Featured Articles

Monitoring and Control Systems and Information Processing Systems to Support Safe Water Supply Operation

Hiroto Yokoi
Tadao Watanabe
Tatsuhiko Kagehiro, Ph.D.
Koji Kageyama, Ph.D.
Yukako Asano, Ph.D.
Hideyuki Tadokoro, P.E.Jp

OVERVIEW: An important part of the social infrastructure, water supply, is moving from an era characterized by expansion in scale to one based on maintenance and management, leading to growing expectations for the use of ICT to provide safe and rational management. While ICT development in the water industry has pursued objectives that include safe water quality and reliable water supply, advances in information infrastructure and the growing diversity of control network systems in recent years have also created an urgent need for measures to deal with the security risks associated with IT equipment. Taking note of the future spread of the IoT and changes in the structure of society, Hitachi is developing monitoring and control systems and information processing systems to overcome these challenges. This article describes diagnostic control techniques that contribute to the safety of equipment and water quality, and technologies for information system security and physical security.

INTRODUCTION

WATER supply is a vital part of the infrastructure of society, with coverage in Japan reaching 97.7% of the population as of the end of 2013[1]. In addition to strengthening the provision of safe water quality and reliable water supply, maintaining high-quality water services in the future will also require measures for dealing with things like demographic changes and advances in information infrastructure.

According to the National Institute of Population and Social Security Research, the population of Japan is already on the decline, with a forecasted fall from 127.24 million in 2013 to 86.74 million in 2060[2]. Looking to the long term, this means that there will be a need to rationalize operation and maintenance to cope with falling demand. Another concern is the difficulty of maintaining safe water quality during adverse circumstances, such as water quality incidents, if knowledge of how to maintain services is not passed on due to the diminishing number of skilled staff. Meanwhile, with the Tokyo 2020 Olympics estimated to attract around five million domestic and overseas visitors[3], along with controlling demand for water at particular times and places, ensuring the physical security of facilities also poses a challenge.

In terms of information infrastructure, there is scope for the rationalization of maintenance by taking advantage of the growing prevalence of the Internet of Things (IoT), for example, to utilize functions such as automatic meter reading, remote equipment diagnosis, and efficient control systems. On the other hand, this

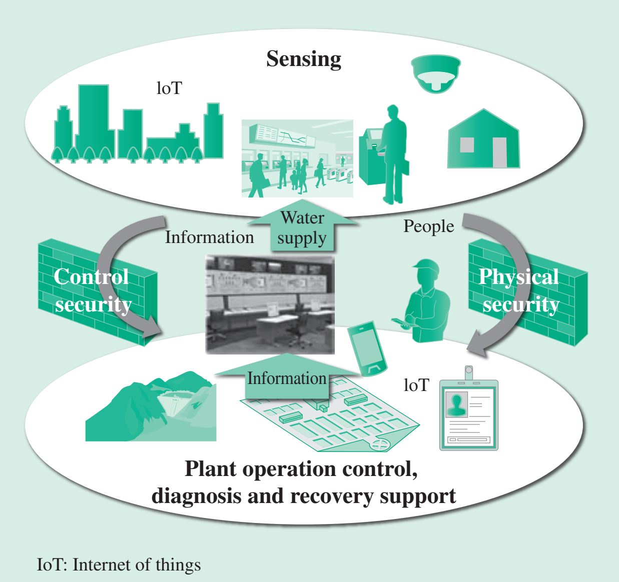


Fig. 1—Monitoring and Control Systems and Information Processing Systems to Support Safe Water Supply Operation.
Advances in information infrastructure are recognized as enabling the rationalization of water supply maintenance and management. In parallel with this is the growing importance of supporting security measures for data and people.

results in an increase in information security risks. Accordingly, the National Center of Incident Readiness and Strategy for Cybersecurity has listed water as one of the 13 key infrastructure sectors and is looking at what actions can be taken[4], also prompting the publication of the Information Security Guidelines for Water Industry[5] by the Ministry of Health, Labour and Welfare. Similarly, a report by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)[6] has noted a rapid rise over recent years in the frequency of cyber-attacks on water control systems in the USA, concluding that there is an urgent need for information and control security measures (see Fig. 1).

Given this background, Hitachi is working on the development of safer water supply systems, meaning systems that ensure the safety of everything from the water itself to plants and information. From among these, this article looks specifically at technologies for operation and control of water treatment, on-site multi-factor water quality measurement, support for fault prediction and recovery, control security, and physical security.

DIAGNOSIS AND CONTROL FOR SAFETY OF PLANT AND WATER QUALITY

Water quality incidents continue to occur with some frequency, including a large formaldehyde spill into the Tone river system that occurred in 2012. Working through the plan, do, check, act (PDCA) cycle to make continuous improvements is an effective way to ensure that the safety of the water supply is maintained at a high level. Examples of "planning" that form part of the routine operation of water treatment include planning for the safety of water and water quality testing. Operation control, equipment inspection and faultfinding in accordance with these plans are examples of "doing." "Checks" are conducted on the supplied water and remedial is action taken if necessary. Finally, "action" refers to the periodic review of these activities and the consequent updating of "plans." The following sections describe information and communication technologies (ICT) that facilitate the PDCA cycle.

Risk Assessment and Monitoring and Control of Treatment Plants

The primary purpose of water safety planning is to consider the potential risks that exist across the entire process and decide in advance on what actions to take when harm occurs. The New Water Supply Vision published by the Ministry of Health, Labour and Welfare identified taking account of natural weather events in risk management as an important factor for ensuring the safe supply of water, in consideration of the increasing frequency of events such as drought or heavy rain in recent years.

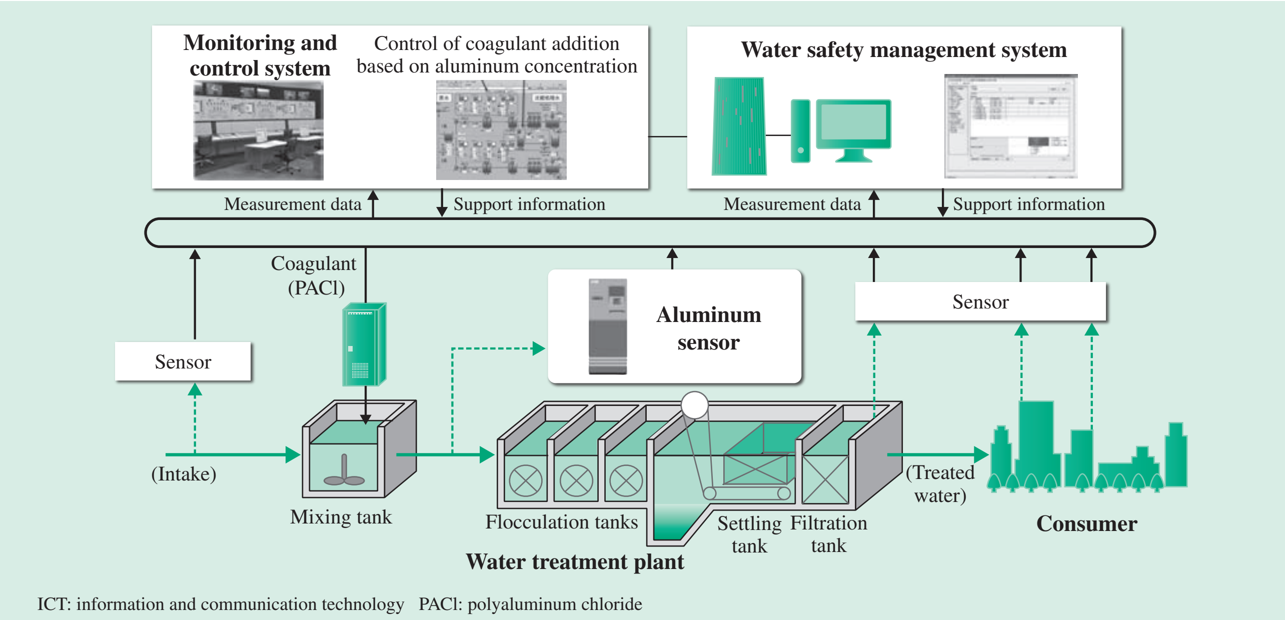


Fig. 2—Operational Support for Water Treatment Using ICT such as Monitoring and Control, etc.
Using ICT to measure the aluminum content of the water being treated and convert it into an indicator shortens the delay time for feedback control. The water safety management system supports risk assessment and response measures using monitoring information that includes water quality from initial intake to the consumer.

Hitachi supplies systems for planning (the "plan" of PDCA). These are intended to improve accountability and pass on know-how by using reaction models and pipe network models to provide quantitative criteria for whether or not to take actions.

Also, in the case of treatment plant operation (the "do" of PDCA), manual intervention based on the experience of skilled staff has an important role to play, especially during natural disasters when non-standard operation is called for. With the decreasing number of such experienced treatment plant staff, Hitachi supplies a control system that performs chemical dosing automatically in response to sudden changes in the quality of intake water (see Fig. 2).

A feature of this system is that it controls the dosing of coagulant based on the concentration of aluminum in the small flocs in which the flocculation process has not sufficiently advanced, measured immediately downstream of the mixing tank (flocculation is the process whereby the addition of a coagulant causes suspended solids to come out of suspension and form flakes called "flocs"). A trial performed using actual intake water demonstrated that the system can shorten the feedback time and minimize the deterioration in the quality of treated water when sudden fluctuations in water quality occur. Because aluminum coagulants such as polyaluminum chloride (PACl) and high basicity PACl account for more than 80% of coagulant use at water treatment plants in Japan, the system has potential for widespread use.

On-site Multi-factor Water Quality Measurement

Compact instruments for certain types of water quality measurement have appeared on the market in recent years, thereby enabling regular on-site measurement. Nevertheless, there are still a large number of measurements that require complex manual operations by specialist staff, or that require samples to be sent to specialist measurement agencies, meaning it is difficult to identify sudden changes in water quality for all types of measurement.

For these reasons, Hitachi has been working with Professor Miyake's group at the University of Tokyo, with support from the Core Research for Evolutional Science and Technology (CREST) program of the Japan Science and Technology Agency (JST), to develop a multi-factor water quality measurement system that can be used on-site to enable regular multi-point monitoring that is both automatic and realtime[7]. This water quality measurement system controls the flow of liquid through a micro-channel to enable measurement to be performed using minute amounts of sample and reagents (chemicals required for measurement), to obtain results rapidly, and to improve the repeatability of measurements.

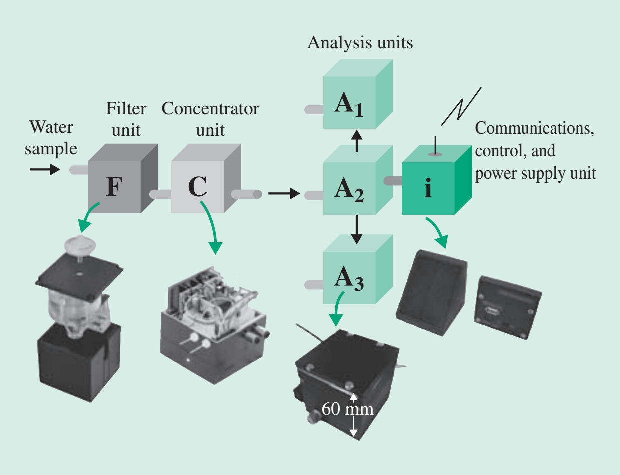


Fig. 3—On-site Multi-factor Water Quality Measurement[7].
The system components include a filter unit, a concentrator unit, analysis units for performing each measurement, and a communications, control, and power supply unit.

The system is made up of the various individual units required for measuring water quality. These include a filter unit for removing impurities from the water (when necessary); a concentrator unit for increasing the concentration of the water sample (when necessary); analysis units for performing each of the measurements; and a communications, control, and power supply unit that controls the other units and can transmit the measurement results (see Fig. 3). Units have been developed to test for residual chlorine and nitrate nitrogen, and to perform bacteria counts, with further units to be added. The standard size for each unit is 60 mm cubed.

The compact design of the measurement system makes it easy to install on-site. Furthermore, by speeding up and automating the measurement process, it can be used for realtime multi-point monitoring, making it possible to respond to sudden changes in water quality. In doing so, it makes it possible to provide a reliable supply of water that is safe and trustworthy.

Support for Fault Prediction and Recovery

Failures in water infrastructure equipment and machinery due to aging or other reasons can have severe consequences for the public and for industry. The challenge that must be overcome to prevent this is to predict faults before they happen and then respond before problems become serious.

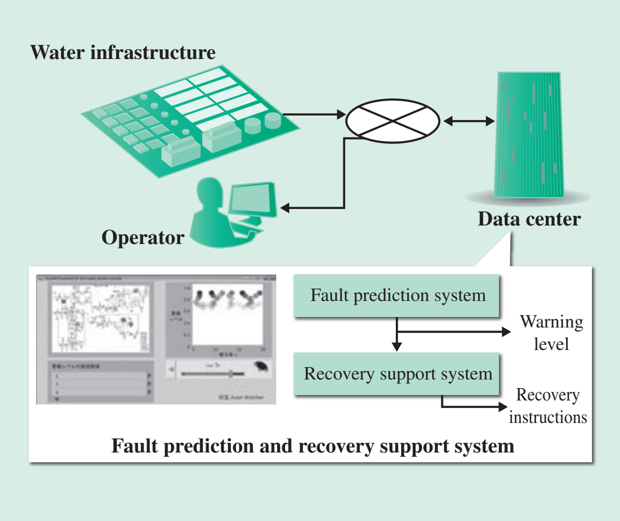


Fig. 4—Structure of Fault Prediction and Recovery Support System.
The system uses big data analytics to analyze plant operational data and predict faults, infer the underlying cause of predicted faults, and output instructions on how to recover.

In response, Hitachi is currently developing a fault prediction and recovery support technique (see Fig. 4) that is based on operational data from plants and equipment and that incorporates two specific techniques. The first of these involves statistical analysis using adaptive resonance theory (ART). A feature of this technique is that it can identify the warning signs of potential faults at an early stage by detecting small deviations from normal behavior based on the relationships between a large number of input variables.

The second is a semantic network technique that can infer the underlying cause of these warning signs from the plant flowchart and suggest ways of restoring normal operation. This means the operator can be quickly presented with instructions on what to do to prevent the fault from occurring.

Used together, these techniques can prevent plant and equipment failures. In addition to preventing the faults themselves, this also minimizes the detrimental effects on other equipment or on the operation of the overall system.

Hitachi has already applied these techniques to water treatment and seawater desalination plant data, and demonstrated their ability to predict things like damage to pump bearings or fouling of RO membranes. There is also scope for putting these broadly applicable techniques to use for other water industry equipment, such as enabling pre-emptive measures for dealing with abnormalities in sludge-based sewage treatment systems or problems with water quality.

HITACHI'S SECURITY TECHNOLOGIES

Advances in networking and other ICT have enabled the monitoring and control systems, namely, supervisory control and data acquisition (SCADA) or distributed control system (DCS), for water supply infrastructure to be put together in a variety of configurations, and have contributed to improvements in operational efficiency at water utilities. For example, monitoring and control systems that operated on a standalone basis in the past can now be linked together to provide centralized information and seamless operation and management across multiple facilities. The problem that comes with moving away from previous systems with closed networks, however, is the need to deal with the security risks resulting from this greater diversity and sophistication of system configurations.

Measures for the physical security of water supply facilities is also important given their role as critical infrastructure. Preventing access by unauthorized people and unwanted material requires consideration as to what is the best combination of physical security techniques to suit the nature of facility operations, including the movement of people and material during emergency situations as well as routine operation.

The following sections describe the work Hitachi is doing on control security, the security features of the monitoring and control system, and physical security technologies.

Hitachi's Work on Control Security

Taking note of the characteristics of infrastructure that remains in operation for long periods of time, and also of developments in the area of cyber-threats, Hitachi has adopted what it calls the "H-ARC concept," which identifies three specific security requirements for social infrastructure, namely that it be "adaptive," "responsive," and "cooperative"[8]. This H-ARC concept provides the basis for thinking about monitoring and control systems from implementation to operation.

Along with industry-specific standards for electric power, petrochemicals, and railways, work is proceeding on developing the IEC 62443 international standards covering all aspects of control security.

The IEC 62443-1-x series of standards deal with common concepts and terminology, the IEC 62443-2-x series with security policies and organizational management systems for organizations that own control systems, the IEC 62443-3-x series with technology requirements for system developers, and the IEC 62443-4-x series with control equipment security requirements for equipment manufacturers.

To ensure ongoing control system security, it is essential to work through the PDCA cycle to adapt to changes such as monitoring and control system configurations and the security requirements for each system. To achieve this, the Cyber Security Management System (CSMS) Conformity Assessment Scheme provides a framework that supports the PDCA cycle. CSMS certification is the control systems equivalent of the Information Security Management System (ISMS) specified for information systems in ISO/IEC 27001. The Japan Institute for Promotion of Digital Economy and Community (JIPDEC) published certification criteria based on IEC 62443-2-1 in April 2014[9] (see Fig. 5).

Hitachi has been a member of the Control System Security Center (CSSC) ever since it was first established in March 2012 as a public-private-academia partnership for strengthening the security of control systems that underpin social infrastructure, with involvement that includes research and development. Backing up this involvement, Hitachi has been developing in-house support structures that extend beyond incorporating security technologies into Hitachi's product range (the control system and control equipment covered by IEC 62443-3-x and IEC 62443-4-x) to also encompass assistance for control system owners such as water utilities to obtain CSMS certification. In the future, Hitachi intends to continue contributing to the provision of sustainable social infrastructure that can be used with confidence.

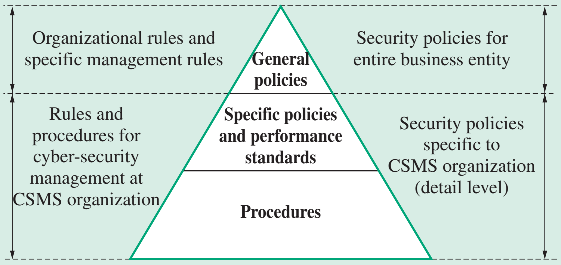
Security Features of Monitoring and Control System

Hitachi's monitoring and control system for water supply and sewage has been designed to incorporate an extensive range of security functions that take account of the increasingly diverse aspects of operational and management safety. The following section describes two such enhanced functions: a user management function and an anti-virus feature that works based on a whitelist.

User Management Function

The user management function assigns detailed permissions to each user of a monitoring and control system and controls their use. It consists of the following three function groups (see Fig. 6).

(1) The user authentication function prevents unauthorized access to the control system by using login ID and password to verify identity.

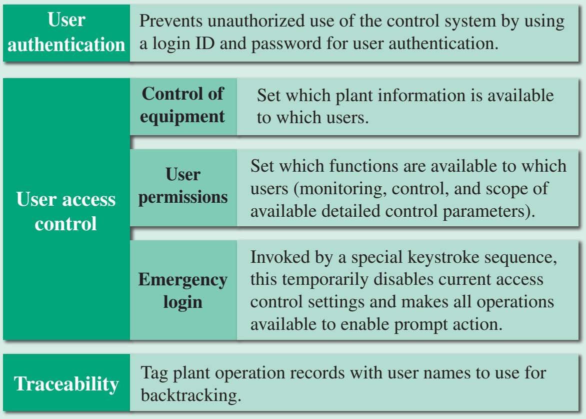

Organizational rules and specific management rules
General policies
Security policies for entire business entity
Rules and procedures for cyber-security management at CSMS organization
Specific policies and performance standards
Security policies specific to CSMS organization (detail level)
Procedures

Source: JIPDEC "CSMS Users' Guide"

JIPDEC: Japan Institute for Promotion of Digital Economy and Community
CSMS: Cyber Security Management System

Fig. 5—Overview of CSMS Certification.
The security policies of the individual organizations that operate control systems link in with the security policies and other information management rules of the higher level organizations. The formulated security policies must be approved by the relevant administrator.

(2) The user access control function can specify the scope of operations available to each user. It has predefined permissions set for each category of user within the operation and management team, including operation administrators, regular operators, and contract operators, and can be managed from within the monitoring and control system. Different access levels are assigned to different users, for example, a regular operator is only permitted to operate equipment and modify settings whereas an administrator is also able to modify control parameters. It also provides an emergency login function that is able to temporarily



User authentication		Prevents unauthorized use of the control system by using a login ID and password for user authentication.
User access control	Control of equipment	Set which plant information is available to which users.
	User permissions	Set which functions are available to which users (monitoring, control, and scope of available detailed control parameters).
	Emergency login	Invoked by a special keystroke sequence, this temporarily disables current access control settings and makes all operations available to enable prompt action.
Traceability		Tag plant operation records with user names to use for backtracking.

Fig. 6—Monitoring and Control System User Management Function.
To reduce security risks associated with control system operation and management, Hitachi's monitoring and control system includes security functions that are tied to user authentication.

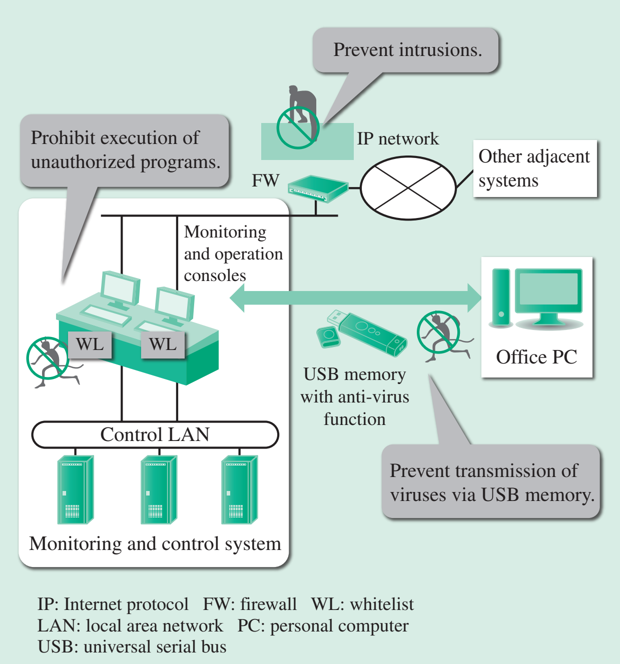

Prevent intrusions.
Prohibit execution of unauthorized programs.
IP network
FW
Other adjacent systems
Monitoring and operation consoles
WL
WL
Office PC
USB memory with anti-virus function
Control LAN
Prevent transmission of viruses via USB memory.
Monitoring and control system
IP: Internet protocol FW: firewall WL: whitelist
LAN: local area network PC: personal computer
USB: universal serial bus

Fig. 7—Security Features Provided by Monitoring and Control System.
The monitoring and control system provides security features to suit different aspects of operation and management.

disable access controls. This is invoked by a special keystroke sequence that disables access control to make it possible for every operation and management staff member to operate the system in case of disaster.

(3) The traceability function links user IDs and console data to a facility's operational records to enable backtracking to determine whether instructions issued to the plant were appropriate.

Whitelist Anti-virus Feature

There have been cases in recent times of monitoring and control systems being infected by computer viruses, a consequence of factors such as the use of universal serial bus (USB) memories to copy data from monitoring and control systems and the ease of interconnecting with other adjacent systems(10). Once an infection is present, it poses a problem for the operation and management of water facilities, and given the potential for unanticipated problems, it can take a long time to remove the virus and restore the system to normal operation. To deal with this risk, the monitoring and control system provides an anti-virus feature that works based on a whitelist. This works by restricting execution to only those programs designated on a whitelist in advance as permitted to run on the system, thereby preventing the execution of any intruding virus program that does not have permission.

The benefits of this approach compared to the blacklist method are that it consumes less central processing unit (CPU) time in the monitoring and control system and that it avoids the need for an Internet connection for updating virus definitions. It also helps prevent zero-day attacks and attacks from unknown viruses.

The monitoring and control system provides strong security features designed for use with operation and management. In addition to its whitelist anti-virus feature, these include compatibility with a firewall and USB memories equipped with security features (see Fig. 7).

Physical Security Technologies

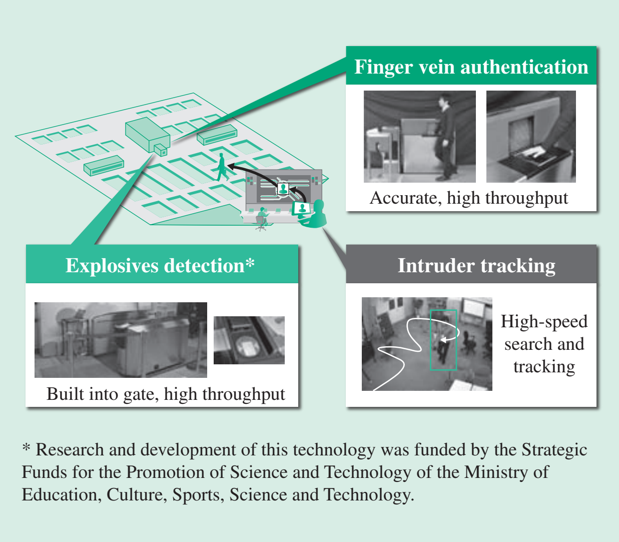
Because water treatment plants are a critical part of the social infrastructure and play an important public role, the impact on the public of a terrorist attack or similar incident would be large. To minimize damage by protecting facilities against vandalism or terrorist activity while still maintaining continuous 365-day operation, the following three measures are vitally important.

(1) Preventing intruders from entering facilities

(2) Preventing people from bringing in dangerous goods

(3) Identifying causes and minimizing damage if an incident does occur

The following sections describe technologies owned by Hitachi (see Fig. 8).


Finger vein authentication
Accurate, high throughput
Explosives detection*
Built into gate, high throughput
Intruder tracking
High-speed search and tracking

* Research and development of this technology was funded by the Strategic Funds for the Promotion of Science and Technology of the Ministry of Education, Culture, Sports, Science and Technology.

Fig. 8—Physical Security Technology for Social Infrastructure.
Hitachi is developing systems for responding to incidents when they happen as well as preventing intruders or people from bringing dangerous goods into its facilities.

The prevention of intruders (1) requires monitoring of facility surroundings and verifying identity at entrances and exits. While it is standard practice to use cards for premises access control, even tighter control can be achieved by using biometric information for personal identification. Examples of biometric information include fingerprints, irises, faces, voiceprints, genetic markers, and finger veins. Among these, finger vein patterns, in particular, do not change with age and are difficult to counterfeit due to being located inside the person's finger. Hitachi has commercialized personal authentication systems that use finger vein patterns and deployed them for premises access control systems. To improve convenience without compromising accuracy of identification, Hitachi has also prototyped touch panel and walk-through finger vein authentication systems. These provide strict control while also reducing staff workload by providing "unconscious authentication" (without the user being aware) and greater throughput.

To prevent people from bringing in dangerous goods (2), such as explosives or dangerous chemicals, it is necessary to conduct bag and body checks. The problem with this is that performing such checks manually on all operating staff is not practical due to the time it would take. It is possible, however, to detect dangerous goods with a walk-through system by fitting security gates with a dangerous goods detection system that has a built-in mass spectrometer. These systems blow air at workers that is then drawn in, concentrated, heated, and injected into the mass spectrometer. This can identify any material adhering to the worker by providing a mass spectrum of the microscopic particles collected from them.

To identify the cause and minimize damage if an incident does occur (3), it is necessary to collect image data, such as from surveillance cameras located around the periphery of the facility or images captured when people enter the site, and to search this huge repository of images for clues so that prompt action can be taken. To this end, a high-speed image search engine that can search for similar images in large amounts of image data is used to identify useful images from fragmentary data in a process called similar image search. This makes it possible to quickly discover unauthorized people or goods and enables action to be taken to minimize damage.

The safety of water treatment facilities can be further ensured by building integrated physical security systems that use these technologies in tandem.

CONCLUSIONS

This article has described monitoring and control systems and information processing systems that support the safe operation of water supplies. These have included technologies for information system security and physical security, and diagnostic and control techniques that contribute to equipment security and water quality while also allowing for the future spread of the IoT and changes in the structure of society. While these are primarily targeted at water and sewage systems, the technologies are also recognized as having growing potential for future use in tandem with other social infrastructure for purposes such as maintaining systems in good condition and providing operational support. Hitachi intends to continue contributing to society through the development of superior, original technology and products and by offering solutions.

REFERENCES

(1) Ministry of Health, Labour and Welfare, "Trends in Water Supply Coverage," http://www.mhlw.go.jp/file/06-Seisakujouhou-10900000-Kenkoukyoku/0000077465.pdf in Japanese.

(2) National Institute of Population and Social Security Research, "Population Projection for Japan," (Jan. 2012), http://www.ipss.go.jp/syoushika/tohkei/newest04/gh2401.asp in Japanese.

(3) Mizuho Research Institute Ltd., "Mizuho Report (Dec. 2014)," http://www.mizuho-ri.co.jp/publication/research/pdf/report/report14-1210.pdf in Japanese.

(4) National Center of Incident Readiness and Strategy for Cybersecurity, "Action to Date by Cabinet Secretariat for Protection of Important Infrastructure," http://www.nisc.go.jp/active/infra/torikumi_past.html in Japanese.

(5) Ministry of Health, Labour and Welfare, "Information Security Guidelines for Water Industry (Revised Version) (Mar. 2008)," http://www.mhlw.go.jp/topics/bukyoku/kenkou/suido/houkoku/dl/guideline.pdf in Japanese.

(6) Information-technology Promotion Agency, Japan, "2009-2011 ICS-CERT Incident Response Summary Report (Aug. 2012),"
http://www.ipa.go.jp/files/000025084.pdf in Japanese.

(7) R. Miyake, "Development of Technology for Implementing Model-based Water Cycle Smart Water Quality Monitoring Networks," "Research into Innovative Technology and System for Sustainable Water Use" Section, Proceedings of Third Symposium on "Strategy of CREST Water Use Project Aimed at Solving Changing Global Water Problems." (Jan. 2015) in Japanese.

(8) T. Nakano et al., "Control System Security for Social Infrastructure," Hitachi Review **63**, pp. 277–282 (Jul. 2014).

(9) Japan Institute for Promotion of Digital Economy and Community (JIPDEC), Information Management System Promotion Center, "Publishing of Documents Relating to Cyber Security Management System (CSMS) Auditing and Certification for Control Security," http://www.isms.jipdec.or.jp/csms/csmspublish.html in Japanese.

(10) JPCERT/CC, "Stuxnet – First malware to Target Control Systems – (Feb. 2011)," https://www.jpcert.or.jp/ics/2011/20110210-oguma.pdf in Japanese.

ABOUT THE AUTHORS

Hiroto Yokoi

Process Engineering Research Department, Center for Technology Innovation – Materials, Research & Development Group, Hitachi, Ltd. He is currently engaged in the research and development of water treatment and control technology for water supply and sewage. Mr. Yokoi is a member of The Society of Environmental Instrumentation Control and Automation (EICA).

Tadao Watanabe

Public Control Systems Engineering Department, Electrical Equipment Information & Control Systems Division, Omika Works, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in the development of monitoring and control systems for water supply and sewage.

Tatsuhiko Kagehiro, Ph.D.

Customer Co-creation Project, Global Center for Social Innovation – Tokyo, Research & Development Group, Hitachi, Ltd. He is currently engaged in the research and development of image processing and recognition. Dr. Kagehiro is a member of The Institute of Electronics, Information and Communication Engineers (IEICE), the Information Processing Society of Japan (IPSJ), and the Auditory and Visual Information Research Group (AVIRG).

Koji Kageyama, Ph.D.

Process Engineering Research Department, Center for Technology Innovation – Materials, Research & Development Group, Hitachi, Ltd. He is currently engaged in the research and development of water-related systems. Dr. Kageyama is a member of the EICA.

Yukako Asano, Ph.D.

Advanced Simulation Research Department, Center for Technology Innovation – Mechanical Engineering, Research & Development Group, Hitachi, Ltd. She is currently engaged in the development of micro-fluidics systems. Dr. Asano is a member of The Society of Chemical Engineers, Japan (SCEJ), the Society for Chemistry and Micro-Nano Systems (CHEMINAS), and the International Society for Pharmaceutical Engineering (ISPE).

Hideyuki Tadokoro, P.E.Jp

Public Control Systems Engineering Department, Electrical Equipment Information & Control Systems Division, Omika Works, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in the development of monitoring and control systems for water supply and sewage. Mr. Tadokoro is a member of The Institute of Electrical Engineers of Japan (IEEJ) and The Society of Instrument and Control Engineers (SICE).