A global perspective on grid resilience : Japanese situation and contribution of CSSC

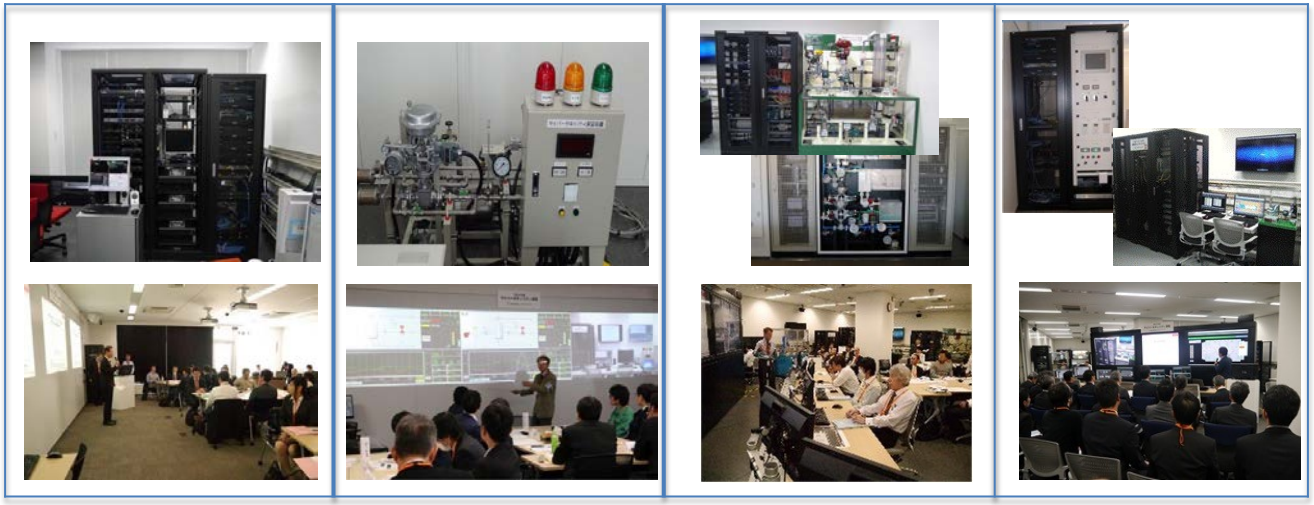
Introduction of CSSC

Makoto Takahashi, Director CSSC Japan

<Control System Security Center: CSSC>

- Research and development with highly-secure control systems
- Testing and certification of control systems, control devices, etc.
- Training human resources to disseminate and promote awareness of control system security

Electric power **Gas** **Chemicals** **Buildings**



- *Extracted characteristic functions of ICS*
- *Developed plant simulations for demonstration and cyber exercises*
- *Implemented 8 kinds of plant simulations*

Japanese situation of Grid Resilience

Makoto Takahashi, Director CSSC Japan

Ministry of Economy, Trade and Industry: METI

- Industrial Cybersecurity Society has led the discussion on cybersecurity
  - Sub-working group for Building
  - Sub-working group for Space Industry
  - **Sub-working group for Electric Power**
    - For large scale electric power company
      - Electric power control security guideline
    - For retail electricity company, resource aggregator
      - Cybersecurity countermeasure guideline for retail electricity company
- CSSC is now making contribution to supply chain risk management
  - CPIC（Cyber Product International Certification)
- Regulation
  - Based on the tech-spec for large scale power generation and transmission, two guidelines have issued
    - Electric power control security guideline
    - Smart meter security guideline
  - For small scale power generation (Solar,etc.), discussion is ongoing to introduce cybersecurity issue in the safety regulation.

Enhancing grid resilience

Makoto Takahashi, Director CSSC Japan

- Grid should be considered as “socio-technical system”, in which human make positive contribution to enhance resilience.
- The capacity to be resilient only partly depends on the technical infrastructure of an organization
- Traditional risk assessment approaches tend to break down when it is difficult to clearly identify the threats, assess vulnerabilities, and quantify consequences
- Cyber threats cannot be clearly identified and quantified through historical measures due to the **rapidly changing threat environment**.

Concept of Resilience Engineering should be adopted to enhance grid resilience.

In resilience engineering, focuses has been set on the ability to succeed under varying conditions.