Featured Articles I

Power Sector Examples

Hitachi's Approach to Security for Power Control Systems

Masahiro Murakami
Hideki Hanami
Hiromichi Konno
Ryuichi Okamoto
Mitsuaki Ishiba

OVERVIEW: The power market reforms in Japan, which include wide-area operation, retail market deregulation, and the separation of generation and transmission, are expected to widen the scope of the networks that connect power systems in the future. Accompanying this is growing interest in security measures for power control systems together with recognition of the importance of these measures. Hitachi is drawing on its experience with power control systems built up over many years to investigate security measures that make the most of technologies for control and for information security by identifying what form power control security should take and analyzing security risks in terms of control, people (behaviors), and information. This article describes Hitachi's approach to power control security and presents a case study of its work.

INTRODUCTION

THE power market reforms in Japan, which include wide-area operation, retail market deregulation, and the separation of generation and transmission, will lead to a wider scope of operation for the communication networks that connect power systems, including the transmission of information about power use as well as the power itself from consumers to generators. Safety is the top priority for power equipment, and together with the ongoing requirement for security of supply, this means that there is a need for security measures that can deal with increasingly sophisticated attackers.

This article describes Hitachi's approach to power control security in terms of contributing to the security of the power supply, and presents a case study of its work[1].

SECURITY THREATS TO THE POWER INFRASTRUCTURE

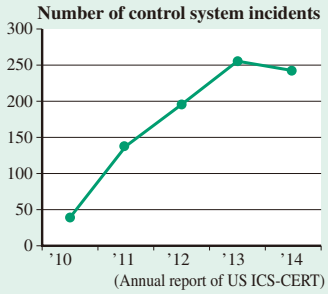
Increasing Ingenuity and Diversity of Cyber-attacks

Numerous instances of damage resulting from cyber-attacks on critical infrastructure around the world, such as nuclear power plants and power transmission and distribution systems, have been reported since the 2010 cyber-attack on nuclear facilities in the Islamic Republic of Iran (see Fig. 1).

Damage-causing attacks on critical infrastructure are increasing in frequency and ingenuity

- Growing prevalence of cyber-threats against control systems
- Optimization of attacks based on investigations that take account of targets

➡ Actual incidents of damage



Instances of cyber-attacks on critical infrastructure

Date	Target (location) Damage inflicted	Cost
2010/7	Nuclear facilities (Islamic Republic of Iran) Equipment damage	NR
2012/3	Financial institutions (worldwide) Information theft	$80M
2012/8	Oil company (Middle East) Equipment damage	NR
2013/3	Broadcaster, financial institution (South Korea) System shutdown	$800M
2015/6	Public agency (Japan) Information theft	NR
2015/12	Power plant (Ukraine) System shutdown	NR

US: United States ICS-CERT: Industrial Control Systems Cyber Emergency Response Team NR: not reported

Fig. 1—Security Incidents on Critical Infrastructure.
Attacks on critical infrastructure are increasing and their effects are expanding.

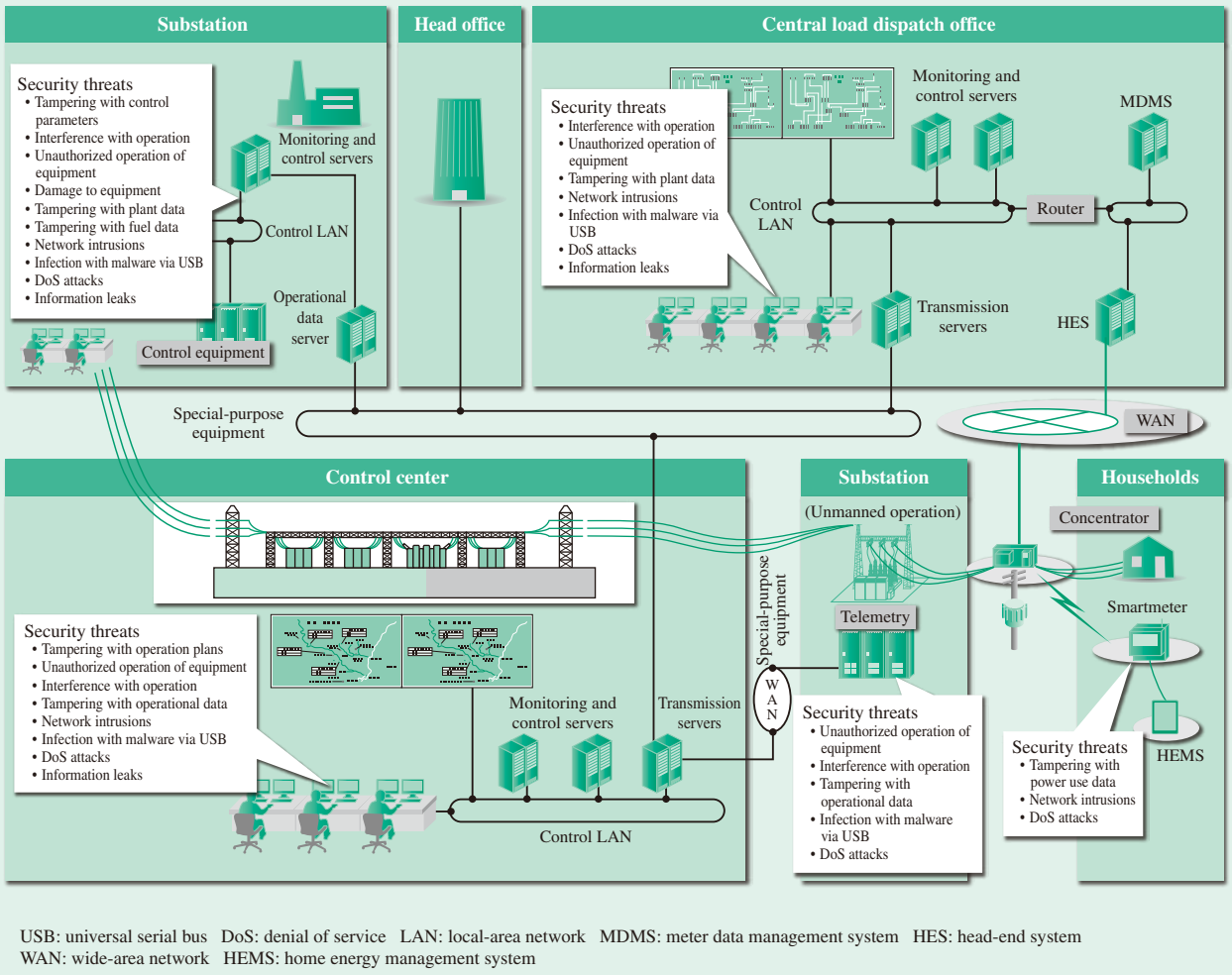


Fig. 2—Typical Security Risks for Electric Power Control Systems.
Critical infrastructure is connected to a large number of networks, each of which poses security threats. The consequences of a serious incident extend from localized damage such as faulty equipment operation to damage to important facilities such as power plants or substations, carrying a risk of damage spreading to the wider power system.

The methods used in recently reported cyber-attacks on critical infrastructure are seen as exposing critical infrastructure to the threat of highly malicious and ingenious cyber-attacks, with instances in which, rather than a simple cyber-attack such as one that seeks to exploit information, the aim has been to gain access to control systems and acquire and decode control information to identify specific equipment and prevent it from being controlled properly.

Risks Faced by Power Control Systems

Potential cyber-attacks on power control systems include both physical attacks, such as intrusions by people with malicious intent, and sophisticated cyber-attacks, such as intrusions that use universal serial bus (USB) or other media and control network intrusions from the Internet that enter via data networks.

In the past, power control systems in Japan were at very low risk of cyber-attack from the Internet due to the use of proprietary technology and special-purpose closed control networks. Nowadays, however, these systems are increasingly connected via firewalls or other security equipment to information systems for purposes such as big data applications or greater convenience. As a result, they are at increased risk of attack by people with expertise in advanced cyber-attack technology.

The sorts of cyber-attacks that might occur on a power control system go beyond the exploitation of control information or denial of service (DoS) attacks on networks to also include attacks aimed at disrupting the reliable operation of critical infrastructure by means such as tampering with control signals or unauthorized operation of equipment (see Fig. 2).

HOW HITACHI VIEWS POWER CONTROL SYSTEM SECURITY

Security Concepts

In addition to complying with international and industry standards, it is important for power companies in particular to demarcate the required security measures into different levels based on the importance (in terms of safety and potential for damage) of the equipment concerned.

The Hitachi system security concept under which security is required to be adaptive, responsive, and cooperative has been adopted by Hitachi and has also been applied to power control systems.

To repel sophisticated modern cyber-attacks, it is becoming increasingly important to undertake adequate security design and provide detection and defense functions in the development phase, and to implement security measures, establish infrastructure for dealing with cyber-attacks, share information through collaboration with other relevant organizations such as Industrial Control Systems Cyber Emergency Response Teams (ICS-CERTs), and stage routine drills to enable the correct response when an attack occurs in the operational phase.

It is necessary during the operational phase not only to maintain the security levels assigned in the development phase, but also to maintain and enhance the security system by collecting the latest security knowledge. This is achieved by collecting and analyzing data from various points around the system to assess the state of system security, detect problems quickly, and respond appropriately when needed (see Fig. 3). That is, to strengthen security measures by utilizing the observe, orient, decide, act (OODA) loop to achieve quick and accurate decision-making as well as using the plan, do, check, act (PDCA) cycle of planning, improvement, and adjustment[2), (3)].

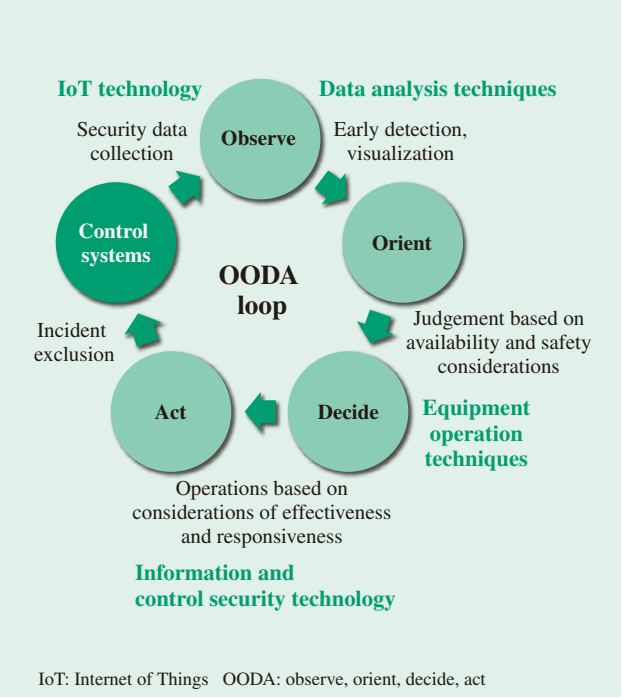


Fig. 3—Security Concept for Improving Availability of Power Control Systems.
The concept involves using the OODA loop to protect critical infrastructure from cyber-attack.

Introduction of Security Maps

Of greatest importance when providing security measures for critical infrastructure is to determine what needs to be protected and to ensure secure protection in order to maintain operation while also preserving robustness. Accordingly, Hitachi believes it is essential to consider the possibility of both physical and cyber-based attacks on power control systems, and to determine in advance for each item of equipment how to respond to an incident and the criteria for action.

This response requires the preparation of security maps in which the overall power system is split into zones and the potential consequences are assessed for each zone based on a risk analysis that considers both control security (a risk analysis based on control considerations) and system security, covering physical attacks on system equipment as well as cyber-attacks on networks and other information technology (IT) equipment.

Formulation of Security Policies

The next steps are to break the system down into the individual control systems, including central load dispatch offices and power plants, and to formulate individual security policies in accordance with the guidelines defined in the security map (see Fig. 4).

To produce these policies, Hitachi drew on its knowledgeable experience in power control systems, first to assess possible attack patterns by considering how attackers might go about attacking each system, then to collate specific defense measures for system equipment by considering how the system could be defended against each of these attacks.

In this way, Hitachi believes it is contributing to the reliable operation of power control systems by formulating responses for each item of equipment in the power system in a security map and security policies.

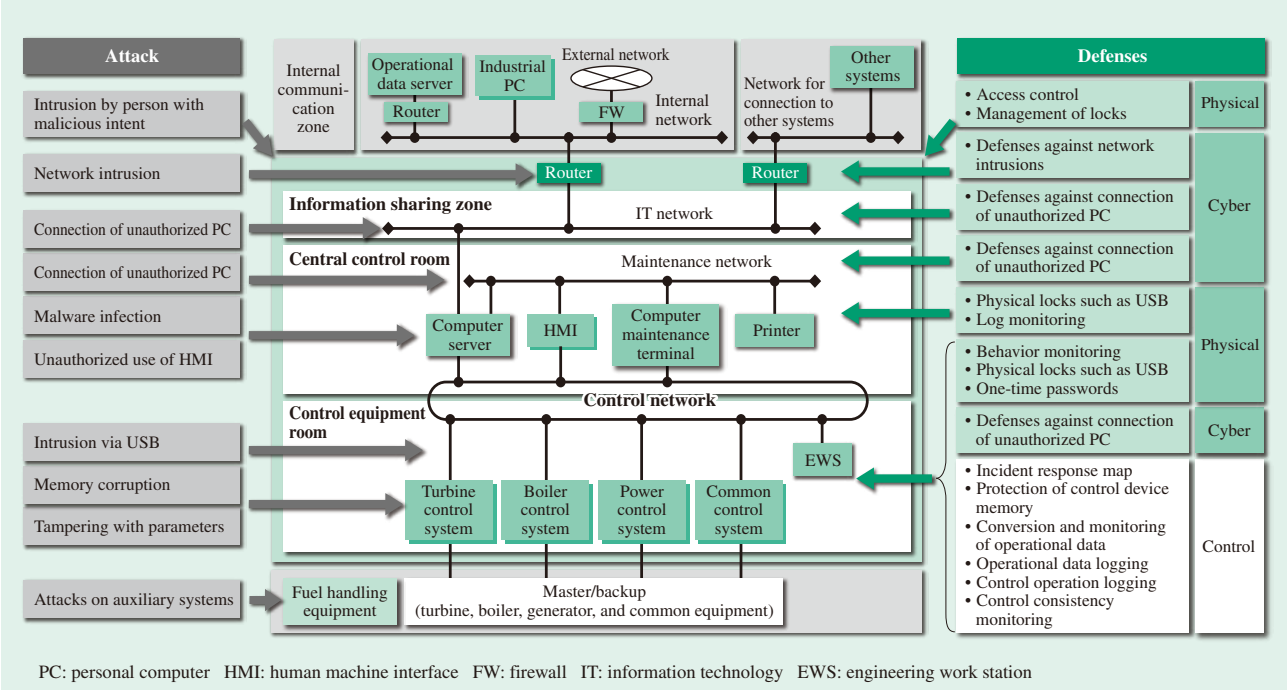


Fig. 4—Control System Security Policies.
By formulating security policies for control systems, power systems are protected by identifying all the different means of attack and implementing ways to detect and defend against them.

SECURITY SOLUTIONS

Power Grid Monitoring and Control Systems

Power grid monitoring and control systems have in the past run on closed control networks. It is anticipated that this will change in the future toward greater use of open control networks, bringing with it increasing opportunities for network interconnection with the outside world. Because such an environment carries a risk of large-scale power outages due to cyber-attacks on power grid monitoring and control systems, appropriate measures are needed. While the security measures on past power grid monitoring and control systems have included measures for preventing unauthorized access by installing firewalls at points of interconnection with systems at other sites or the various support systems, the threat of modern-day cyber-attacks and the increase in concerns about them have led to a growing trend toward stronger security measures, including intrusion detection systems (IDSs), whitelist control, and access control using identification (ID) cards.

Power Plants and Monitoring and Control Systems

Nuclear power plants in Japan have traditionally implemented physical security measures as required by the Act on the Regulation of Nuclear Source Material, Nuclear Fuel Material and Reactors. In the future, safety measures for workers will be tightened in the light of the accident at Fukushima Daiichi Nuclear Power Station. Similarly, while cybersecurity will continue to include use of conventional practices such as firewalls and data diodes, measures will also be strengthened to bring them up to international standards, with reference to factors such as previous work on security measures in the USA that has gone as far as to formulate design-basis threats and consider deep safeguards.

Likewise, with thermal and hydro power plants, control systems have traditionally been protected against external threats by the use of zoning, whereby systems are split into control and IT zones, and the installation of firewalls and other security devices at interfaces with the outside world.

A variety of measures are required for the control systems at some thermal and hydro power plants because they include equipment from different vendors. This makes it necessary to adopt practices that are not vendor-specific and to implement security measures with reference to the International Electrotechnical Commission (IEC) 62443 international standard for control security. In addition to control-based measures that cover protection, control, and operational data monitoring, Hitachi is strengthening security by

hardening through the use of equipment with Embedded Device Security Assurance (EDSA) certification and using a combination of physical and cyber-security.

Physical Security

As restricting physical access to important equipment and monitoring and control systems helps reduce cybersecurity risks as well as its obvious role in preventing unsafe activities, physical and cybersecurity complement each other. Access restriction involves assigning people to categories and limiting those who are able to access equipment to the bare minimum, while at the same time preventing people from bringing in dangerous goods and controlling possession of mobile media and other devices.

Because power plants are characterized by occupying large sites and buildings, locating where people are is important for security management and also useful for guiding staff in the event of an emergency.

With transmission and distribution equipment being spread across a wide area, Hitachi uses centralized management for access control and login authentication for control systems, and operates it in tandem with physical security.

CONCLUSIONS

The power control systems that support the electricity infrastructure are required not only to help optimize operations through the monitoring and control of transmission, distribution, and generation equipment, but also to counter new threats such as physical and cyber-based attacks while maintaining a reliable supply of power.

Along with power control systems, Hitachi also has expertise in power supply systems and technologies for control, physical security, and cybersecurity. This enables it to establish ways to deal with attacks on customer equipment using multiple layers of different types of defense. Hitachi is able to improve the resilience of both the hardware and software used in control equipment and to provide ongoing defense against increasingly sophisticated cyber-attacks on control and information systems through support supplied by its own Computer Security Incident Response Teams (CSIRTs), and it intends to contribute to the reliable supply of power and solving management challenges by protecting customer equipment.

REFERENCES

(1) Ministry of Economy, Trade and Industry, "2015 White Paper on Manufacturing Industries (Monodukuri)," http://www.meti.go.jp/report/whitepaper/mono/2015/honbun_html/index.html in Japanese.
(2) T. Nakano et al., "Control System Security for Social Infrastructure," Hitachi Review **63**, pp. 277–282 (Jul. 2014).
(3) M. Mimura et al., "Hitachi's Concept for Social Infrastructure Security," Hitachi Review **63**, pp. 222–229 (Jul. 2014).
(4) ZDNet Japan, "Establishment of Ecosystems Required by IT Companies," (Feb. 2015), http://japan.zdnet.com/article/35060584/ in Japanese.
(5) H. Horii et al., "Power System Technologies for Reliable Supply of Electric Power and Wide-area Grids," Hitachi Review **62**, pp. 53–59 (Feb. 2013).
(6) Hitachi, Ltd., Autonomous Decentralized System, http://www.hitachi.co.jp/products/infrastructure/product_solution/platform/middleware/autonomy_dispersion/index.html in Japanese.
(7) H. Kuwahara, "Experience Teach us the Future of Autonomous Decentralized Systems," International Symposium on Autonomous Decentralized Systems/Keynote Address, pp. 169–175 (1997).

ABOUT THE AUTHORS

Masahiro Murakami

Power Generation Plant & Power Grid Control Systems Engineering Department, Power Information & Control Systems Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the power infrastructure O&M services design business utilizing the Internet of Things (IoT).

Hiromichi Konno

Power Generation Plant & Power Grid Control Systems Engineering Department, Power Information & Control Systems Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the power infrastructure O&M services design business utilizing the IoT.

Mitsuaki Ishiba

Nuclear Power Control and Instrumentation Systems Engineering Department, Power Information & Control Systems Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the nuclear power control systems design business.

Hideki Hanami

Nuclear Power Control and Instrumentation Systems Engineering Department, Power Information & Control Systems Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the design and development of nuclear power control systems and security systems.

Ryuuichi Okamoto

Power Systems Engineering Department, Power Information & Control Systems Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the power grid systems design business.