Featured Articles I

Water and Sewage Industry Examples

Security Technology for Wide-area Monitoring and Control Systems

Tadao Watanabe
Kosuke Yamaguchi
Hideyuki Tadokoro, P.E.Jp
Takahiro Tachi

OVERVIEW: Water and sewage are important parts of the social infrastructure, and a variety of initiatives are being considered for overcoming the business challenges they face. One such challenge is the consolidation of their operations, with reports having been prepared in Japan that consider organizational consolidation from a variety of perspectives[1]*. When considering the opportunities for interconnecting existing systems that come with consolidation, cybersecurity measures are essential. With security threats becoming more diverse, the changing business environment represented by consolidation means that security measures need to be considered when connecting what were previously closed systems through reconstruction, etc. Hitachi is working on security measures for its monitoring and control systems, paying attention to security trends in the water and sewage industries.*

INTRODUCTION

FOLLOWING a period of rapid economic growth, the coverage of water and sewage infrastructure in Japan is at a historically high level, namely 97.7% for water (in FY2013)[2] and 77.6% for sewage (in FY2014, excluding Fukushima Prefecture)[3]. The future maintenance of water and sewage infrastructure is a major challenge for the industry. Moreover, operating conditions are expected to become increasingly difficult as the demographics associated with the aging population and low birth rate indicate falling demand for water in the future. With small and medium-sized organizations facing workforce shortages, many operators are struggling with how to inherit technical skills.

There has been considerable activity aimed at encouraging the consolidation of the scope of organizations, which is an effective way to sustain safe and secure water and sewage service. In the water industry, such initiatives were under consideration by 22 prefectural-level local governments as of December 2015, with the establishment of working groups included among the numerous amalgamation proposals[4]. In the sewage industry, the revised Sewerage Act enacted in May 2015[5] encouraged consolidation projects by freeing up the rules on the establishment of working groups for discussing ways to go about regional coordination between different sewage system operators.

In the field of monitoring and control systems, meanwhile, the consolidation of plant operations will be brought about through the interconnection of existing systems or the installation of new integrated systems. It has become possible to target the optimization of operations at a regional level in place of past practices, which were limited to optimizing the operation of individual plants. This means seeking to achieve system-wide optimization by reallocating water and electric power between organizations to maintain reliable operation and lower energy costs, and by using realtime control. The interconnection of existing monitoring and control systems opens up the prospect of not only optimal control that takes account of the entire system but also improved reliability by allowing central control rooms to provide backup for each other and the ability to manage operations with a smaller workforce through system integration.

Based on this background, this article considers the trends in cybersecurity at water and sewage system operators and describes the security technologies provided by Hitachi's monitoring and control system.

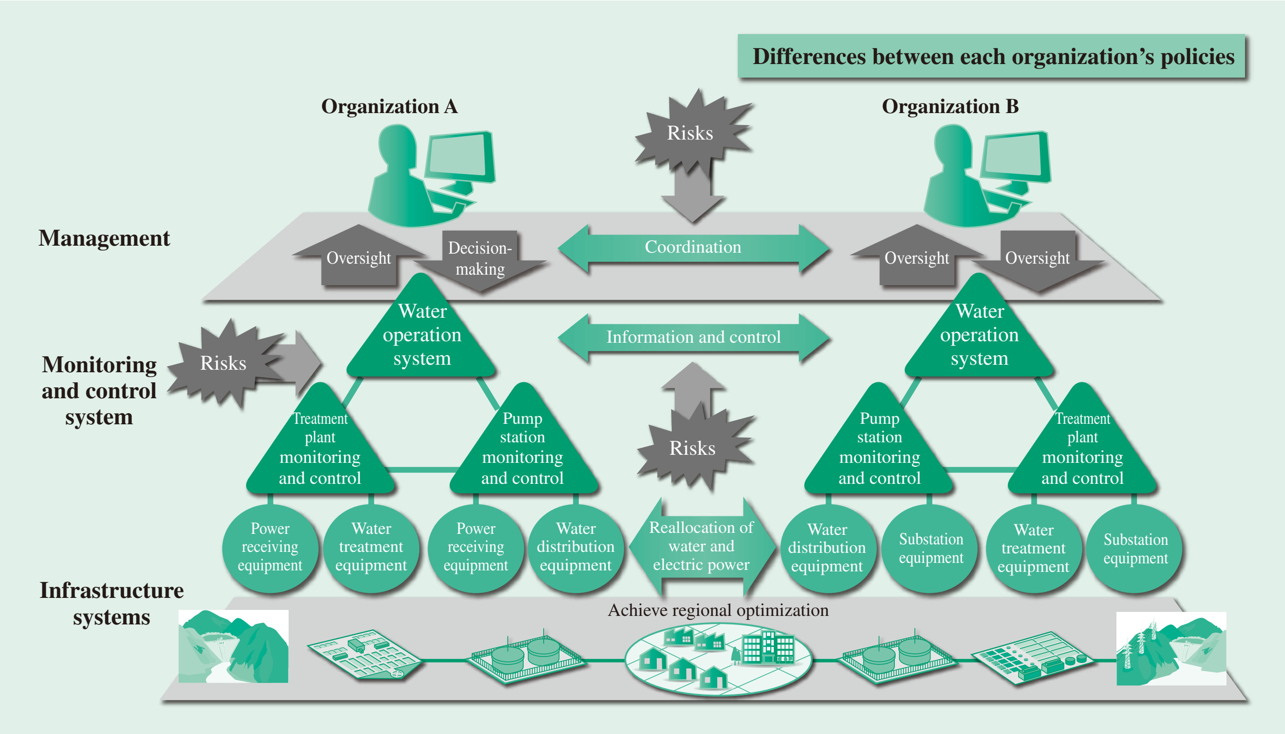

Differences between each organization's policies
Organization A
Risks
Organization B
Management
Oversight
Decision-making
Coordination
Oversight
Oversight
Water operation system
Information and control
Water operation system
Monitoring and control system
Risks
Treatment plant monitoring and control
Pump station monitoring and control
Risks
Pump station monitoring and control
Treatment plant monitoring and control
Power receiving equipment
Water treatment equipment
Power receiving equipment
Water distribution equipment
Reallocation of water and electric power
Water distribution equipment
Substation equipment
Water treatment equipment
Substation equipment
Infrastructure systems
Achieve regional optimization

Fig. 1—Security Risks Resulting from System Integration.
The interconnection of systems is essential to achieving optimal operation at a regional level. When different organizations are working together, it is essential to consider security measures on the assumption that the security policies of each organization will be different, including the risks posed by interconnection points.

SECURITY TRENDS

Status of Security in Water and Sewage Industry

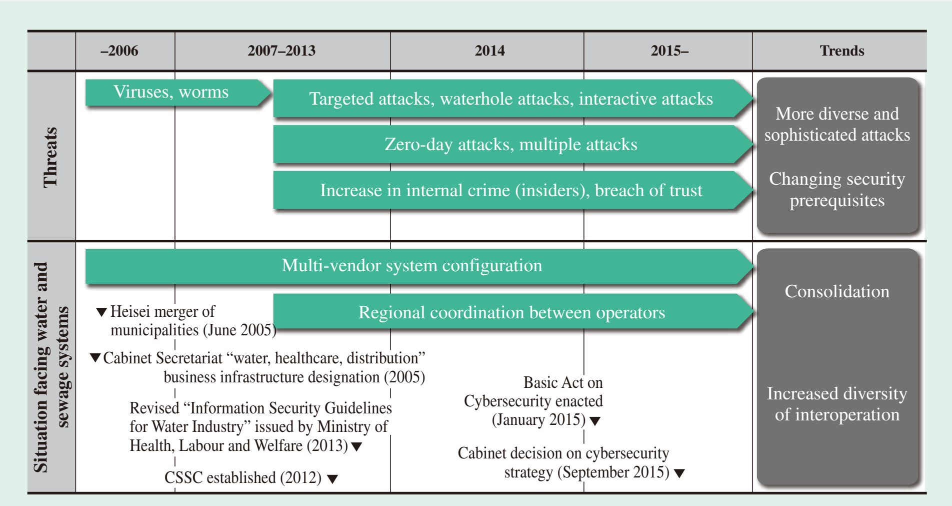
An issue raised by interconnection is security. In the case of interconnections between different organizations, risk assessments need to be based on the assumption that the respective security policies of each organization will be different. When a number of different monitoring and control systems are connected via a network, security measures are essential to deal with such risks as the infiltration and spreading of malware via interconnection points (see Fig. 1). It is also recognized that security measures are becoming more complex due to the increasing diversity of security threats and of the methods used to mount attacks (see Fig. 2). Accordingly, when considering security measures, it is important to make a theoretical determination of what type of measures to adopt together with their relative priorities based on a clear understanding of the risks in terms of frequency of incidents and their effects on plant operation.

In October 2015, an experts' committee at The Institute of Electrical Engineers of Japan, Investigating R&D Committee on Survey on the Current Situation and Issues of Security Practices for Water Facilities in Japan, looking at the status and challenges associated with security technology at water and sewage facilities undertook a questionnaire-based survey of security at water and sewage system operators[(6)]. The survey considered the changes that occurred since the previous survey conducted in 2007. What it found was a small increase in opportunities for interconnection between systems due to changes in the business environment. It also found that there had been no change in how secure systems were, with isolation from external networks being the primary mechanism. However, there is potential for these past assumptions to be overturned as the consolidation of water and sewage systems progresses in the future. It seems likely that demands for security measures will accompany consolidation.

Guidelines for Operation

To date, the issuing of guidelines on security measures that indicate their necessity and importance has been driven by the government.

The Ministry of Health, Labour and Welfare issued "Information Security Guidelines for Water Industry," in October 2006. This document contained basic


–2006
2007–2013
2014
2015–
Trends
Threats
Viruses, worms
Targeted attacks, waterhole attacks, interactive attacks
Zero-day attacks, multiple attacks
Increase in internal crime (insiders), breach of trust
More diverse and sophisticated attacks
Changing security prerequisites
Situation facing water and sewage systems
Multi-vendor system configuration
Heisei merger of municipalities (June 2005)
Regional coordination between operators
Cabinet Secretariat "water, healthcare, distribution" business infrastructure designation (2005)
Revised "Information Security Guidelines for Water Industry" issued by Ministry of Health, Labour and Welfare (2013)
CSSC established (2012)
Basic Act on Cybersecurity enacted (January 2015)
Cabinet decision on cybersecurity strategy (September 2015)
Consolidation
Increased diversity of interoperation

CSSC: Control System Security Center

Fig. 2—Security Trends.
As threats become more diverse and sophisticated, the prerequisites for security measures are changing. Security measures are becoming an issue for water and sewage systems due to their consolidation and interoperation of different systems.

instructions that included measures for preventing interruptions to the water supply, which is an important part of the infrastructure. These guidelines were revised in March 2008, and a third edition was published in June 2013 with updates on how to deal with new threats, such as targeted attacks, and changes in how telecommunications technology is used, such as smart devices[7].

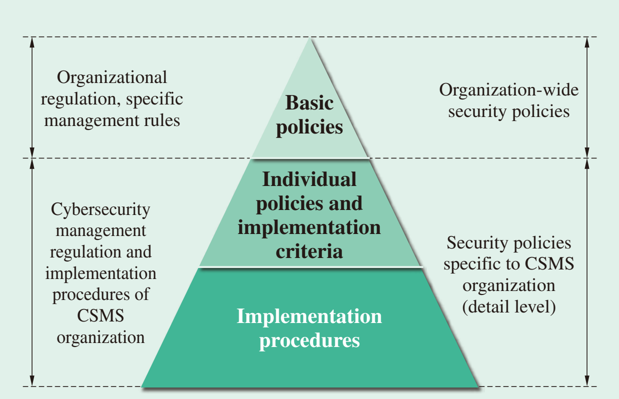
The Basic Act on Cybersecurity enacted in January 2015 called for autonomy on the formulation of criteria for security measures and the staging of drills and exercises by operators of critical infrastructure, including water. Similarly, a cabinet decision on cybersecurity strategy[8] issued based on the new law in September 2015 called for the government, operators of critical infrastructure, and relevant companies to work together voluntarily in giving consideration to national crisis management and security in order to take action on increasingly sophisticated cyber-attacks.

Internationally, meanwhile, following on from industry-specific standards for electric power, petrochemicals, and railways, progress is being made on formulating the International Electrotechnical Commission (IEC) 62443 standard covering all aspects of control systems.

The IEC 62443-1-x series of standards deals with common concepts and terminology. The IEC 62443-2-x series deals with security policies and organizational management systems for the owners of control systems. The IEC 62443-3-x series deals with the technical requirements for control systems for those who implement the systems. The IEC 62443-4-x series is for equipment manufacturers and deals with security requirements for control equipment.

The plan, do, check, act (PDCA) cycle for dealing with system security requirements and changes to the structure of monitoring and control systems is essential for maintaining the security of control systems. Cyber security management system (CSMS) certification provides a framework for this use of PDCA. CSMS certification is the control system equivalent of an information security management system (ISMS) as defined in ISO/IEC 27001 for information systems, and was announced in April 2014 by JIPDEC as a set of certification criteria based on IEC 62443-2-1[9] (see Fig. 3).

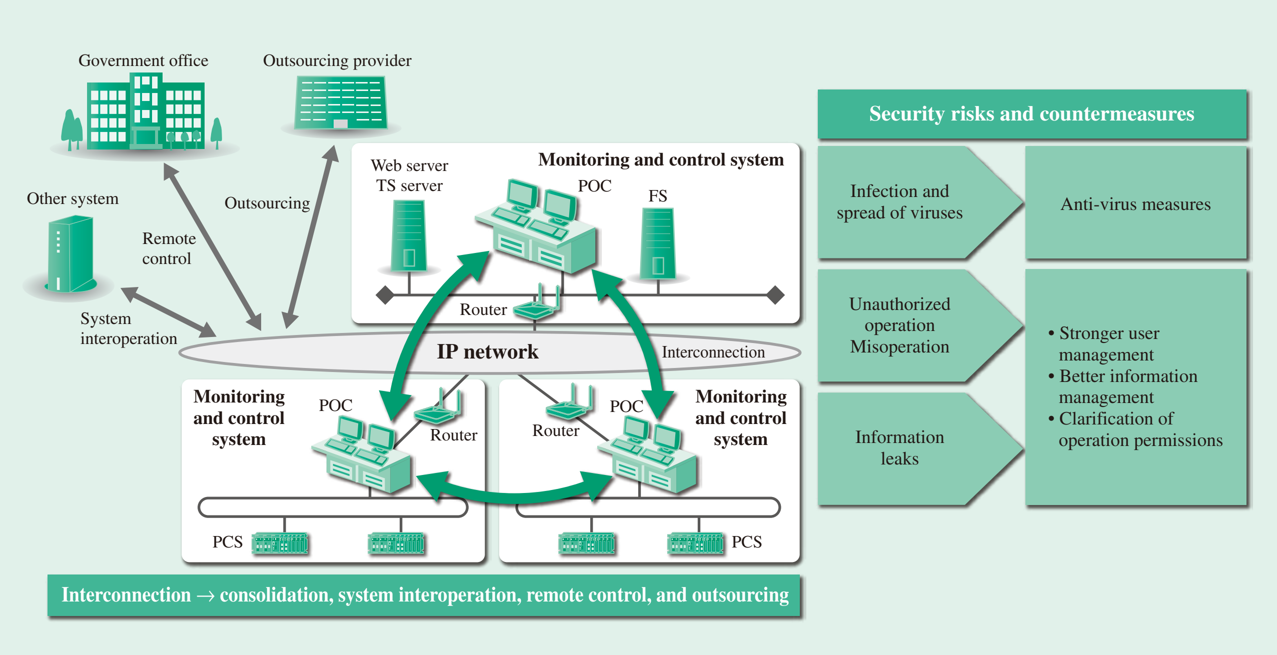
It is anticipated that water and sewage system operators will be expected in the future to manage security in accordance with CSMS.


Organizational regulation, specific management rules
Basic policies
Organization-wide security policies
Cybersecurity management regulation and implementation procedures of CSMS organization
Individual policies and implementation criteria
Implementation procedures
Security policies specific to CSMS organization (detail level)

Source: JIPDEC CSMS user guidelines

CSMS: cyber security management system

Fig. 3—Organizational Overview of CSMS Certification.
The security policies of organizations that operate control systems are linked to the security policies and information management rules of their parent organization. The formulated security policies must be approved by the relevant manager.


Government office
Outsourcing provider
Other system
Outsourcing
Remote control
System interoperation
Web server
TS server
Monitoring and control system
POC
FS
Router
IP network
Interconnection
Monitoring and control system
POC
Router
Router
POC
Monitoring and control system
PCS
PCS
Interconnection → consolidation, system interoperation, remote control, and outsourcing
Security risks and countermeasures
Infection and spread of viruses
Anti-virus measures
Unauthorized operation Misoperation
Information leaks
• Stronger user management
• Better information management
• Clarification of operation permissions

PCS: process control station POC: process operator's console TS: terminal service IP: Internet protocol FS: file server

Fig. 4—Interoperation of Monitoring and Control Systems and Security Risks.
Advances in IP networking can help with consolidation by enabling the interconnection of monitoring and control systems. However, this means there is a need for ways of dealing with the security risks that come with interconnection.

SECURITY MEASURES IN MONITORING AND CONTROL SYSTEMS

The interconnection of monitoring and control systems both encourages the integration of monitoring to enable operation with a small number of staff and makes it possible to use outsourcing to achieve rapid fault response and to deal with shortages of technical staff. The possibilities include further efficiencies through interoperation with the systems of adjacent system operators, and skills transfers achieved through the accumulation of know-how and its wider deployment. It also offers a way to create new value by sharing information with other industries and systems.

Given this background, Hitachi's monitoring and control system provides wide-area monitoring and control based on a new domain-based concept that encourages the use of distributed servers connected to a closed Internet protocol (IP) network spanning multiple sites that can be used for cross-system monitoring[(10)]. Web, terminal service (TS), and other servers can also be installed to provide monitoring and control over a more open IP network.

Anti-virus measures	Whitelist	Prevents execution of viruses that have gained unauthorized access to the system by prohibiting execution of other than a predefined list of programs	
Prevent unauthorized operation or misoperation	User management	User authentication	Excludes unauthorized users by login/password authentication of users and an automatic logoff function
		Emergency login	Provides a temporary login for equipment operation in times of emergency by pressing a special key combination
	Information management (traceability)	Operation logs	The user name and the device used to perform each operation is recorded in plant operation logs, which can be viewed using a search function.
		Portable media	A record is kept of removal to external media or printing of data, which can be viewed using a search function.
	Execution control based on user accounts	Operation permissions	The scope of equipment jurisdiction is specified for each user. Equipment can be designed as required with input and output signals to suit plant operation.
		Equipment jurisdiction	Each operational function is assigned a level (routine operation, control parameter modification) based on user permissions.

Fig. 5—Security Functions of Hitachi's monitoring and control system.
To provide reliable system operation and an environment for safe equipment operation, the monitoring and control system is equipped with anti-virus, user authentication, and user operation permission features to protect system assets and functions against security risks.

Whereas past monitoring and control systems were based on a closed architecture, the interconnections associated with system enhancements bring a variety of security risks (see Fig. 4). Hitachi's monitoring and control system, described below, has ways of dealing with these security risks (see Fig. 5).

Whitelist-based Anti-virus Measures

When monitoring and control systems are connected to other systems, there is the risk that a virus infection on one machine could quickly spread to the other connected machines.

Hitachi's monitoring and control system uses whitelist-based anti-virus measures to prevent the infection and spread of viruses. This prevents infection by an unknown virus because it only permits the execution of a predefined list of programs. Because whitelisting does not require an Internet connection to get virus definition updates (unlike blacklisting), it is suitable for use on closed systems and has the advantage of not compromising system stability or responsiveness by having to run routine scans.

On the other hand, whitelisting has no way of eliminating pre-existing viruses. Accordingly, the monitoring and control system uses it in conjunction with virus scanning using a blacklist that is updated by portable universal serial bus (USB) memory to provide dependable measures for preventing the infection and spread of viruses.

User Management and Traceability

The growing use of remote control and outsourcing means that the physical security of the locations from which monitoring and operation are performed may no longer be adequate, creating a requirement for user and information management in response to the risk of unauthorized people operating the systems or stealing data.

User management involves the use of an identity (ID) and password for authentication when accessing the system to prevent login by other than authorized users. To prevent intrusion by an unauthorized person when a user forgets to log off, the monitoring and control system also has a function to automatically log users off if they do not perform any action for a predetermined length of time. Together with improved password management criteria, the system also includes password management functions for specifying how long passwords remain valid and for disabling users who enter an incorrect password more than the permitted number of times.

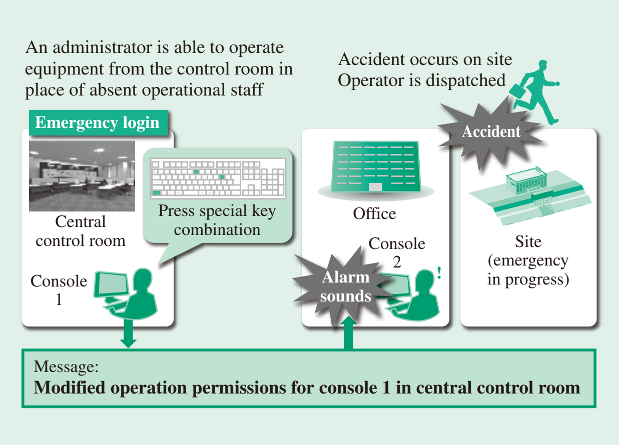

An administrator is able to operate equipment from the control room in place of absent operational staff
Accident occurs on site Operator is dispatched
Emergency login
Accident
Central control room
Press special key combination
Office
Console 2
Site (emergency in progress)
Console 1
Alarm sounds
!
Message:
Modified operation permissions for console 1 in central control room

Fig. 6—Emergency Login.
An emergency login function that provides temporary access to equipment operation is provided to deal with the situation when operational staff with operation permissions are absent during an accident or natural disaster.

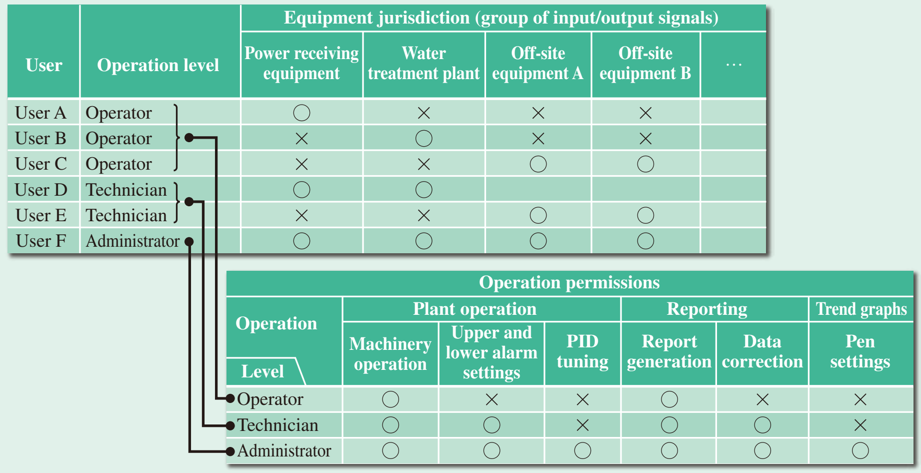
Another function is provided for the case when operational staff are not present in the central control room to deal with on-site response and other matters when a major accident or disaster occurs, and permitting emergency login by administrators who are able to handle control room operations on their behalf. It provides a temporary login that permits the sorts of equipment operation required in an emergency, enabled by pressing a predefined key combination on the keyboard. An alarm tone sounds continuously during an emergency login to make it clear that emergency operation is in progress (see Fig. 6).

Information management includes a function for appending the user name and the device the user is using to operation logs in order to enable any unauthorized or mistaken operations to be identified afterward. Records are also kept of the removal or printing of system data to ensure that the identity of anyone who removes data can be determined along with the time and the device they used.

Use of User Accounts for Execution Control

Because interconnected monitoring and control systems are used by operational staff at different sites, as shown in Fig. 4, there is a risk of misoperation of equipment outside a user's jurisdiction.

The use of user accounts for execution control makes it possible to combine operation permissions, which specify the level of operations the logged in user is allowed to perform, with an equipment jurisdiction that specifies the range of equipment the user is allowed to operate (see Fig. 7).



User	Operation level	Equipment jurisdiction (group of input/output signals)				
		Power receiving equipment	Water treatment plant	Off-site equipment A	Off-site equipment B	…
User A	Operator	○	×	×	×	
User B	Operator	×	○	×	×	
User C	Operator	×	×	○	○	
User D	Technician	○	○			
User E	Technician	×	×	○	○	
User F	Administrator	○	○	○	○	

Operation / Level	Operation permissions					
	Plant operation			Reporting		Trend graphs
	Machinery operation	Upper and lower alarm settings	PID tuning	Report generation	Data correction	Pen settings
Operator	○	×	×	○	×	×
Technician	○	○	×	○	○	×
Administrator	○	○	○	○	○	○

PID: proportional – integral – differential

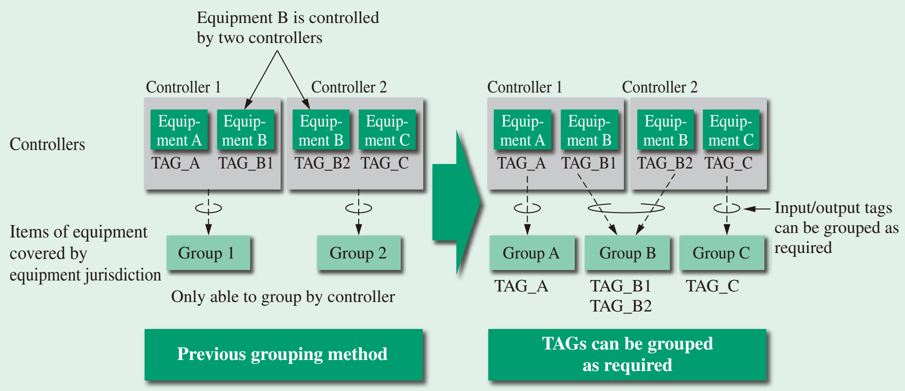
Fig. 7—Level Settings for Operation Permissions.
The system allows equipment jurisdiction and operation permissions to be specified for individual users.

Operation permissions work by predefining the level of operations permitted to operators, technicians, administrators, and other staff, and then assigning each type of user to one of these levels. It is possible, for example, to configure the system such that operators are only permitted to operate equipment, technicians are permitted also to change upper and lower limit alarm settings, and administrators are permitted to perform all of these operations as well as to modify control parameters. The function can be used to assign different operation levels to ordinary and expert operators. Permissions can also be assigned at the level of individual users, such as whether they are permitted to correct report data or specify pen settings for trend graphs.

The equipment jurisdiction function prevents incorrect equipment operation. It works by grouping input and output signals and can be used to specify in detail the scope of monitoring and operation permitted to each operator. The way input and output signals were grouped in the past only allowed grouping to be specified at the level of individual controllers, making it difficult to use in cases when the same controller was used for different equipment or the same equipment was handled by multiple controllers. Because the new method allows all input and output signals handled by the system to be grouped independently, it allows fine-grained control of the scope of monitoring and operation permitted to operators (see Fig. 8).

CONCLUSIONS

This article has described the need for cybersecurity measures in response to the trend toward consolidation of operations, and the security technologies provided by Hitachi's monitoring and control system to meet this need.



TAG: input/output signal tag

Fig. 8—Grouping of Input/Output Signals.
Input and output signals can be grouped as required to provide fine-grained control of the scope of monitoring and operation permitted to an operator.

Hitachi believes that appropriate security measures will improve the convenience of interconnection and lead to the ongoing development of safe and secure water and sewage infrastructure. Hitachi intends to continue developing products with superior security technology and supplying solutions.

REFERENCES

(1) Local Public Enterprise Management Office, Local Public Finance Bureau, Ministry of Internal Affairs and Communications, “Implementation Case Studies of Consolidation Efforts, etc. by Water Utilities,” http://www.soumu.go.jp/main_content/000382947.pdf in Japanese.

(2) Ministry of Health, Labour and Welfare, “Trends in Water Supply Coverage,” http://www.mhlw.go.jp/file/06-Seisakujouhou-10900000-Kenkoukyoku/0000122560.pdf in Japanese.

(3) Ministry of Land, Infrastructure, Transport and Tourism, “Sewage Treatment Utilization Rate,” http://www.mlit.go.jp/common/001103039.pdf in Japanese.

(4) Ministry of Health, Labour and Welfare, “The Need for Water Supply Consolidation, December 2015 Water Supply Division Investigation,” http://www.mhlw.go.jp/file/05-Shingikai-10901000-Kenkoukyoku-Soumuka/0000112382.pdf in Japanese.

(5) Sewerage Act, http://law.e-gov.go.jp/htmldata/S33/S33HO079.html in Japanese.

(6) Investigating R&D Committee on Survey on the Current Situation and Issues of Security Practices for Water Facilities in Japan, “Security Management System for Water Facility: A Survey on the Current Situation of Security Practices for Water Facilities in Japan,” IEEJ Technical Reports No. 1362 (Oct. 2015) in Japanese.

(7) Ministry of Health, Labour and Welfare, “Information Security Guidelines for Water Industry (the third version)” (Jun. 2013), http://www.mhlw.go.jp/file/06-Seisakujouhou-10900000-Kenkoukyoku/0000046638.pdf in Japanese.

(8) Cabinet Decision, “Cybersecurity Strategy,” (Sep. 2015), http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

(9) JIPDEC, “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) T. Watanabe et al., “Information and Control Systems to Support Planning, Operation, and Maintenance Activities for Sustainability of Water Supply and Sewage Facilities,” Hitachi Review **63**, pp. 500–507 (Sep. 2014).

ABOUT THE AUTHORS

Tadao Watanabe

Public Control Systems Engineering Department, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of monitoring and control systems for water supply and sewage.

Kosuke Yamaguchi

Public Control Systems Engineering Department, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of monitoring and control systems for water supply and sewage.

Hideyuki Tadokoro, P.E.Jp

Public Control Systems Engineering Department, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the research and development management of water supply and sewerage operation and control systems. Mr. Tadokoro is a member of The Institute of Electrical Engineers of Japan (IEEJ), the Society of Instrument and Control Engineers (SICE), and The Society of Environmental Instrumentation Control and Automation (EICA).

Takahiro Tachi

Water Solutions Division, Water Business Unit, Hitachi, Ltd. He is currently engaged in general management of research and development on water environments. Mr. Tachi is an expert member of the International Organization for Standardization (ISO) Technical Committee 224, Working Groups 7 & 9, and a member of EICA, and the Catalysis Society of Japan (CATSJ).