
# IoT for energy infrastructure

- For loss cost reduction and sustainability of **O&M**

August 30th, 2016

**Yoshiaki Ichikawa**

Research and Development group
Hitachi Ltd.

HITACHI
Inspire the Next

# Contents

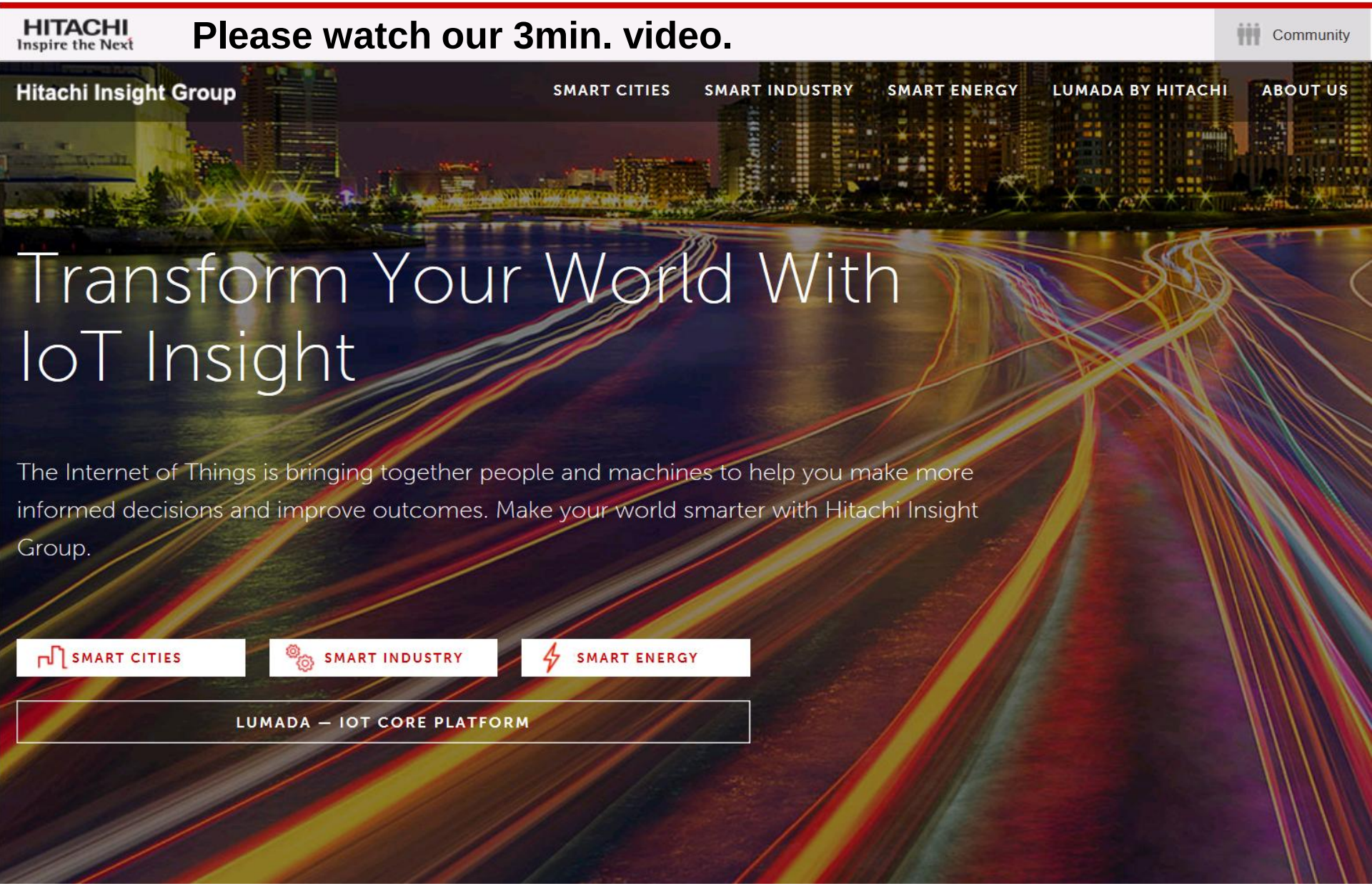
HITACHI
Inspire the Next

1. **Introduction**
2. How to utilize IoT for energy infrastructure
3. ICT Security trend
4. Security for energy infrastructure

# 1-1 IoT Overview

HITACHI
Inspire the Next

**Please watch our 3min. video.**




https://www.hitachiinsightgroup.com/en-us/home.html

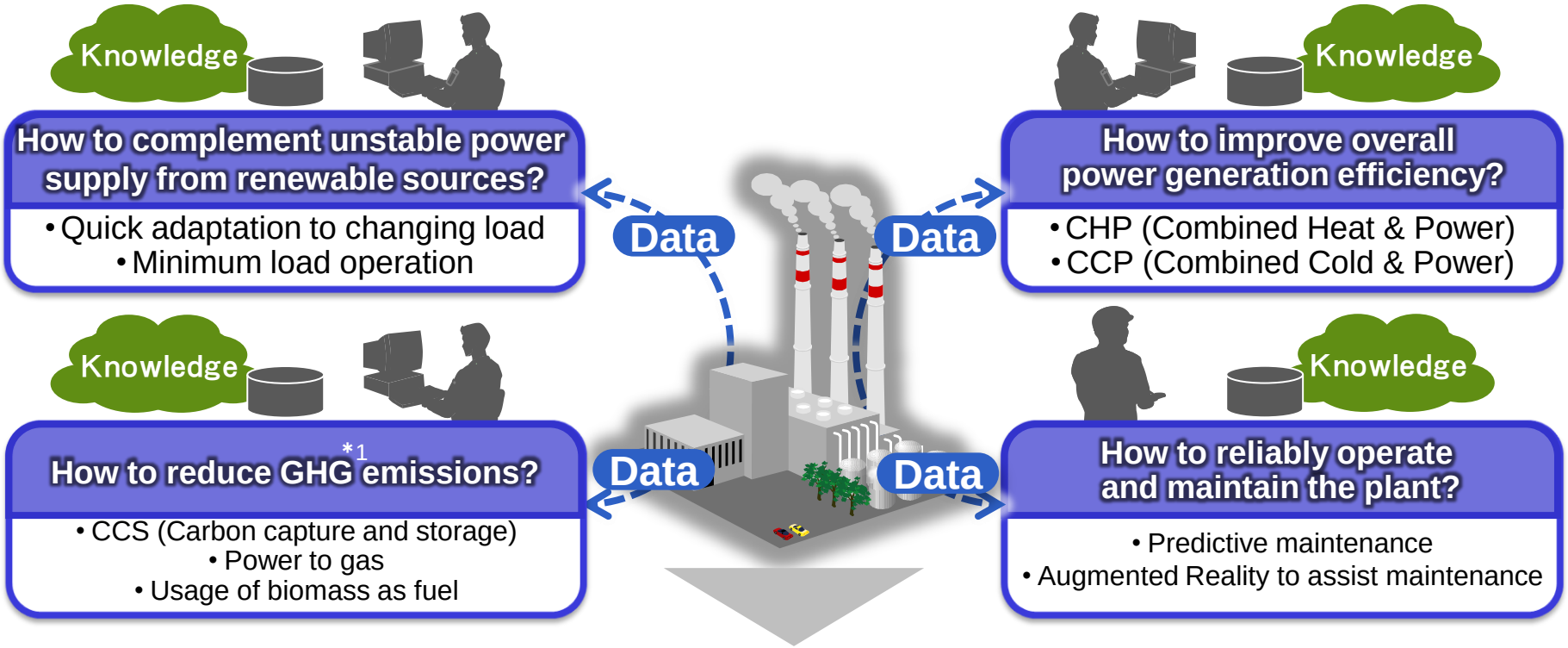
HITACHI
Inspire the Next

1. Introduction
2. **How to utilize IoT for energy infrastructure**
3. Cyber Security trend
4. Security for energy infrastructure

# 2-1 Challenges accompanying O&M of power plants

HITACHI
Inspire the Next

Total optimization of a thermal power plant becomes difficult as sub-optimized measures are separately developed with dispersive knowledge




- **Knowledge to improve ROA or to develop an investment plan is not effectively accumulated**
- **Return on investment on a system remains limited**
- **ROA and ROI deteriorate**

*1)GHG: Greenhouse gases

# 2-2 Concept to utilize IoT in power generation plants

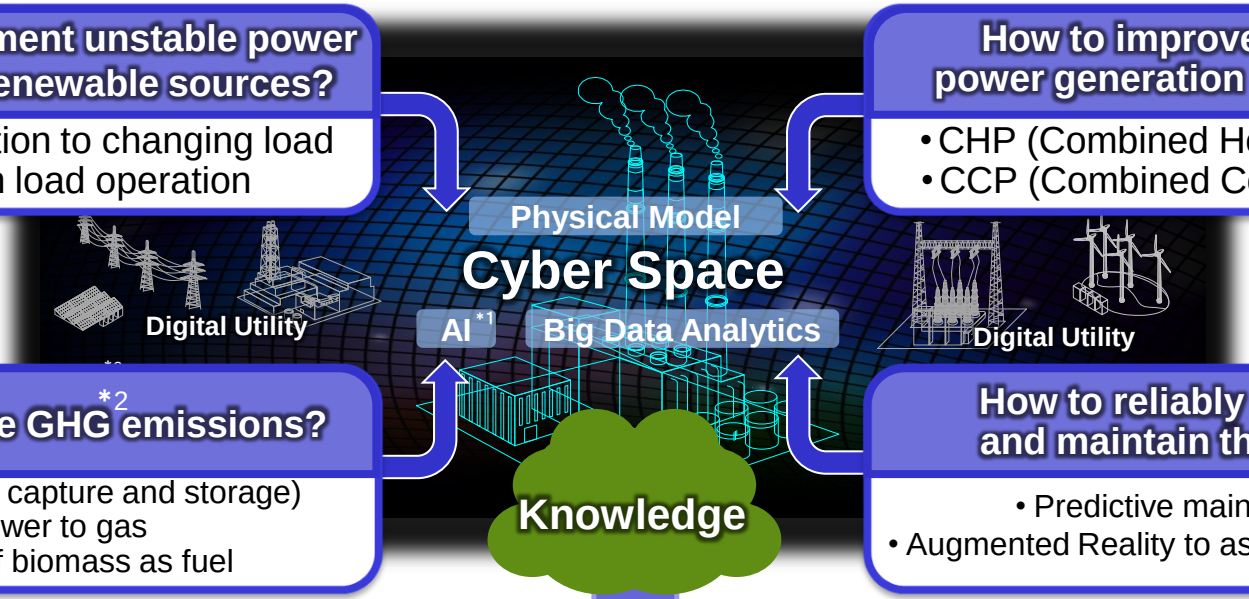
HITACHI
Inspire the Next

Totally optimize the plants and solve each issue through a platform to share in the cyber space know-how to operate power plants

**1 Connect the knowledge through the IoT under a secure cloud**

**How to complement unstable power supply from renewable sources?**
- Quick adaptation to changing load
- Minimum load operation

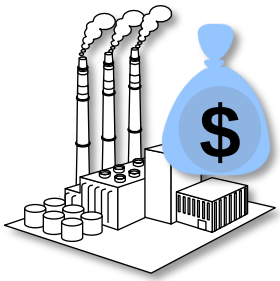
**How to improve overall power generation efficiency?**
- CHP (Combined Heat & Power)
- CCP (Combined Cold & Power)




**How to reduce GHG *2 emissions?**
- CCS (Carbon capture and storage)
- Power to gas
- Usage of biomass as fuel

**How to reliably operate and maintain the plant?**
- Predictive maintenance
- Augmented Reality to assist maintenance

**2 Optimize the total value chain and solve individual issues with analysis of big data**




**Improved ROI**

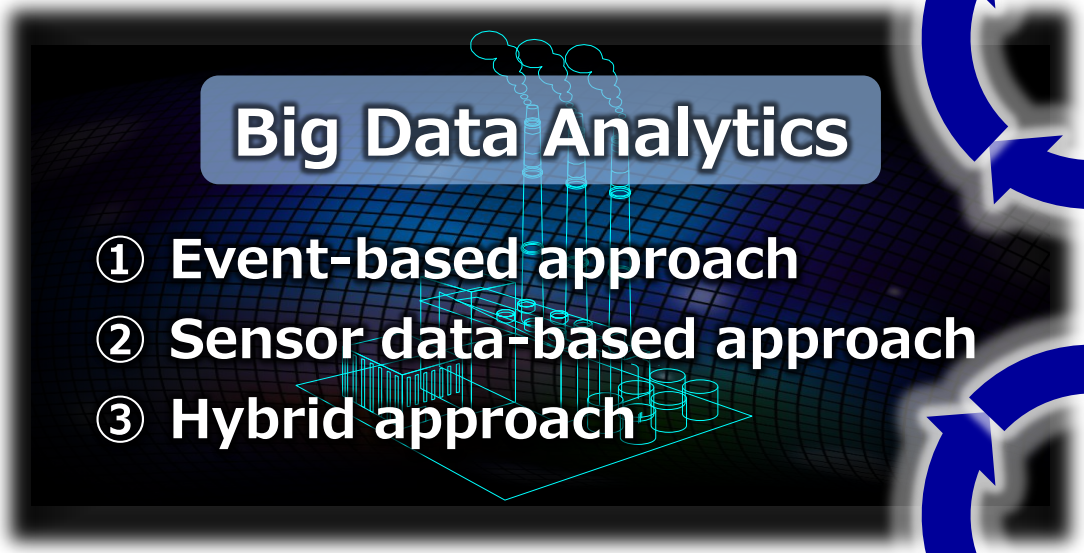
**Enhanced sustainability**

*1)AI: Artificial Intelligence 2) GHG: Greenhouse gases

# 2-3 Performance and Maintenance Effectiveness Analysis

HITACHI
Inspire the Next

The Performance Modeling and Analytics for Predictive Maintenance solution enables early detection of performance degradation and operational efficiencies and reduction of ineffective maintenance activities.

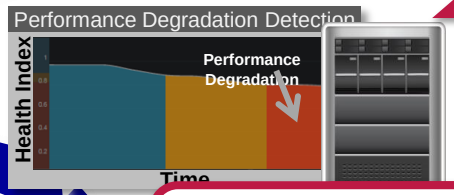



Orient


Decision

- Increase in ROI
- Sufficient information for decision

Management




- Accumulated knowledge
- Empowered workforce
- Improved safety

Decision

Field

Observe

Action

# 2-4 Event-based approach

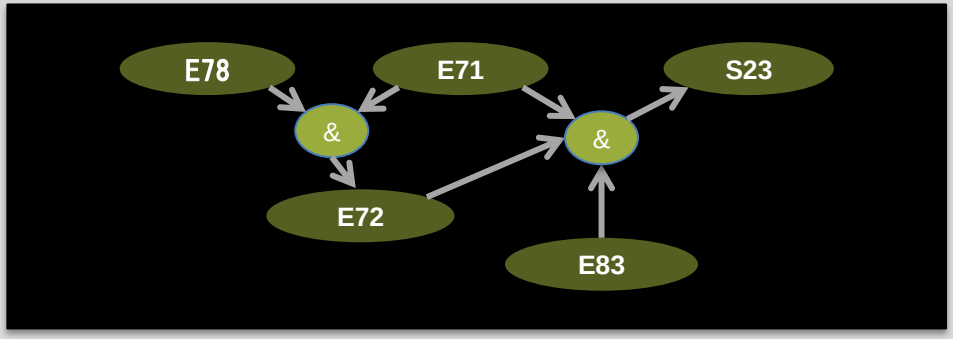
HITACHI
Inspire the Next

The Failure Prediction for Predictive Maintenance solution enables equipment and component failure prediction by monitoring sensor and event data.
The solution benefits include increasing equipment availability, avoiding catastrophic failures and reducing repair and maintenance costs.

Event-based failure prediction by learning prediction rules from historical events and applying the rules over real time event data.

## Event-based Failure Prediction

(1) Learn association between past events
(2) Use associations to predict future events



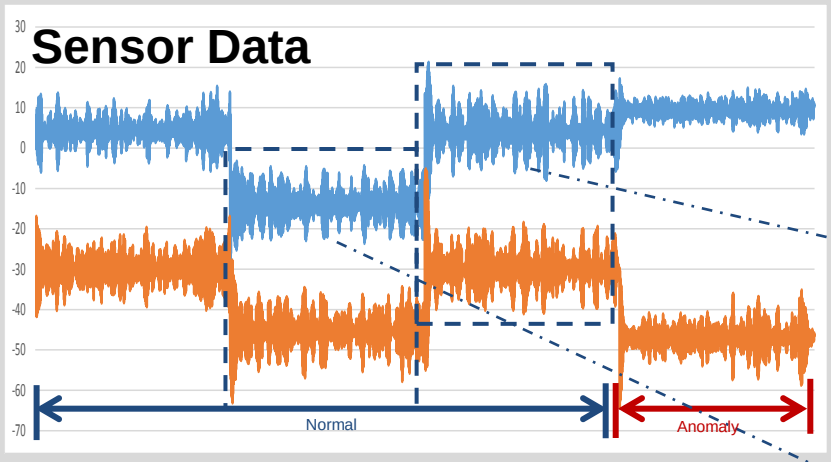

| Event | Description | Predicted Event | Impact | Confidence |
|---|---|---|---|---|
| E71, E72, E83 | Electrical System, Engine, Tires | S23 | Standby | 99% |
| E71_A | Engine | S23 | Standby | 96% |
| E77 | Hydraulic Oil Leak | S23 | Standby | 95% |
| E71, E78 | Electrical System, Propulsion | E72 | Engine | 64% |

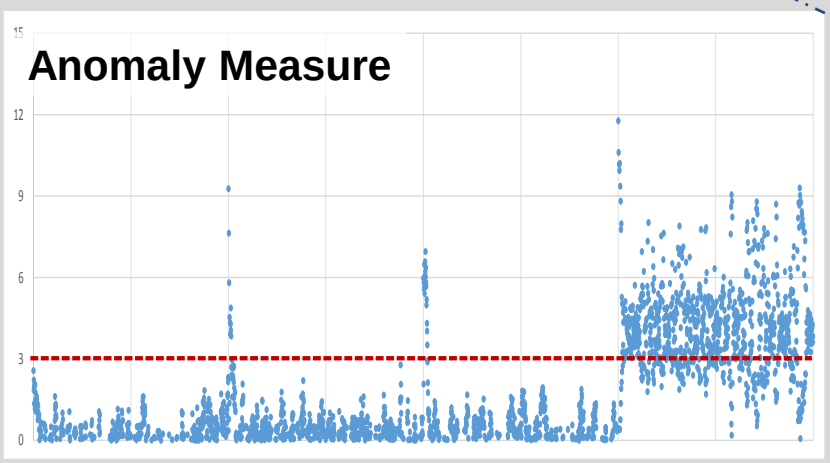
# 2-5 Sensor data-based approach(1)

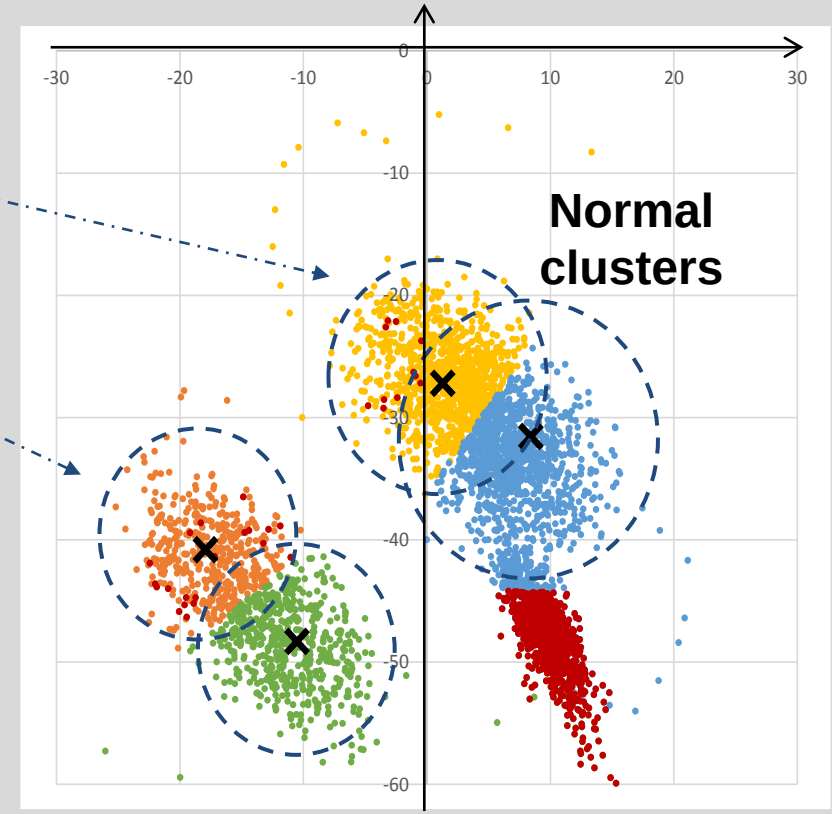
HITACHI
Inspire the Next

Sensor-based failure prediction by learning normal behavior of sensors and detecting deviation in real time from this normal behavior as potential failure.

## Using Anomaly Detection



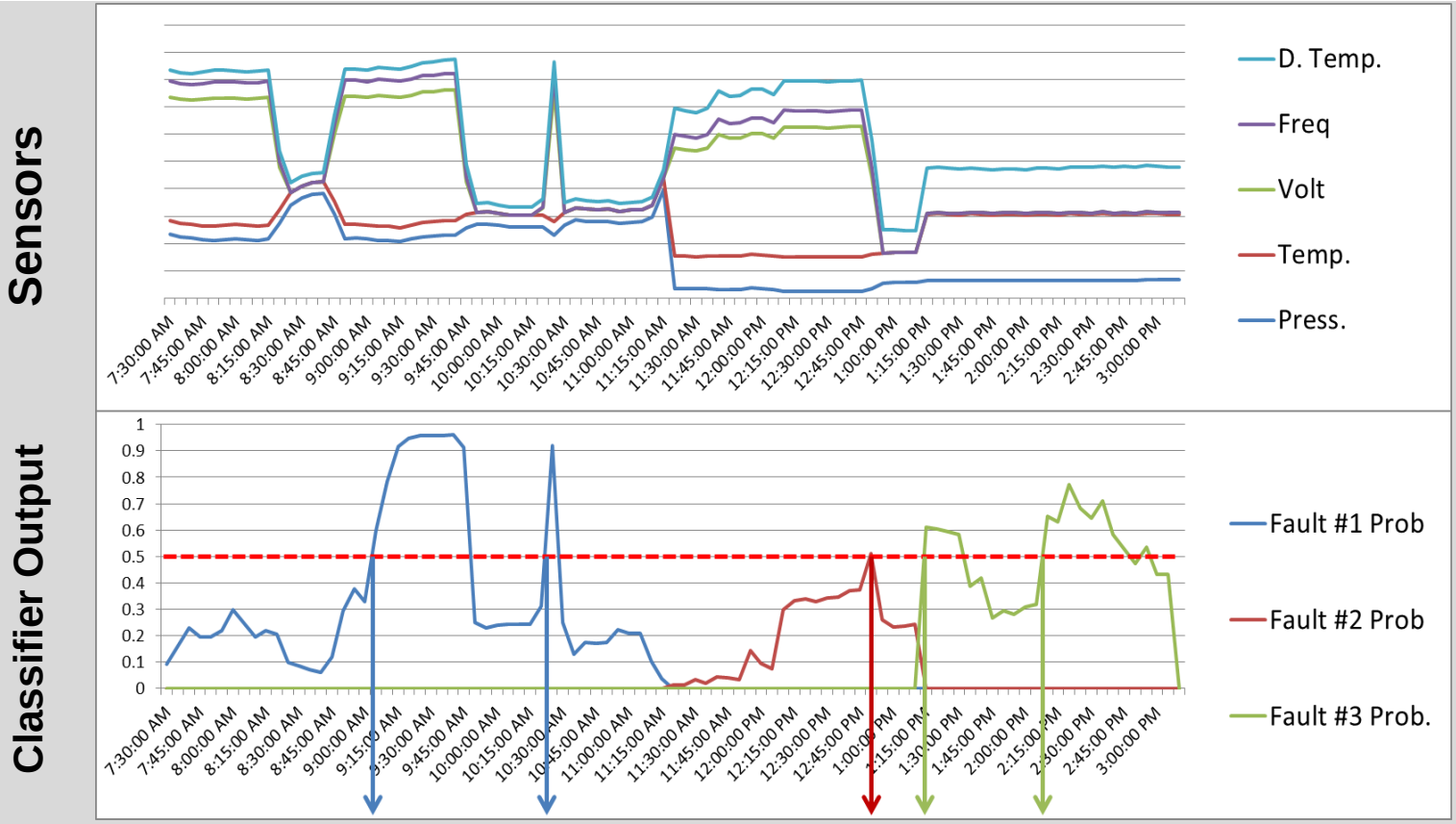



# 2-6 Sensor data-based approach(2)

HITACHI
Inspire the Next

Sensor and event based failure prediction by learning classification based models for different categories of failures (from previous failure instances) and predicting failure by applying models over real time sensor data.

## Using Classification Models

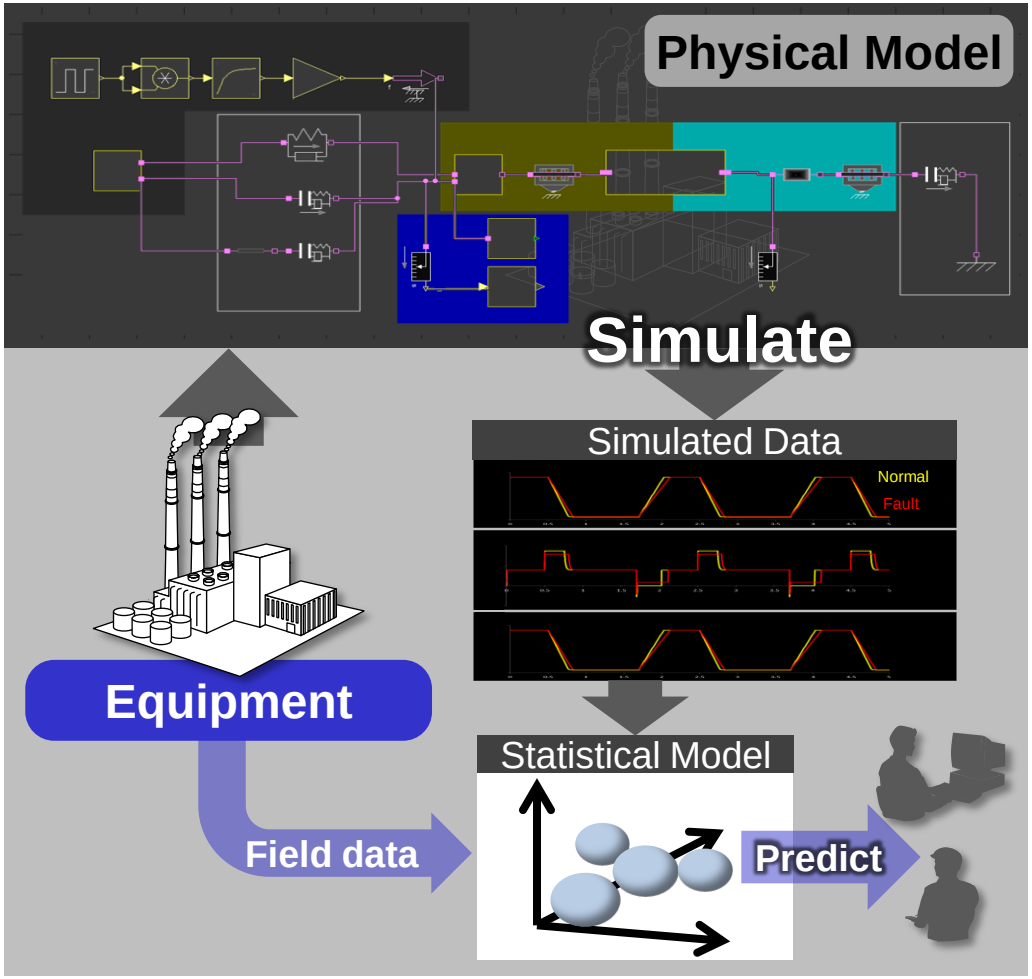


# 2-7 Hybrid approach

HITACHI
Inspire the Next

A challenge companies are often faced with is the limited amount of failure data available for training the machine learning model. This is especially relevant in regards to reliable equipment that often do not fail in the field.

A physical model can simulate normal and faulty behavior. Once a statistical model is learned from simulated and field data, it can predict the severity of fault mode over real time data.



HITACHI
Inspire the Next

1. Introduction
2. How to utilize IoT for energy infrastructure
3. **Cyber Security trend**
4. Security for energy infrastructure

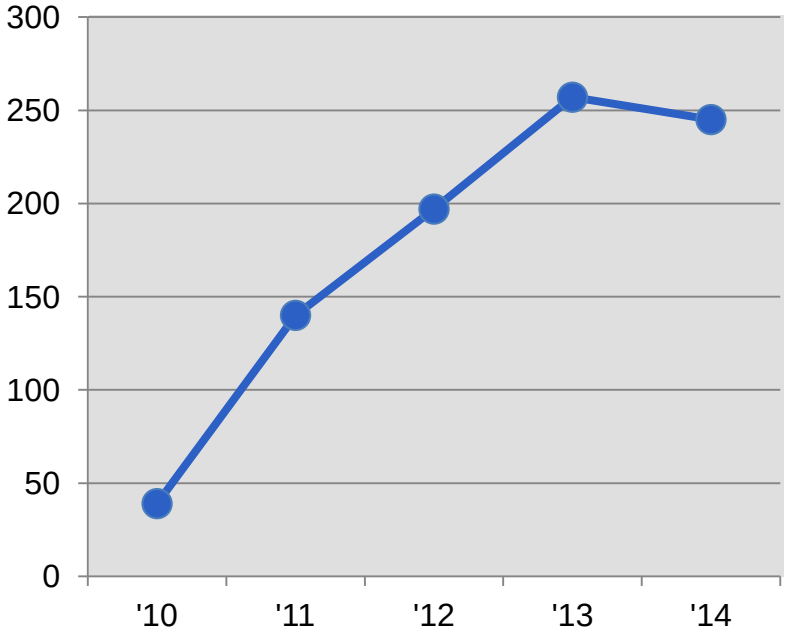
# 3-1 Trends in cyber threats

HITACHI
Inspire the Next

## Increase in number and in sophistication of cyber attacks causing actual damages

- Cyber threats on control systems are increasing
- Attacks are optimized with careful examination of targets
  - ➡ Actual damages are caused

Number of incidents in control systems




(SOURCE: Annual Reports of US ICS-CERT)

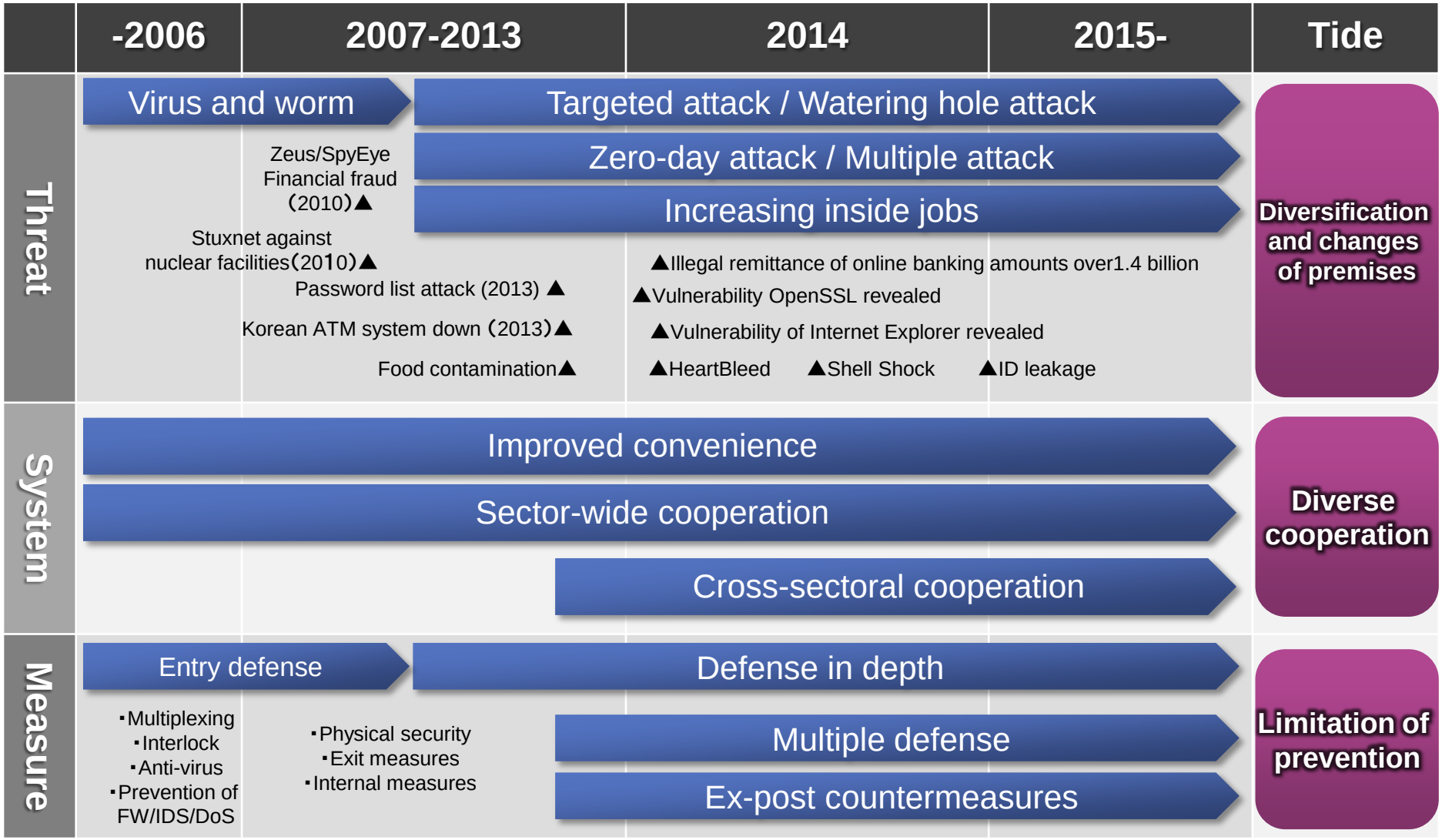
Examples of cyber attacks on important infrastructures

| Date | Target (country/area)<br>Content | Amount of damages |
|---|---|---|
| **Jul. '10** | Nuclear facility (Iran)<br>Destruction of the facility | NR |
| **Mar. '12** | Financial institutions (World)<br>Information leakage | $80M |
| **Aug. '12** | Oil company (Middle East)<br>Destruction of the facility | NR |
| **Mar. '13** | Broadcasting and financial institutions (South Korea)<br>System down | $800M |
| **Jun. '15** | Public authorities (Japan)<br>Information leakage | NR |
| **Dec. '15** | Power Plant (Ukraine)<br>System down and area blackout | NR |

ICS-CERT: The Industrial Control Systems Cyber Emergency Response Team
NR: Not Reported

# 3-2 Trends in security: Transition of attacks

HITACHI
Inspire the Next




FW: firewall IDS: Intrusion Detection System DoS: Denial of Service

# 3-3 Trends in security measures

HITACHI
Inspire the Next

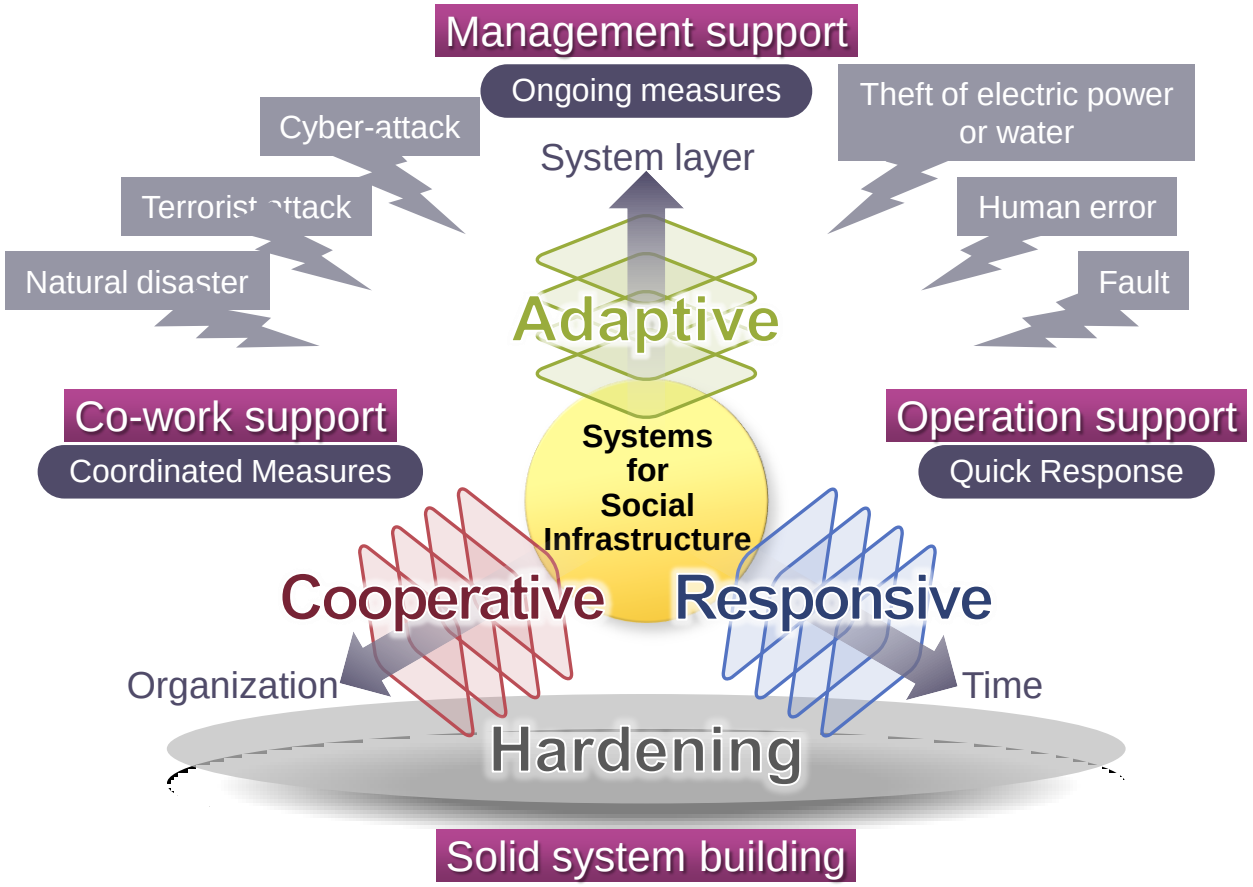
## Besides hardening of systems, continual adaptation, responsive counter and information sharing become important

| Category of measures | Description |
|---|---|
| **Hardening of systems** | Zone a system into manageable units and detect suspicious behaviour within each unit |
| **Continual adaptation to threats** | Considering trends in threats, regularly grasp risks within the system and update/enhance measures to harden the system |
| **Responsive counter to threats** | Ensure that a threat does not invade in the system by full-time monitoring and analyzing the operation states of measures to harden the system |
| **Sharing information on threats** | Prepare for a potential incident by sharing front line's threats and risks with stakeholders such as the managers, the industry, the customers |

# 3-4 Hitachi's security concept: "H-ARC® Concept"

HITACHI
Inspire the Next

- Adopted by the IEC White Paper "Factory of the future"
- Proposes a total security system covering the entire life cycle of customers

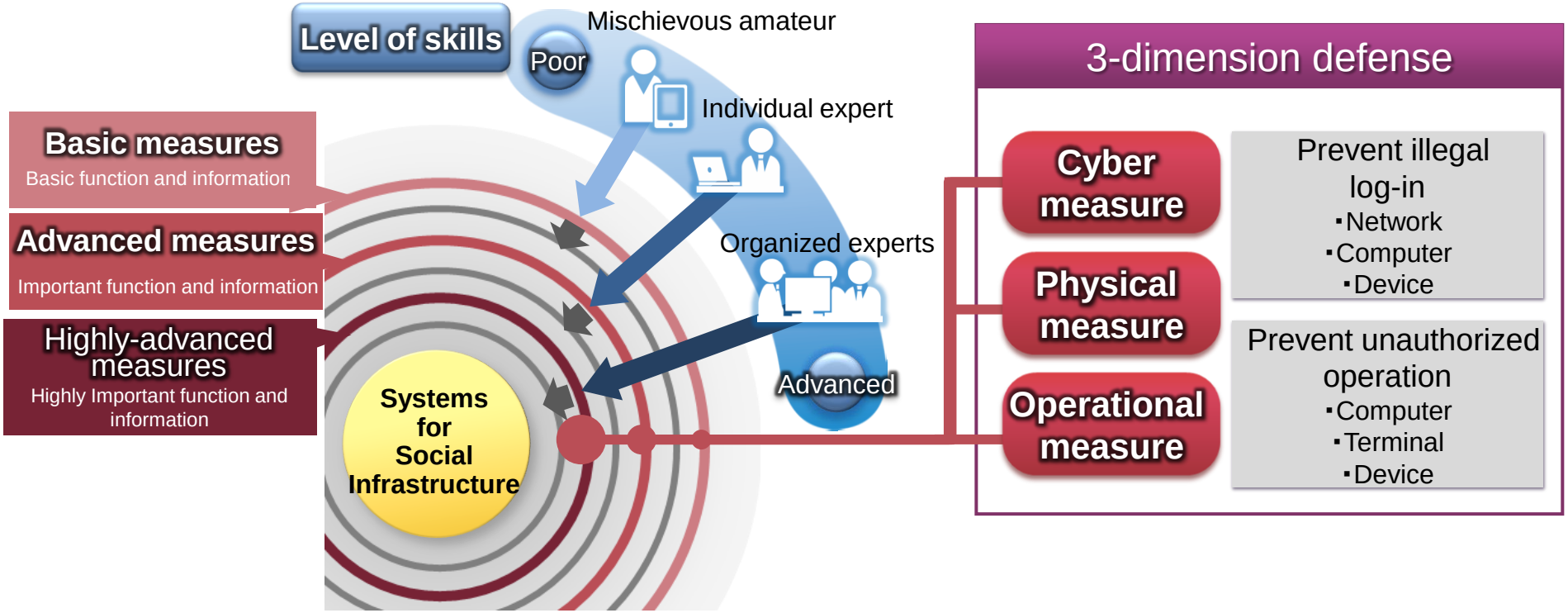




Hitachi provides integrated security system based on the **H-ARC®** concept

# 3-5 Concept of security measures

HITACHI
Inspire the Next

- Defense in depth against attackers' multiple skills
- 3-dimension defense measures (i.e. Cyber, Physical & Operation) corresponding with levels of attacks

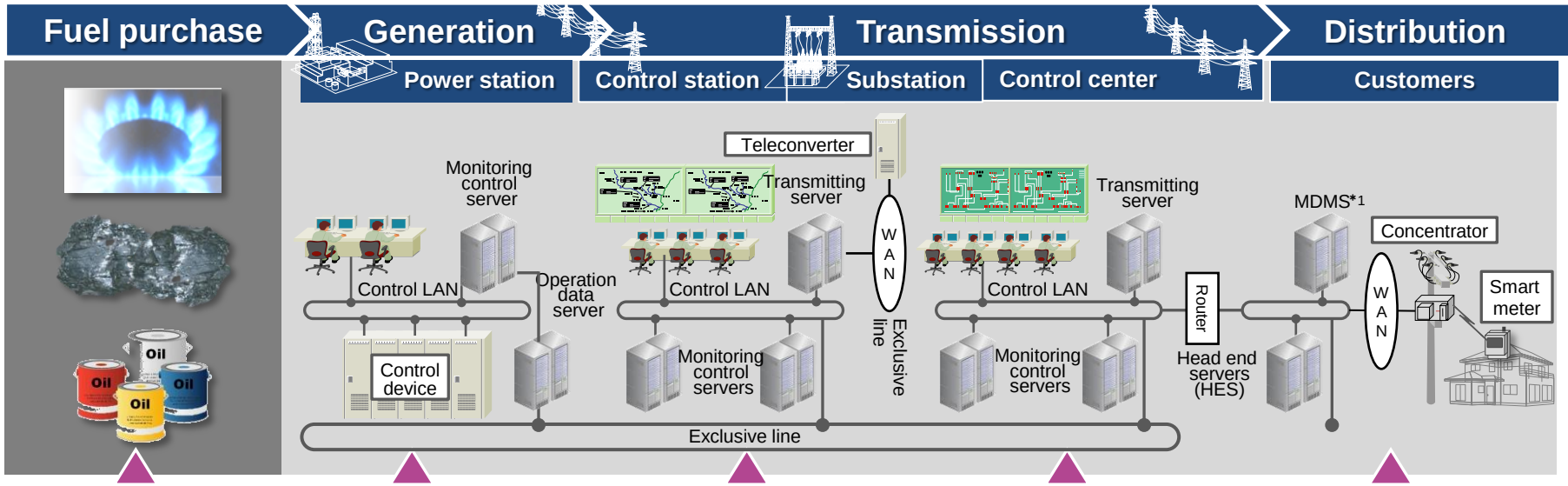


HITACHI
Inspire the Next

1. Introduction
2. How to utilize IoT for energy infrastructure
3. Cyber Security trend
4. **Security for energy infrastructure**

# 4-1 Assumed threats on control systems for power systems

HITACHI
Inspire the Next

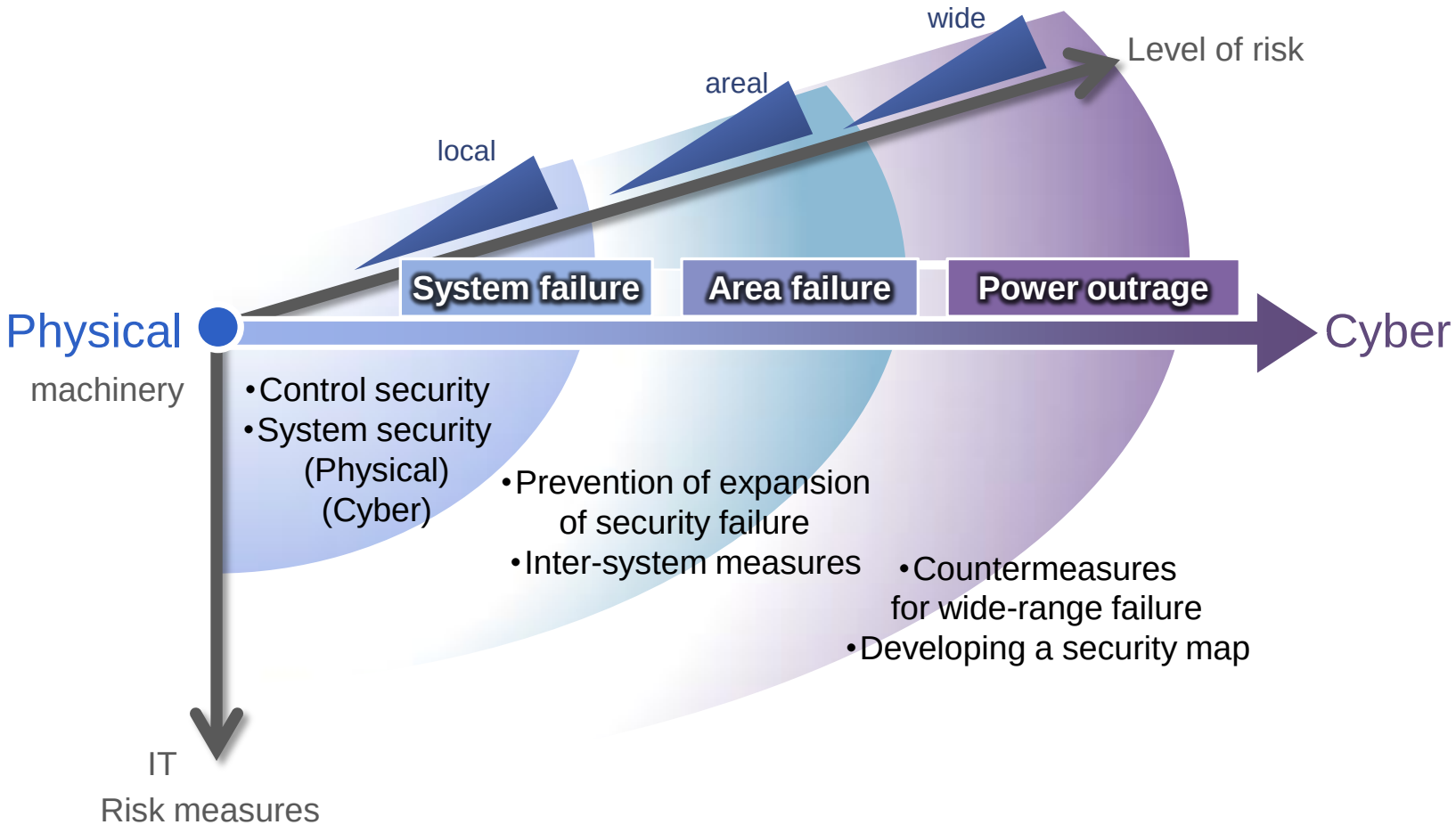



| Terrorism and cyber attacks on **fuel facilities** | Terrorism & cyber attacks on **power stations** | Terrorism & cyber attacks on **substations** | Terrorism & cyber attacks on **control centers** | Terrorism & cyber attacks on **smart meters** |
|---|---|---|---|---|
| | • Falsification of control parameters, plant data, fuel data<br>• Interference of operation<br>• Destruction of devices<br>• Invasion to network<br>• Injection of malware<br>• Denial of service attack<br>• Information leakage<br>• etc. | • Interference of operation<br>• Unauthorized operation of devices<br>• Falsification of plant data<br>• Invasion to network<br>• Denial of service attack<br>• Information leakage<br>• etc. | • Interference of operation<br>• Unauthorized operation of devices<br>• Falsification of operation data and form<br>• Invasion into network<br>• Denial of service attack<br>• etc. | • Falsification of power consumption data<br>• Invasion into network<br>• Denial of service attack<br>• etc. |

# 4-2 Assumed expansion of influence in the power sector

HITACHI
Inspire the Next

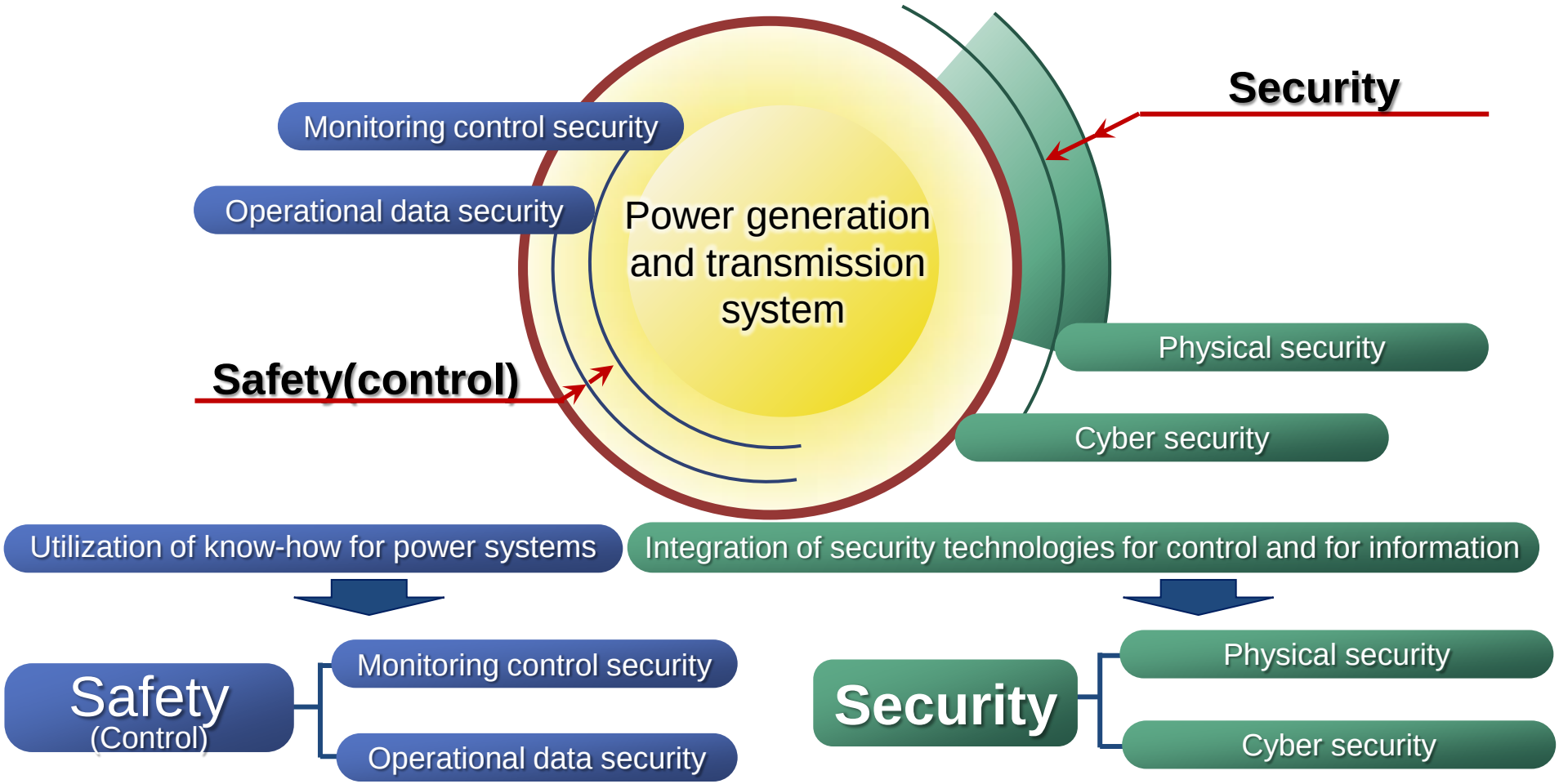
- A local cyber attack can cause a system failure.
- Multiple cyber attacks can cause an area failure.
- A wide-range cyber attack can cause power outrage.



# 4-3 Control security and system security

HITACHI
Inspire the Next

Power system security protects power generation and transmission systems with an in-depth defense composed of the control security (safety) based on know-how of power systems and of the system security integrating security technologies for control and for information.



HITACHI
Inspire the Next

# END

**IoT for energy infrastructure**
- For loss cost reduction and sustainability of **O&M**

August 30th, 2016

**Yoshiaki Ichikawa**

Research and Development group
Hitachi Ltd.


HITACHI
Inspire the Next

# THE FUTURE IS OPEN TO SUGGESTIONS

**Hitachi Social Innovation**

**Delivering new value to society through collaborative creations with our customers and partners**