Nuclear Security and Incident Response

Kazuhiko Tanimura
Hisayuki Ito
Hiroyuki Kimura

OVERVIEW: Since the Great East Japan Earthquake, there has been a requirement for even greater strengthening of nuclear incident response functions. It is also assumed that compliance with new recommendations issued by the IAEA in 2011 aimed at preventing terrorism will be required in the future. In addition to its know-how in ensuring the reliability of nuclear power plants built up through the past activities of its nuclear power business, Hitachi also has know-how in C2 and training exercise functions acquired through its defense business, and technologies and products in the field of crisis management. Hitachi intends to utilize these to make an even greater contribution to nuclear power plant safety and peace of mind in the future, including new nuclear incident response and security functions.

INTRODUCTION

LIVELY debate on the use of nuclear energy is currently ongoing in a variety of forums, and one of the issues raised in the context of new policy for nuclear power has been the strengthening of functions for incident response in the event of a severe nuclear accident.

Meanwhile, it is anticipated that use of nuclear energy will be pursued internationally in the future as an effective means for the development of emerging nations and for countering global warming.

Use of nuclear energy clearly requires meticulous design of systems that provide rigorous levels of safety, and there are calls to strengthen nuclear incident response functions to keep damage to a minimum in the event that a disaster does occur. There is also a need to strengthen security functions that protect against not only natural disaster and accidents, but also human threats such as terrorism[(1)].

In this context, the International Atomic Energy Agency (IAEA) issued a revised version of the "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities" (INFCIRC/225/Revision 5) in 2011. The new revision included additional material relating to preventing nuclear terrorism that was motivated in part by the 9/11 terrorist attack in the USA.

This article describes how, with a view to compliance with Revision 5 of the IAEA Nuclear Security Recommendations, Hitachi aims to make further improvements in the future to the safety and security of nuclear power plants through new nuclear incident response functions that utilize know-how derived from its experience in the defense and security businesses, which include command and control (C2) and training exercise functions, and also technology for security systems.

ROLES OF NUCLEAR SECURITY AND INCIDENT RESPONSE

Table 1 lists the roles of nuclear security and incident response. The purpose of nuclear incident response is to protect the public, as stipulated in the 2004 Civil Protection Law (the Law Concerning

TABLE 1. Roles of Nuclear Security and Incident Response
The purpose of nuclear incident response is to protect the public, and the purpose of security is to protect nuclear material and information about nuclear material.

Items	Nuclear incident response	Security
Potential threat	• Natural disasters • Plant accidents (• Armed or terrorist attack)	• Armed or terrorist attack • Cyber-attack
Objective	• Protect general public.	• Protect nuclear material and information about nuclear material.
Users	• Central government • Local authorities (local government) • Nuclear power companies	• Nuclear power companies • Security forces (police, Japan Coast Guard)
Existing functions	• Radiation management • Radiation monitoring (local government, power companies)	• Nuclear PPS (compliance with Revision 4 of the IAEA Nuclear Security Recommendations)
Common requirements for next-generation systems	• C2 (COP, M&S technology) • Training (exercise scenarios, TTX/CPX/FTX) • Cyber-security	

PPS: physical protection system IAEA: International Atomic Energy Agency
C2: command and control COP: common operational picture
M&S: modeling and simulation TTX: table top exercise
CPX: command post exercise FTX: field training exercise

the Measures for Protection of the People in Armed Attack Situations, etc.), and the purpose of security is defined in the IAEA recommendations as "the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.[2]"

In the past, the systems used for these purposes have been implemented independently. Although planned and implemented separately, parts of the designs and utility systems and equipment can be shared, with examples including differentiating between unnecessary and useful redundancy, mutual backup, and complementarity. Based on experience from incidents such as the Great East Japan Earthquake and the 9/11 terrorist attacks, there is also a need to strengthen cyber-security to prevent malicious attacks and thefts of information, and also to provide comprehensive C2 and training exercise functions so that the organizations that operate incident response and security systems can function more quickly and effectively (see Fig. 1).

NUCLEAR INCIDENT RESPONSE

Training in the defense sector includes the regular conduct of a variety of exercises aimed at raising the preparedness of personnel and organizations, including table top exercises (TTXs), command post exercises (CPXs), and field training exercises (FTXs). This allows these organizations to maintain their ability to react appropriately to all sorts of different situations, as was demonstrated by many news reports relating to their disaster relief activities in the aftermath of the Great East Japan Earthquake.

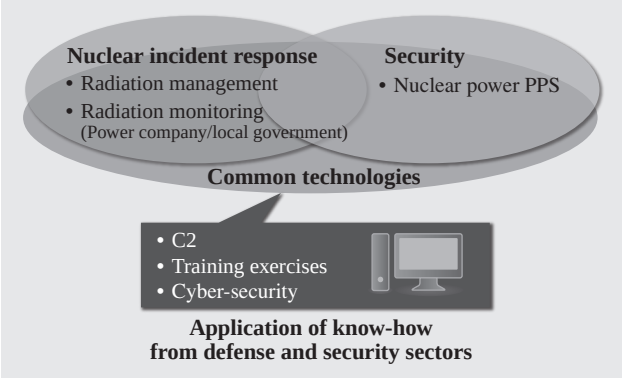


Fig. 1—Application of Know-how from Defense and Security Sector.
Know-how from the defense and security sector is applied to nuclear incident response and security to make further improvements in safety and peace of mind.

In the case of the emergency response to a severe accident at a nuclear power facility, it is worthwhile drawing on know-how in C2, training exercises, cyber-security, and other fields derived from the defense and security sectors to enhance functions for responding to a severe accident.

(1) C2

Establishing a common operational picture (COP) is one of the key concepts of C2. Having participants share a progressively changing situation in realtime allows the commander to issue appropriate instructions on what to do next, and personnel in the field can anticipate what preparations to make for the next tasks to be accomplished. When sharing information, providing people with information in accordance with their particular roles and responsibilities prevents them from being overwhelmed by large amounts of information.

In addition to the current plant status and level of radiation, other information that could be presented in a COP includes drawings and computer-aided design (CAD) data, tasking lists (realtime display of tasks, events, and task progress to groups formed during an emergency), aerial or satellite images, and the security information described later in this article (see Fig. 2).

(2) Training exercises

Training exercises are very important for ensuring that an accurate response is mounted when an incident occurs. The different types of training exercises include TTXs, in which a problem is debated around a table and a solution devised; CPXs, which are used for decision making training, and in which role playing based on simulation plays a central part; and FTXs, which involve practicing actual response activities in the field. In addition to making the various objectives of an exercise clear, establishing the framework for conducting exercises is also important. Once the

Fig. 2—C2 Image.
The COP function for sharing a changing situation in realtime at the command center and in the field is one of the key concepts.

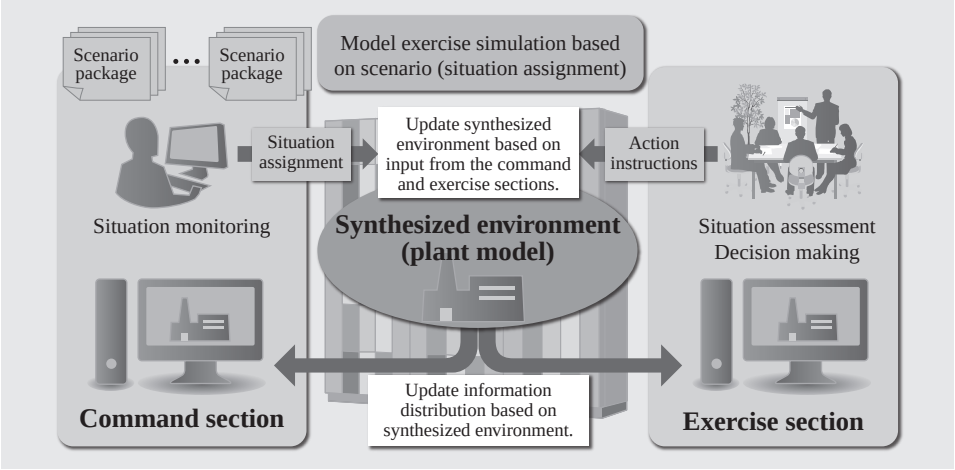


Fig. 3—Training Exercise Image.
To improve the effectiveness of training exercises, they are conducted based on scenarios created for each exercise objective.

objectives and exercise framework have been put in place, the exercise can be organized into scenario packages for each objective. These scenario packages are used in the process of conducting the exercise and for purposes such as assigning situations.

The C2 COP display includes exercise mode functions that enhance the effectiveness of an exercise by allowing people to view the assigned situations on screens that are formatted the same as the actual displays (see Fig. 3).

SECURITY

Security Trends

The focus on security that dates back to the Convention on the Physical Protection of Nuclear Material (CPPNM) in 1980 was initially concerned with ensuring the security of cross-border transportation. Subsequently, taking note of new concerns such as the diversion of nuclear materials resulting from the breakup of the Union of Soviet Socialist Republics and the September 11, 2001 terrorist attacks, the CPPNM was revised in 2005, extending its scope to also include the security of nuclear plants and the nuclear materials held by each country[3]. In December 2005, Japan amended the Nuclear Reactor Regulation Law (Law for the Regulations of Nuclear Source Material, Nuclear Fuel Material and Reactors) to strengthen the scope of nuclear material security. A Nuclear Security Summit was held in Washington, D.C. in the USA in April 2010, and the IAEA issued Revision 5 of its Nuclear Security Recommendations in November 2010.

Revision 5 of the IAEA Nuclear Security Recommendations designates the utilities that possess and manage nuclear material at nuclear facilities or other sites as having primary responsibility for conducting risk analyses of physical protection, and for implementing systems based on these analyses, expanding crisis management plans to include the period after actions that cause damage or other disruption, and putting organizational arrangements in place.

Main Points of Revision 5 of IAEA Nuclear Security Recommendations[1), 3)]

Revision 5 of the IAEA Nuclear Security Recommendations adds the following requirements for the security of nuclear facilities.

(1) Need for design of delaying measures

Consideration of nuclear security from the site selection and design stage

(2) Response that takes account of potential for coordination between external and insider threats

(3) Measures for dealing with remote attacks and cyber-attacks, etc.

(4) Introduction of a nuclear security culture

(5) Force-on-force exercises

Recommendation of regular performance testing and TTX

(6) Sharing of measurement management information

(7) Installation of backup alarm stations

(8) Redundancy for central alarm stations

Security System Solution

The following solutions are available for implementing the security enhancements specified in Revision 5 of the IAEA Nuclear Security Recommendations described above. These solutions are supplied through Hitachi's defense and social infrastructure security businesses.

(1) Flexibility to establish delaying measures

It is assumed that measures such as the installation and reassignment of sensors through the application

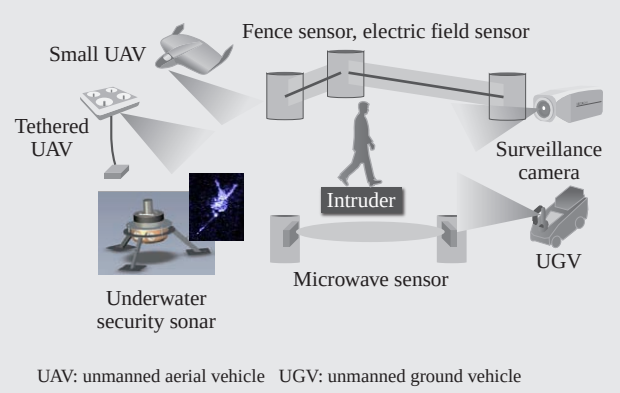


Fig. 4—Overview of Monitoring Sensors.
Appropriate monitoring sensors are selected to suit the location and purpose from among the wide range of sensors available.

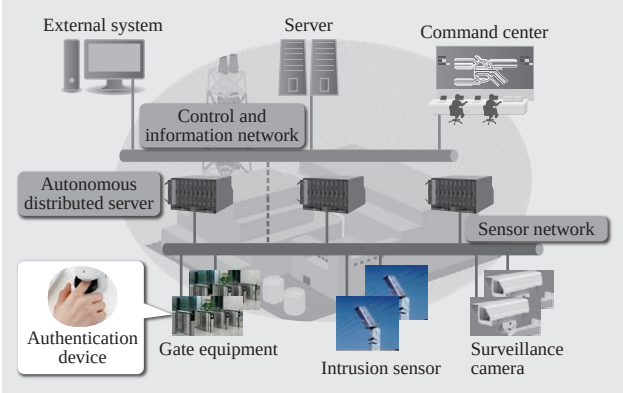


Fig. 5—Highly Reliable Design Using Autonomous Distributed Architecture.
An autonomous distributed architecture is used to achieve a fault-tolerant system design.

of graded methods will be used to establish or change protected areas. When installing gates and other provisions for access control, appropriate sensors, gates, and other devices can be selected from the range of such equipment available for this purpose (see Fig. 4).

These devices are connected to autonomous distributed servers that are installed at different locations, as required. Use of an autonomous distributed architecture with a fault-tolerant system design that complies with the IEC 61508 standards (International Standard for Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems) allows the system to operate continuously in such a way that the overall system can maintain the required level of functional performance even when equipment is upgraded or retrofitted (see Fig. 5).

Command centers are designed to coordinate information from sensors and video surveillance, while also reducing the amount of surveillance work required from security staff by using automatic tracking, whereby suspicious activity and other features of people and vehicles within the monitored area are identified from a large number of surveillance cameras (see Fig. 6).

(2) Cyber-security

As frequent cyber-attacks targeting particular groups or organizations have occurred in recent years, there is a need to provide stronger protection against such attacks on important infrastructure. Measures that can be used against threats from insiders include solutions that encrypt all data on hard disk drives (HDDs) and other devices so as to prevent access from all but authorized personnel (see Fig. 7 and Fig. 8).

(3) Force-on-force exercises

The use of personal equipment such as wearable communications devices, sensors, and ad hoc communications is considered to be an effective way to conduct worthwhile FTXs at a level commensurate with the force-on-force exercises conducted in the USA and other countries. Having guards and other security staff wear such devices facilitates the realtime sharing of information and the rapid and accurate issuing of instructions (see Fig. 9).

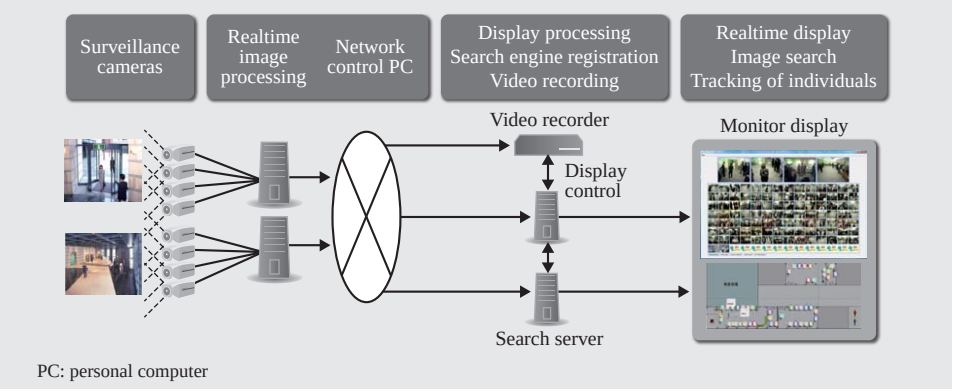
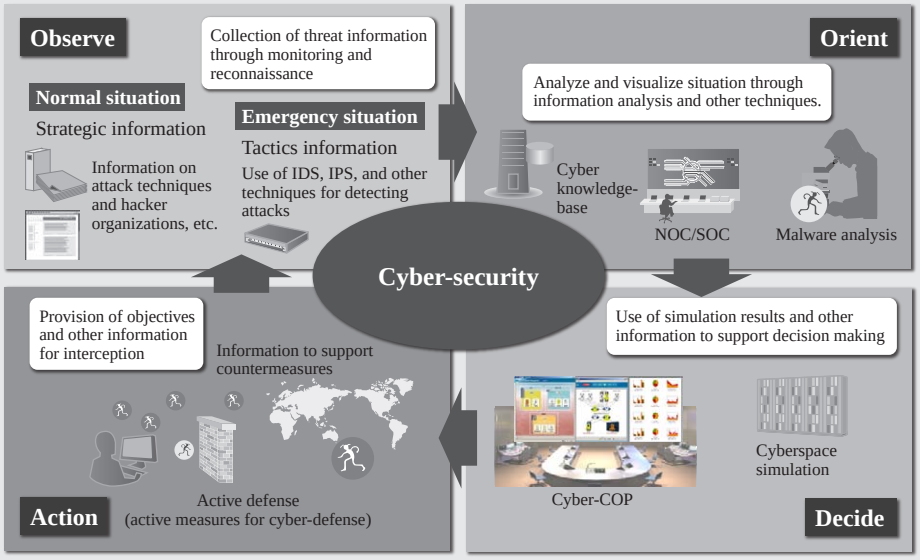
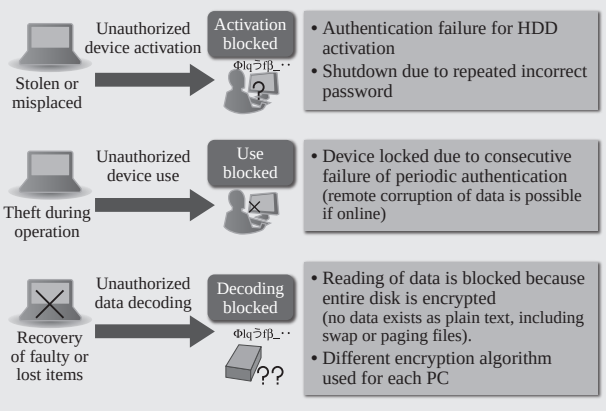


Fig. 6—Extensive Video Surveillance.
Automatic tracking is performed by identifying features or suspicious activity by people or objects from a large number of surveillance cameras.



IDS: intrusion detection system IPS: intrusion prevention system NOC: network operation center
SOC: security operation center

Fig. 7—Cyber-security.
Cyber-security guards against cyber-threats by establishing the cyber-security cycle of observe, orient, decide, and action.



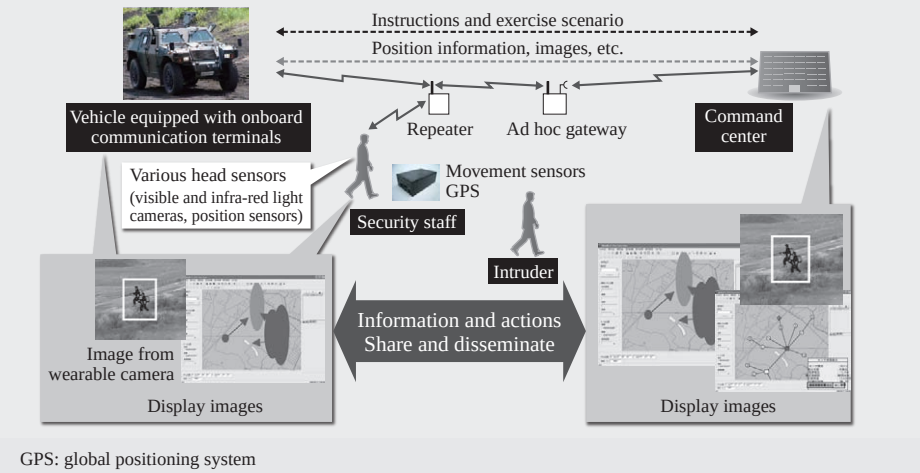
HDD: hard disk drive

Fig. 8—Use of Hard Disk Encryption.
Hard disk encryption is used to protect against theft and other threats.

CONCLUSIONS

This article has described how, with a view to compliance with Revision 5 of the IAEA Nuclear Security Recommendations, Hitachi aims to make further improvements in the future to the safety and security of nuclear power plants through new nuclear incident response functions that utilize know-how derived from its experience in the defense and security businesses, which has been applied to C2 and training exercise functions, and also technology for security systems.

Use of the C2 concept from defense systems is considered to be an effective way of conducting operations efficiently in the event of a severe accident. Conducting regular training exercises is also important, and their uses include demonstrating safety



GPS: global positioning system

Fig. 9—Information Sharing in FTX.
The use of personal equipment, such as wearable communications devices, sensors, and ad hoc communications, is an effective practice for the conduct of training exercises.

and security to the general public as well as preparing for an actual incident.

It is also likely that there will be situations during major disasters, such as the Great East Japan Earthquake, that require joint operations and the coordination of information in incident response and security systems. Possible examples of this include conducting investigations from the perspective of mutual back up of nuclear incident response and security systems in relation to requirements such as the need for redundancy in central alarm stations stipulated in Revision 5 of the IAEA Nuclear Security Recommendations.

In addition to the solutions described here, Hitachi also has a range of other technologies suitable for use in crisis management at nuclear power plants, including enterprise asset management that incorporates preventive maintenance and anomaly prediction and detection techniques that use data from plant sensors, wearable communication devices, and containerized data centers. Hitachi also supplies a wide range of other systems associated with nuclear power generation, including power reactors, reactor core control, electric power generation and transmission control, radiation management, and environmental monitoring systems, and believes itself capable of helping achieve further improvements to the safety and security of nuclear power plants.

REFERENCES

(1) IAEA, "49th IAEA General Conference (2005) Documents" (Sep. 2005).
(2) IAEA, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities," (Jan. 2011).
(3) N. Kimura, "Basics of Nuclear Security," Japan Electric Association, Newspaper Division (Mar. 2012) in Japanese.
(4) "Seoul Communiqué: 2012 Seoul Nuclear Security Summit," Ministry of Foreign Affairs of Japan (Mar. 2012).
(5) Advisory Committee on Nuclear Security, Japan Atomic Energy Commission, "Strengthening of Japan's Nuclear Security Measures" (Mar. 2012).
(6) United States Nuclear Regulatory Commission, "The NRC Incident Response Plan," NUREG-0728 (Rev. 4) (Apr. 2005).

ABOUT THE AUTHORS

Kazuhiko Tanimura
Joined Hitachi, Ltd. in 1981, and now works at the Intelligence and Information System Division, Defense Systems Company. He is currently engaged in system commercialization in the fields of command and control and crisis management.

Hiroyuki Kimura
Joined Hitachi, Ltd. in 2003, and now works at the Nuclear Plant Control and Instrumentation Engineering Department, Hitachi-GE Nuclear Energy, Ltd. He is currently engaged in the planning of instrumentation and control systems for nuclear power facilities.

Hisayuki Ito
Joined Hitachi, Ltd. in 2003, and now works at the Nuclear Power Control and Instrumentation Systems Engineering Department, Infrastructure Systems Company. He is currently engaged in information systems development for nuclear power facilities.