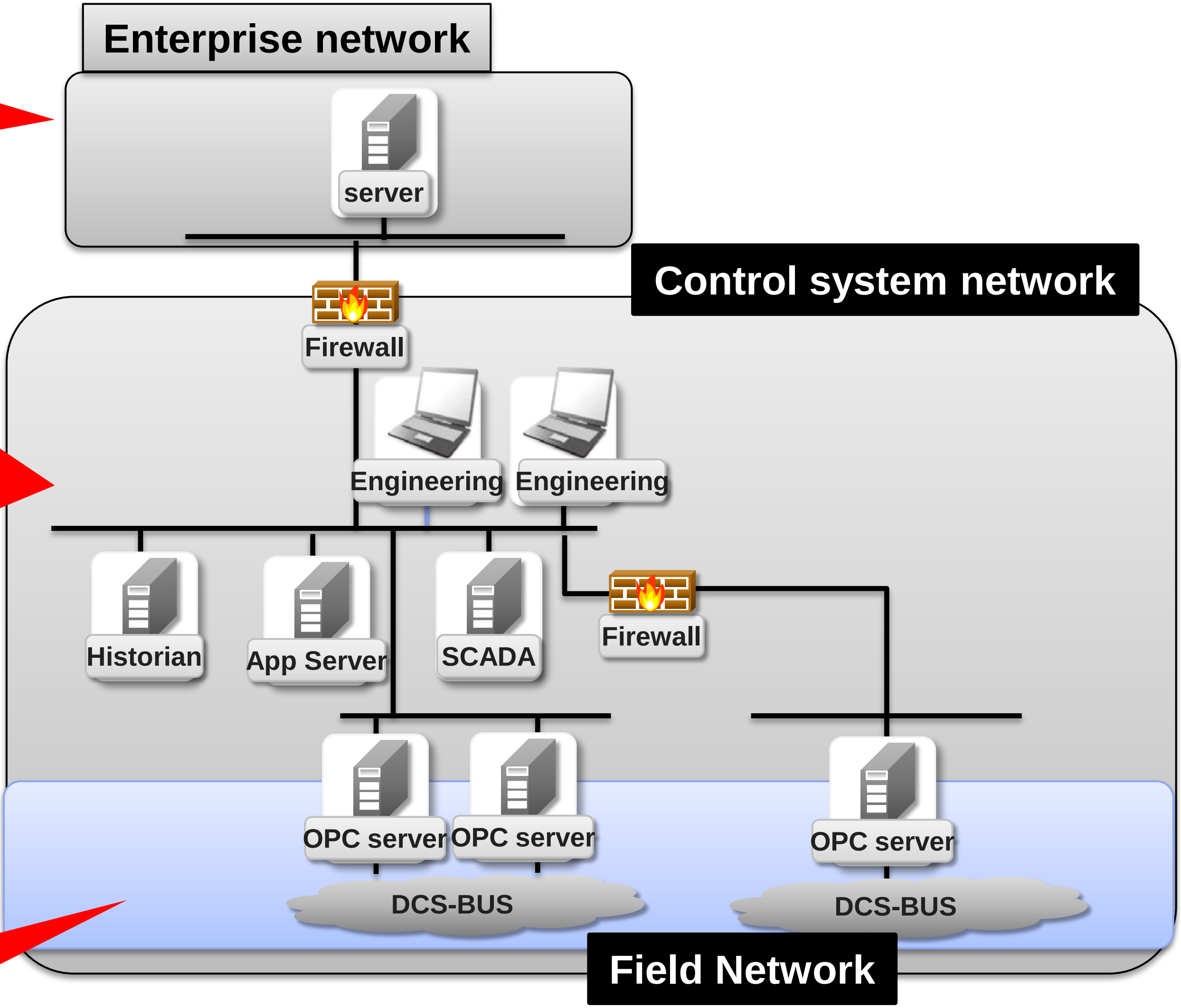
- network segmentation
- remote access control

with IT security control

- Testbed
- Cyber security training
- Assessment&audit

with technical measures(antimalware, network monitoring, application whitelisting,etc)

Security Certification (CSSC-CL)



Questions ???

Diasuke Noguchi

Security Consultant

NRI SecureTechnologies

noguchi@nri-secure.co.jp

NRI SECURE TECHNOLOGIES

Feel Free to Contact Me

Thank you for your time & attention

NRI SecureTechnologies, Ltd.

Please contact us at

Phone : +81-3-6274-1011 (Headquarter in Japan)
E-mail : info@nri-secure.co.jp
HP   : http://www.nri-secure.co.jp/en/index.html