2011 Japan-America
Frontiers of Engineering Symposium
June 6-8, 2011
Japan

Smart Grid Cyber Security

CRIEPI
(Central Research Institute of
Electric Power Industry)
Japan

Mai KIUCHI

Topics

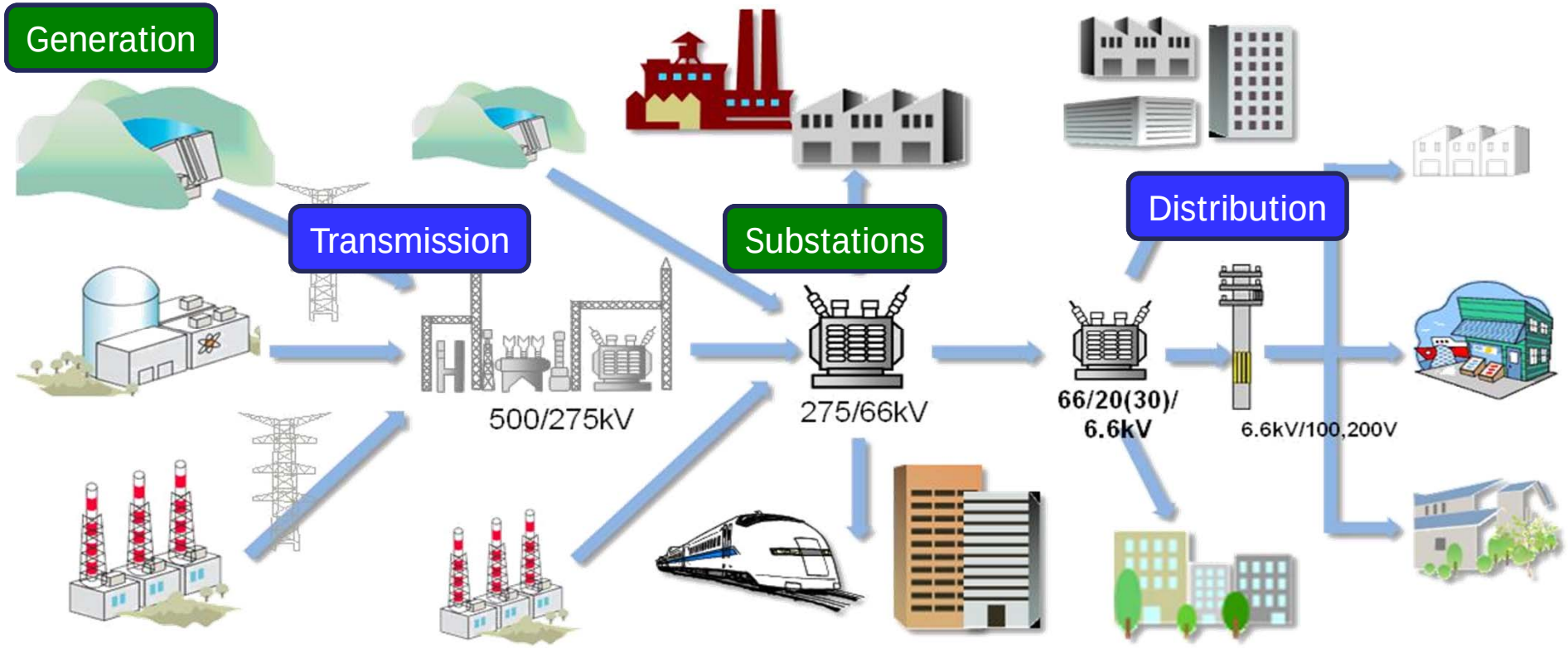
- About the smart grid
- Cyber security in the smart grid
- Problems in implementing security measures
- Security strategy and measures
- Future work

Introduction

- The Smart Grid is
  “a next-generation electrical power system that is typified by the increased use of communications and information technology in the generation, delivery and consumption of electrical energy” (IEEE)

Security Concerns

Control Systems in the (traditional) Electric Grid

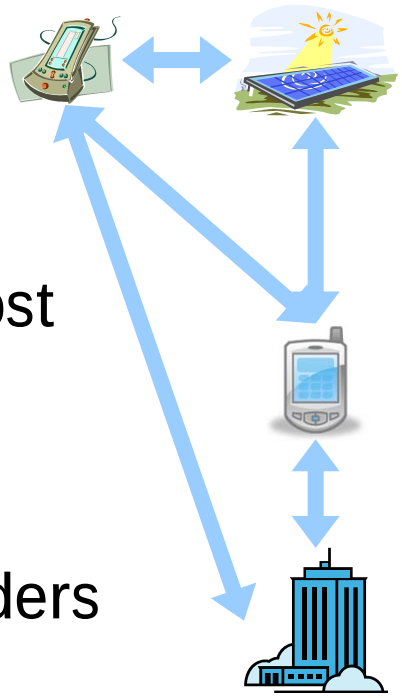


- **Control**
  - **Control generation in accordance with demand**
  - **Remote control of substations**

- **Data acquisition**
  - **Monitor grid state and equipment**

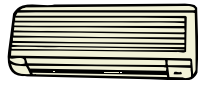
Smart Grid Characteristics

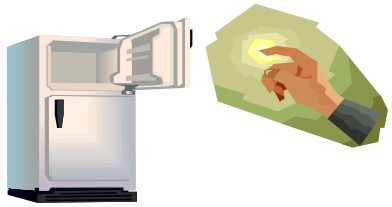
- Various devices such as smart meters and solar power will be connected
  - Communication network not closed to just the electric utility
  - Bidirectional communication between devices
- A large number of connected devices
  - Network architecture must be realized at low cost
  - General IT will be used
- Use of various services and functions
  - Connection and data sharing with service providers



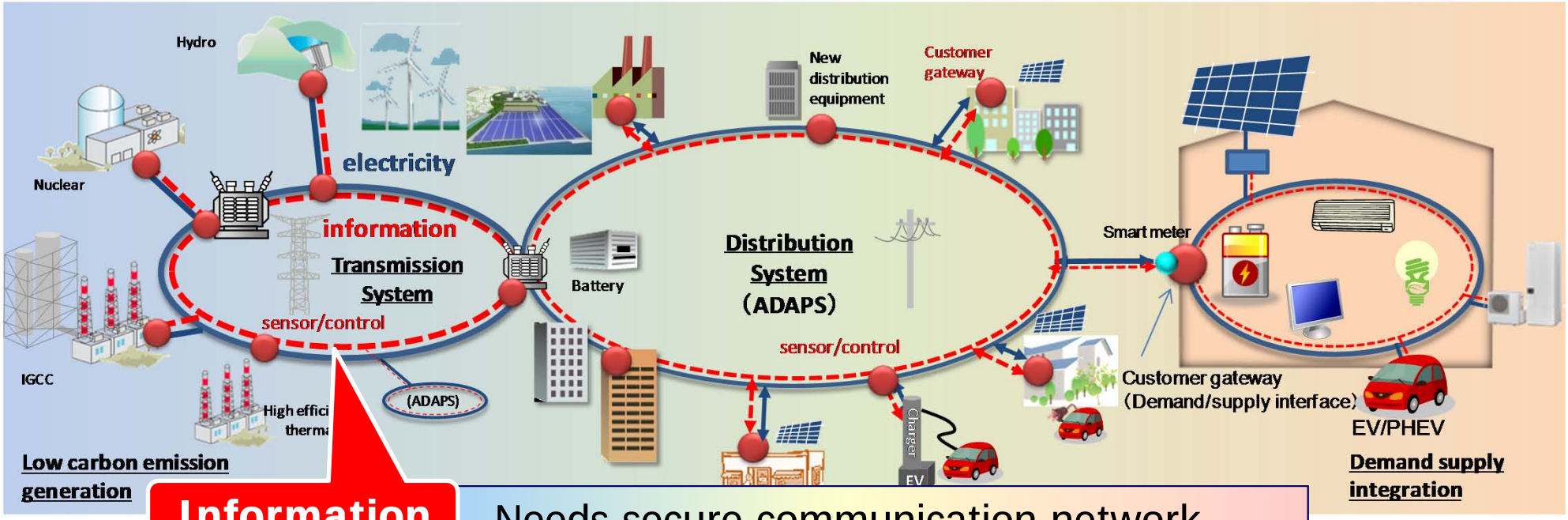
Problems concerning Cyber Security

- Physical damage may occur
  - Different from cyber attacks in the Internet
- More potential intrusion points for the attacker
  - Changes from traditional control systems
- Difficulties in implementing security measures
  - Different from general IT security
    - High requirements in latency and uptime
  - Changes from traditional control systems
    - Home electronics (e.g. air conditioners)
    - Devices that are physically easy to access





Next Generation Grid

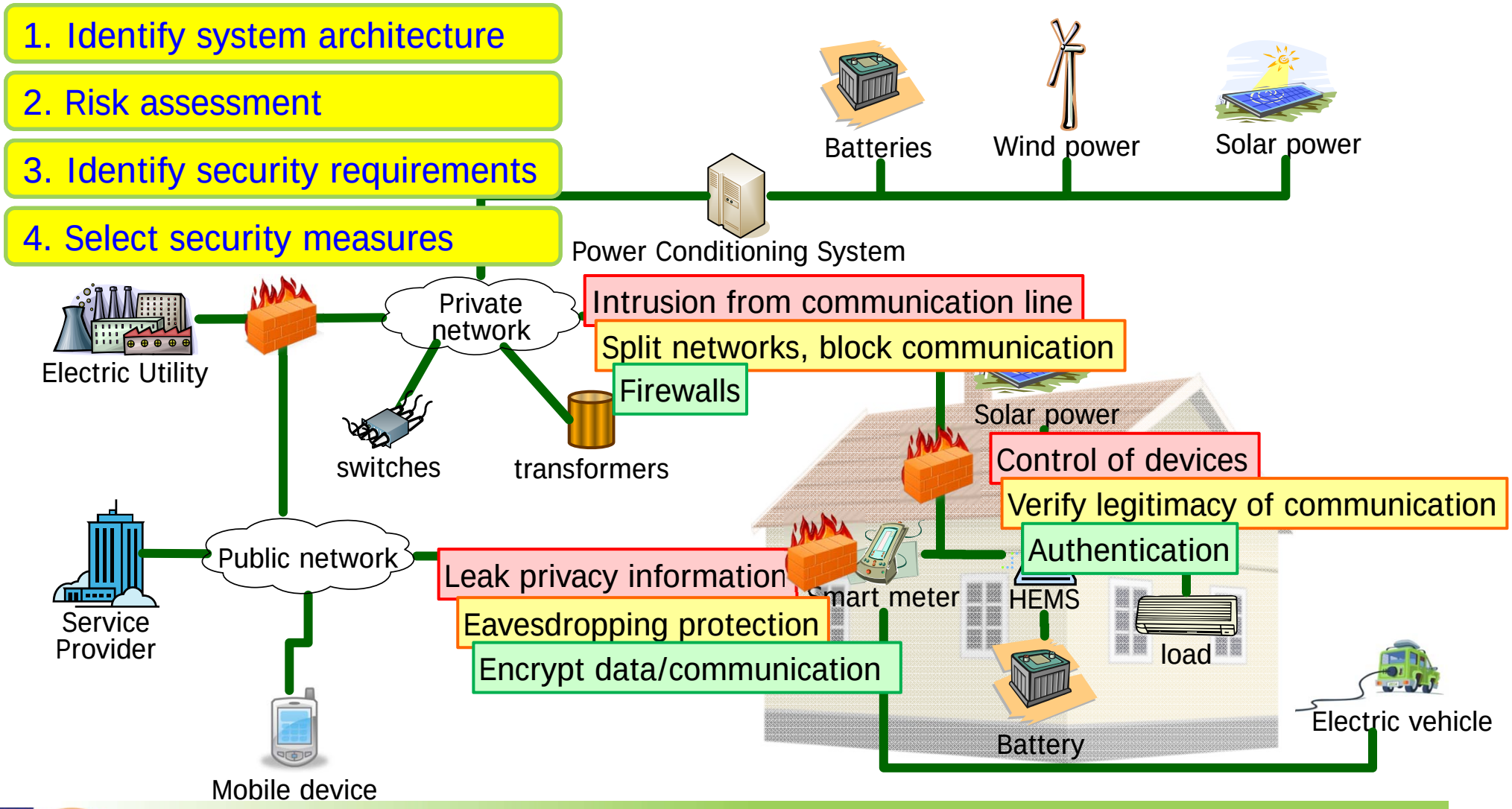


- Minimize risk of large blackouts with secure and stable operation of resilient and self-healing system
- Conservation and efficient utilization of energy with integration of demand and supply
- Enable large penetration and effective utilization of distributed energy resources
- Sophisticate asset management and introduce advanced power system maintenance and devices

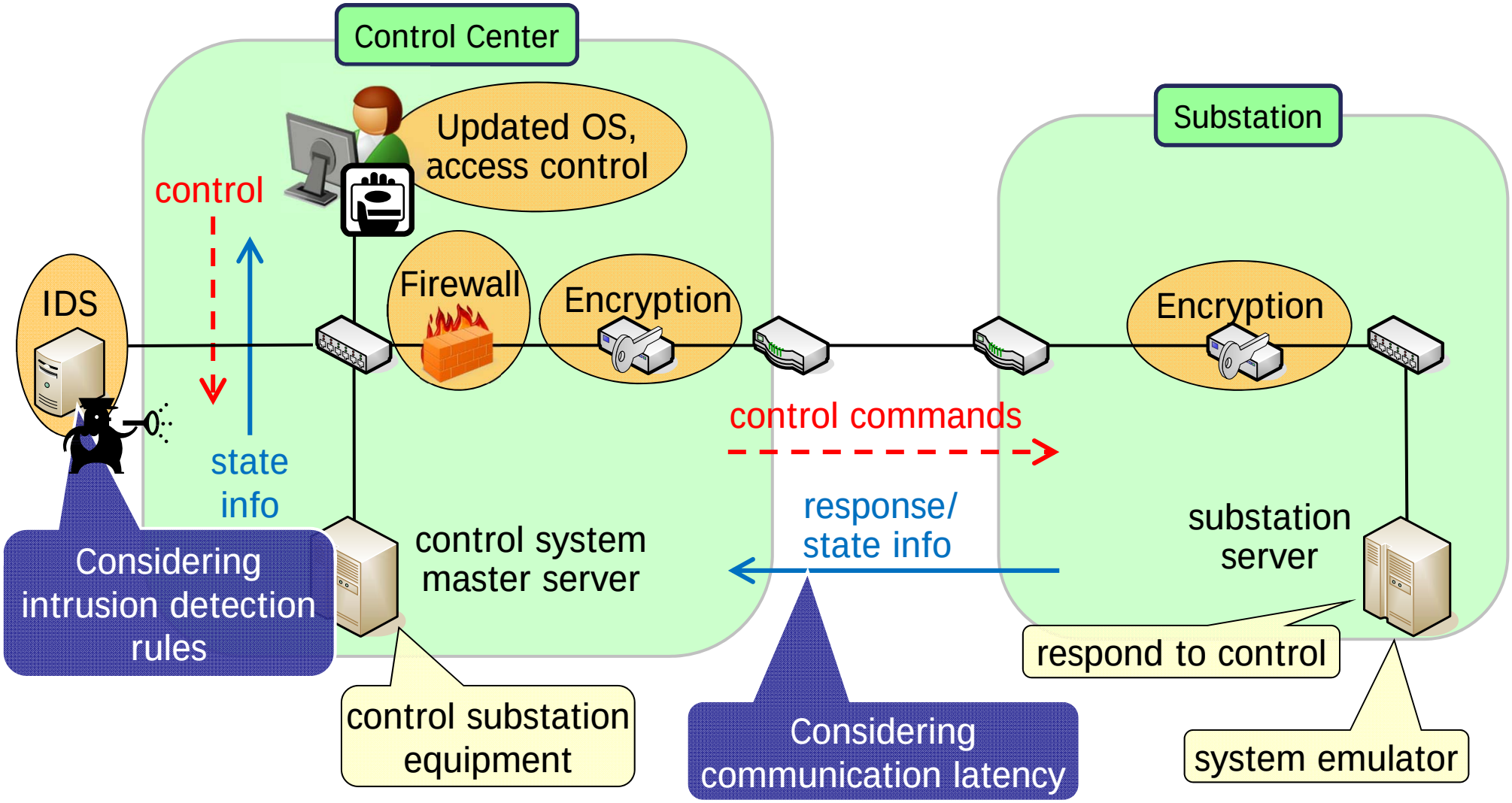
Points when Considering Cyber Security

- IT risk
  - Evaluate IT risk for control systems using general IT
  - Analyze trade-off between cost and security
- Security measures considering communication quality
  - Identifying security for smart meters and other devices
  - Evaluate possibility of combination of various measures
- Placement of security measures
  - Placing security measures according to cost, risk, services, communication requirements, etc.

Secure Communication Network in Demand-Area – Security Strategy and Measures in a Modeled System



Example of Cyber Security Assessment

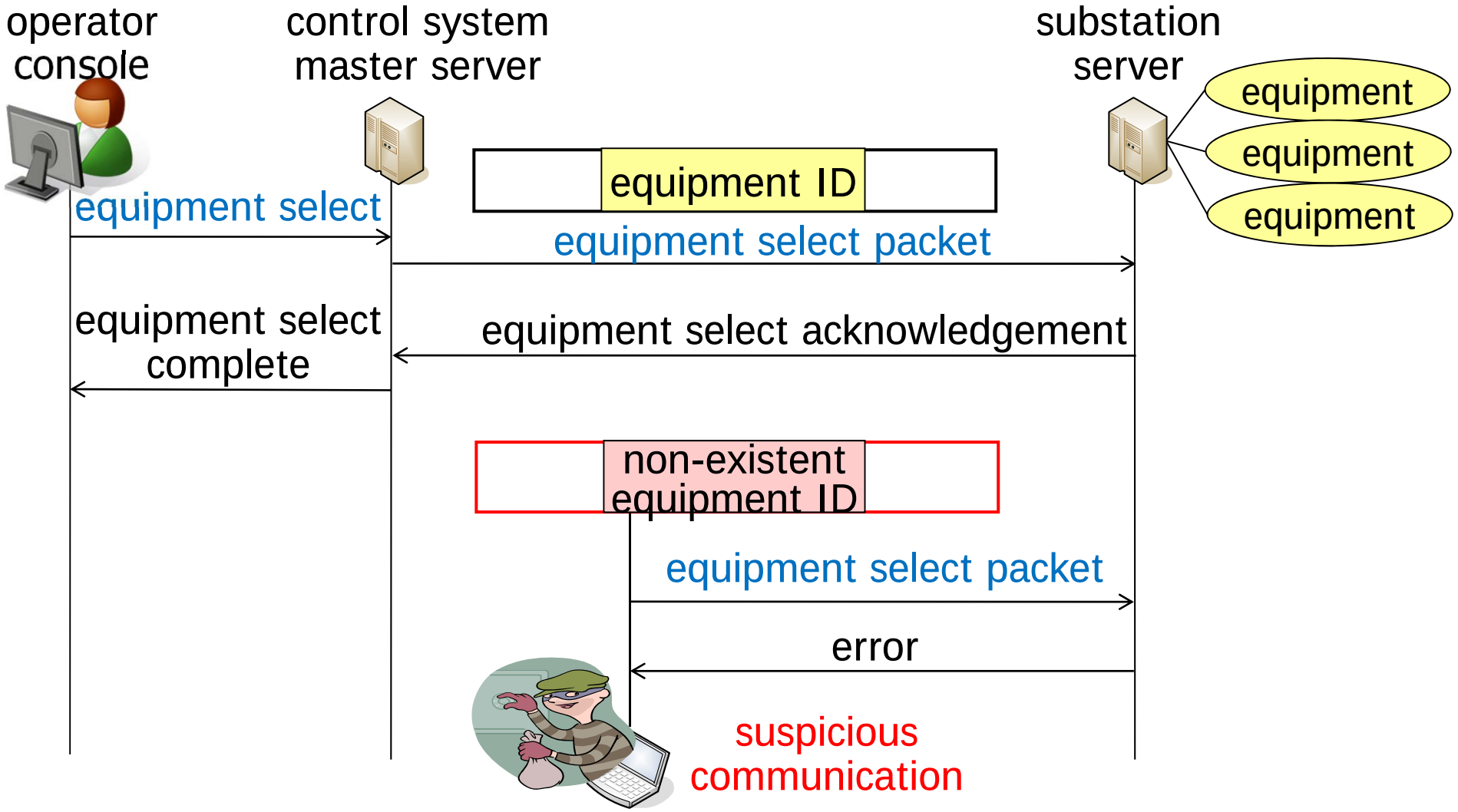


Intrusion Detection Rules

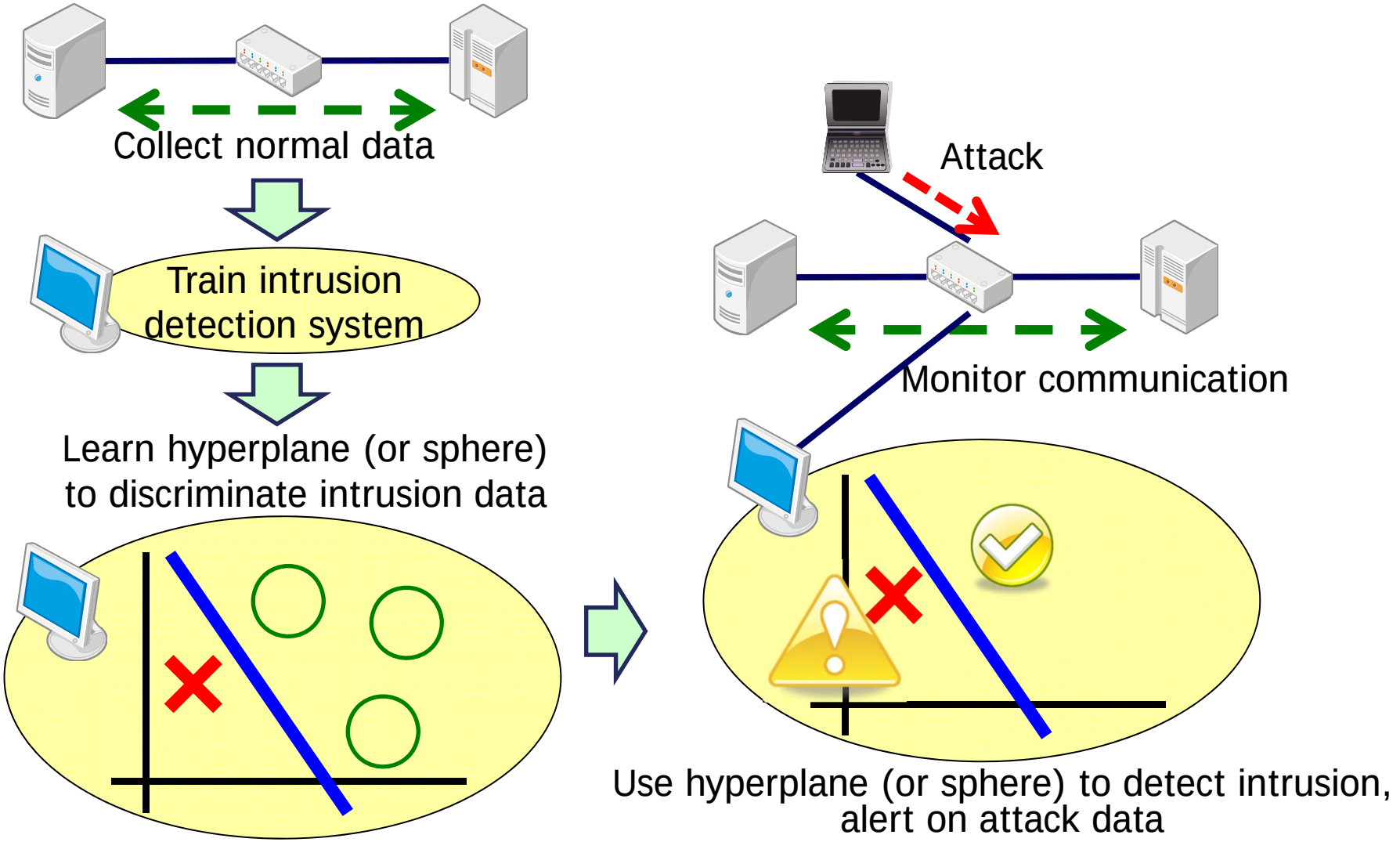
- Control system may benefit from a fine-tuned intrusion detection system, detecting more sophisticated attacks

- Intrusion detection rules checking the protocol used by the control system application
  - Detect traffic patterns that should not occur during normal operation through the operator console
  - Rules tailored to the particular vendor application
  - Use of machine learning algorithms to construct rules

Example of Intrusion Detection at the Application Layer



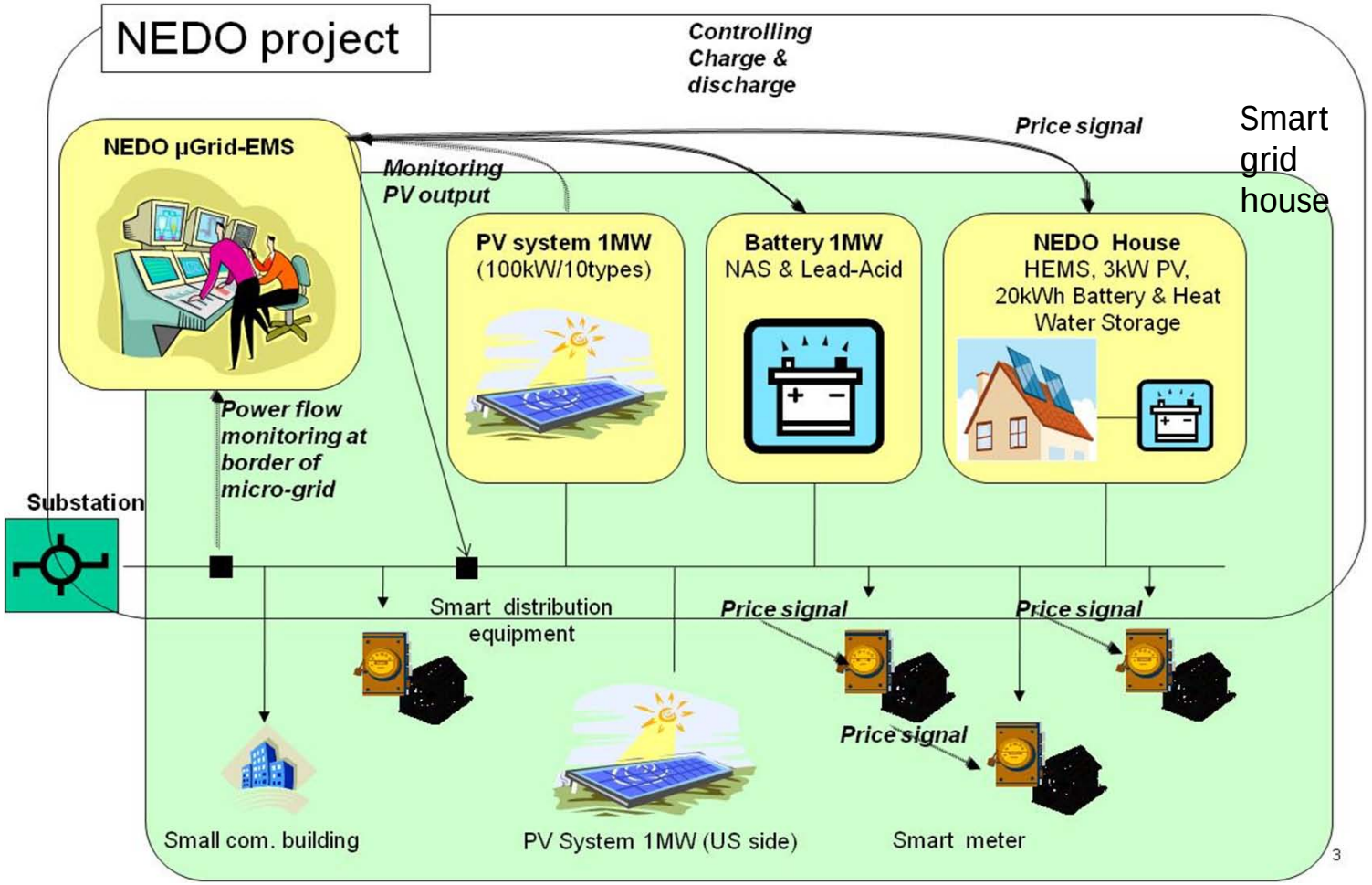
Example of Machine Learning in Intrusion Detection



Future Work

- Security strategy and measures for a detailed, realistic system
  - Application of strategy to actual system
    - NEDO's Japan-U.S. Smart Grid Collaborative Demonstration Project in New Mexico, USA
  - Steps toward securing the system
  - Placement of security measures
  - Cost and security trade-off
    etc.
- Further work on constructing intrusion detection rules
  - Advanced use of machine learning

NEDO's Japan-U.S. Smart Grid Collaborative Demonstration Project in New Mexico, USA



NEDO report No. 1054, 2009.11.4 (in Japanese)
New Energy and Industrial Technology Development Organization (NEDO)

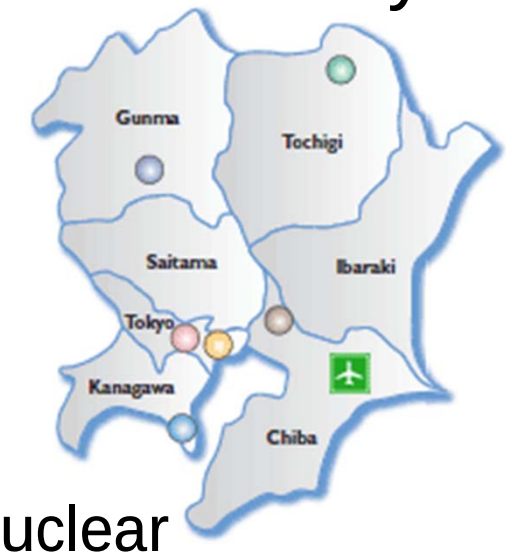
Thank you!

Mai KIUCHI

mai@criepi.denken.or.jp

About CRIEPI

- Central Research Institute of Electric Power Industry
  - Established in 1951
  - Funded by electric utilities in Japan
  - 840 employees
    - 740 researchers
  - Many areas of research
    - Socio-economics, system engineering, nuclear technology, civil engineering, environmental science, electric power engineering, energy engineering, materials science



http://criepi.denken.or.jp/en/index.html

CRIEPI International Collaborations

- International Institutions
  - IAEA
- Asia
  - KEPRI
  - KERI
  - TPC
  - SIIT
  - KAERI
  - Shanghai Jiao Tong Univ.
  - IEM
  - CEPRI
- America
  - EPRI
  - SwRI
  - Univ. of Illinois
  - LLNL
  - Ohio State Univ.
- Europe
  - AEAT
  - EURATOM
  - The Interfaculty Reactor Institute/ The Delft Univ. of Technology
  - NAGRA
  - CEA
  - BNFL
  - SCK/CEN
- Africa
  - ESKOM
- Oceania
  - CSIRO
  - CRCCSD

and others...

http://criepi.denken.or.jp/en/aboutcriepi/partner.html