HITACHI Security Concept for Industrial Control Systems

Hiromichi ENDOH[1], Tsutomu YAMADA[1], Satoshi OKUBO[2] and Toshihiko NAKANO[2]
[1] Hitachi Research Laboratory, Hitachi, Ltd.
7-1-1 Omika-cho, Hitachi-shi, 319-1292, Japan
(hiromichi.endo.be@hitachi.com, tsutomu.yamada.bs@hitachi.com)
[2] Information and Control Systems Company, Hitachi, Ltd.
5-2-1 Omika-cho, Hitachi-shi, 319-1293, Japan
(satoshi.okubo.sz@hitachi.com, toshihiko.nakano.yy@hitachi.com)

Abstract

Security is a necessary factor for the safe and efficient operation of today's control systems. To ensure safe operation of control systems throughout their lifetime, security measures must be carefully planned in the development phase and then maintained continuously during the operation phase and other following phases. To ensure operation within the system's safe states, Hitachi proposes security concept processes (1) to derive security measures rationally and (2) to maintain the security model over the system life cycle. Hitachi also proposes security development programs which support the integration of standards-compliant systems and development of robust control equipment.

1. Introduction

Control systems have an important role in the automatic management of critical infrastructure plants including power plants and electricity grid systems as well as industrial plants. To achieve better service quality and more energy-efficient system operation, more and more functionality and flexibility are being required of control systems through the incorporation of such capabilities as data exchange between enterprise systems over networks and the use of personal-computer-based software components.

Unfortunately, these changes have also introduced potential security risks into control systems such as the malicious takeover of system control. For example, "Stuxnet" malware[1], which was first identified in mid-2010, was capable of falsifying control sequences programmed into some programmable logic controllers (PLCs) to cause erroneous system behaviour [1]. If control systems operating and monitoring public infrastructure plants are taken over or damaged by such attacks, significant impact may be caused to the community. The potential consequences of such security breaches are the reason why cyber-security has become one of the most important concerns in designing, developing and operating control systems.

To provide some guidance for defending control systems from cyber-threats, many industrial security standards and guideline documents have been published such as the NERC CIP [2], the NIST SP 800 Series [3][4], and the CPNI Good Practice Guide [5]. The IEC 62443 international standard [6] has been partially published with the rest still under development. These documents

[1] A generic term for the malicious software such as viruses, worms and spywares.

will provide some criteria on choosing security measures for establishing secure control system architectures; however, they may not provide a direct answer for each system: appropriate security measures may vary depending on the system environment and the specific operational requirements.

In Section 2 of this paper, some issues in providing security measures for control systems are discussed. In Section 3, a security concept to assure safe operation is proposed for addressing these issues. In Section 4, some examples of using the Hitachi security concept are provided.

2. Considerations for Control System Security

Since control systems are tightly coupled with real world equipment, some more issues which are not essential in the scope of information systems should be considered the prerequisites of security functionalities: they are mainly about the variety of the system components, long system lifetime, and awareness of system safety and integrity. The major issues are as follows.

1) Total system security

A control system is comprised of different types of equipment such as programmable controllers, interface consoles and IT components. Since potential adversaries will always seek out the weakest point in a system, security measures must be organized to cover all elements of the system. To choose appropriate security measures, thorough risk assessment must be carried out with assumptions of a wide variety of threats including erroneous operations and general disasters. In order to make such security measures effective, it is also necessary to establish appropriate procedures and training programs for plant operation personnel and other staffs.

2) Security actions and system safety

The main objective of control system security is to maintain the safety of plants, personnel and the environment; therefore, when discussing security for control systems, security actions must be considered carefully on this basis. Malicious behaviour caused by unauthorized access may damage the plant therefore it must be blocked. On the other hand, shutting down all or part of the system damaged by virus infection, Denial of Service (DoS) attacks or some other security incident is not always the safe choice. For example, careless shutdown and restart of a power plant is often harmful to the overall system or plant.

3) Continuous security support throughout the life cycle

Typical lifetime of control systems for public infrastructure plants spans over 20 years from deployment to replacement or disposal. System expansion and partial replacement may also occur after the system has started operation. Therefore, security measures must also be provided and maintained in the phases other than design, development and integration so that the system will not be unnecessarily exposed to threats.

4) Harmonization with availability and performance

Availability and performance are necessary characteristics for control systems to maintain their service integrity and efficiency. These factors should not be degraded beyond the allowable lower limit by security measures. Such a lower limit must be defined in the customer's requirements.

3. Security Concept for HITACHI Control Systems

To provide total security which assures safe operation of control systems through the equipment lifetime, appropriate security measures must be taken during each development phase. Hitachi proposes the "2-Aspects and 3-Dimensions" security assurance model for addressing this requirement when developing control systems. "2-Aspects" means that security must be assured in two aspects: rationally deriving security measures during system development and managing the security measures after system deployment. "3-Dimensions" means that all three types of system elements (equipment, information and personnel) must be protected by corresponding types of security measures: physical, cyber and operational.

This concept consists of three parts following:

1. Safe system state model: A model to specify all system states in which a plant can be kept in safe conditions as well as all security actions to be taken by the system to stay within the current safe state or to transfer to another safe state in response to system events. This model is a key part of the Hitachi security concept in which all security measures must be consistent with the safe conditions and the security actions defined.

2. Security derivation process: A process to derive appropriate security measures rationally from security requirements during system development. Security requirements are broken down step by step and finally security measures are assigned onto the three dimensions noted above.

3. Security management process: A process to maintain the efficacy of the safe system state model by continual risk assessment and improvement of security measures against any newly discovered threats such as malwares and system vulnerabilities.

These three parts of the Hitachi security concept are explained in the following sub-sections.

3.1 Safe System State Model

A control system must manage itself so that the plant is kept in safe conditions and its service integrity is maintained. As noted above, simply shutting down equipment is not always the safe choice; therefore, all safe states as well as safe state to safe state transitions must be defined for each system, and the overall mandate is to stay within one of these states during operation.

Figure 1 shows the abstracted safe system state model. Some safe states are defined in this model, each corresponding to the operation level of the system. In the "In-Service" state, the system can provide enough functionality to control the plant, including the "Normal Operation" state in which the system can operate with full functionality. Another state is the “Secured” state, in which the system is partially shut down or its functionality is limited to prevent further damage. The “In-Service” state and the “Secured” state can be grouped as the “Safety-Controlled” state in which the system must stay during its entire operational lifetime.

Security actions to be taken by the system in each state are also defined in this model. The system needs to take these actions to stay within the current safe state or to transfer to another safe state in response to security incidents.

The detail of these safe states and security actions must be defined for each system because actual safe conditions are different for each target plant.

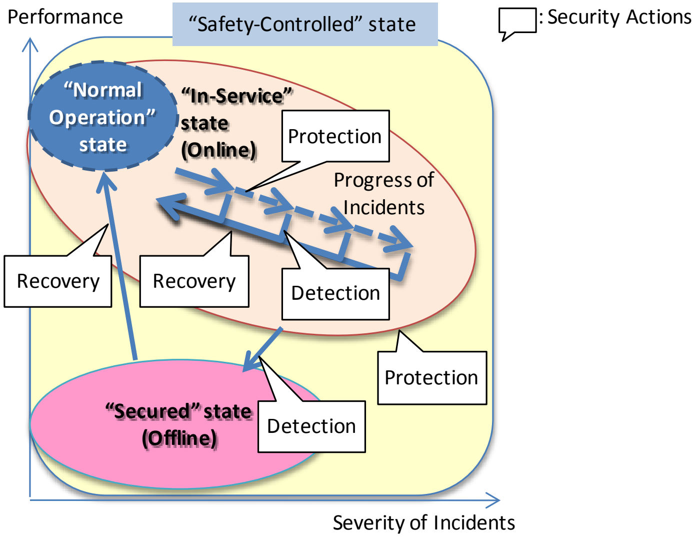

Figure 1 Safe System State Model

3.2 Security Derivation Process

In the system development phase, appropriate security measures must be chosen to ensure adequate coverage against assumed threats. The security derivation process ensures that all security measures are derived from security requirements for the target control system. **Figure 2** shows an overview of the process.

Security requirements must be clarified ahead of time and must be considered from both the business side and the plant side, including safe states and RAS (Reliability, Availability, and Serviceability). Once security policies are available, security strategies should be planned to define how the system elements will be protected. Security strategies are roughly classified into three types: protection, detection and recovery. For example, preventing unauthorized access is a protective measure.

Finally, specific security measures should be chosen to achieve the chosen security strategies. Each security measure is implemented in the manner of physical, cyber, or operational (i.e., assigned to one of the three dimensions of the security model), according to the requirements and limitations of the system. For example, access control for a control system may be implemented as user authentication functionality in controllers or a card lock on the entrance of control rooms. Hitachi can provide a variety of security-related products and technologies for consistent security measures in any of the three dimensions thanks to its various business areas.

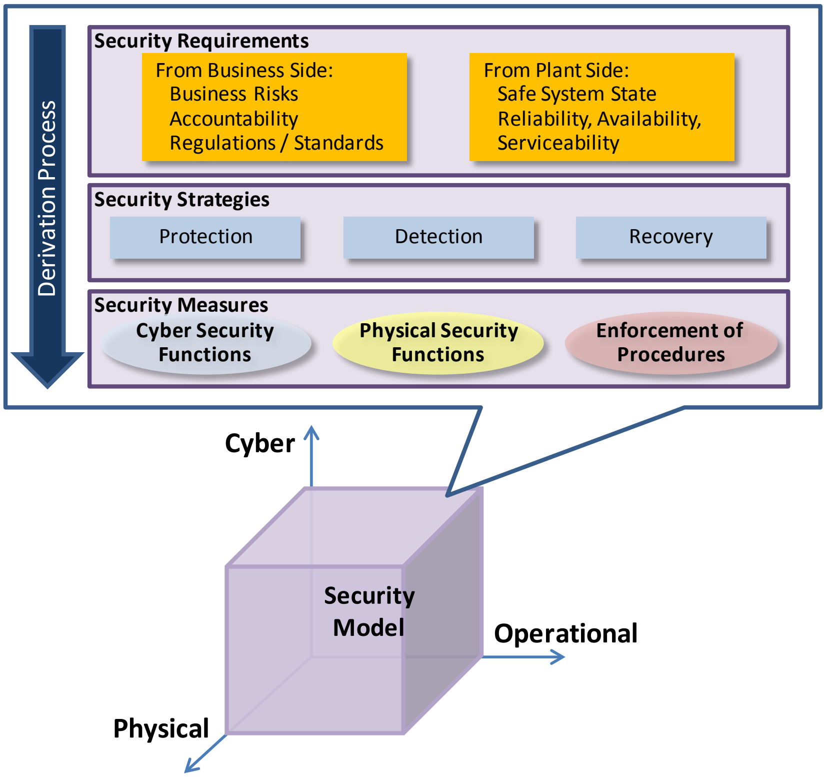

Figure 2 Security Derivation Process

3.3 Security Management Process

After the deployment of the control system, its safe system state models should be reviewed and maintained (e.g., upgraded) so that the system can stay within the defined “Safety-Controlled” states. This security life cycle management process is outlined in **Figure 3**. The continual management process (the Plan-Do-Check-Action cycle) shown in the lower right of **Figure 3** is needed in order to maintain the efficacy of the security measures. Since the system environment and external security environment are subject to change, risk assessments should be conducted regularly to check for new and potential threats such as newly emerged malwares or newly discovered system vulnerabilities. The period of the risk assessments should be derived from the security policy of the operating organization. When any risk is found during risk assessments, existing security measures should be amended or new security measures should be introduced.

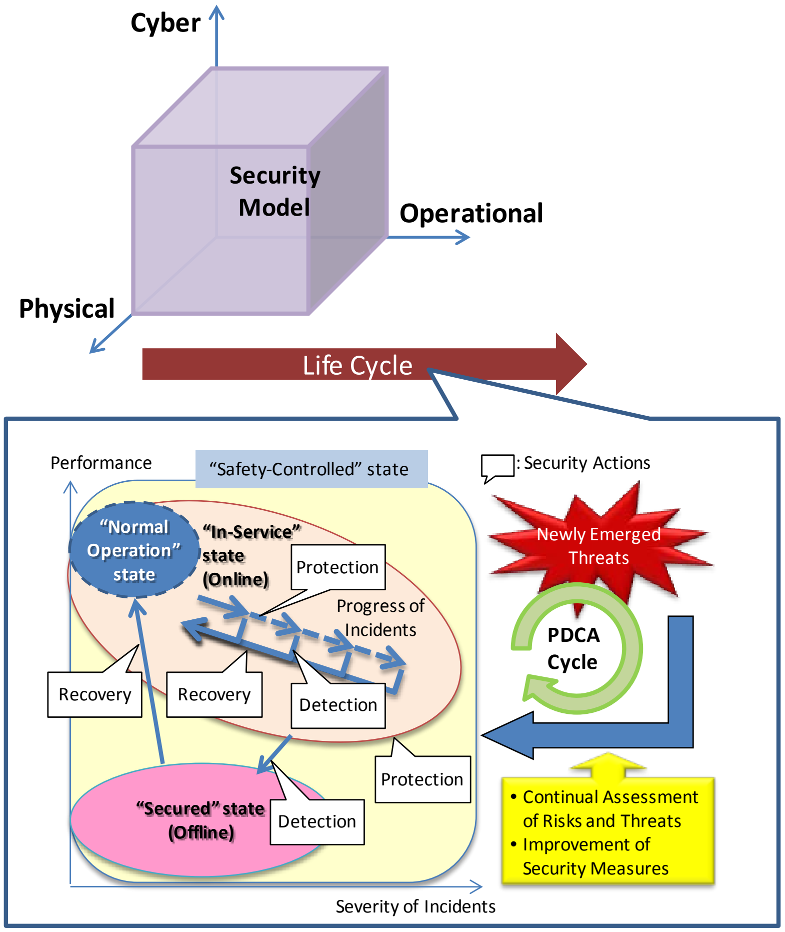

Figure 3 Security Management Process

4. Security Development Program for HITACHI Control Systems

Hitachi has been providing high reliability control systems for various critical infrastructure installations such as power systems [7][8], railway systems [9] and urban facilities [10] for the past several decades. Currently we have been developing a program to support the development of more secure control systems such as G-HIACS ν SAFE[2] platform [11] based on the security concept outlined in section 3 above. The main features of this program are described in the sub-sections below.

4.1 Support for Integration of Secure Control Systems

To develop control systems following the "2-Aspects and 3-Dimensions" development model, engineers must have the knowledge about how to choose appropriate security strategies and security measures for the target systems. Hitachi has developed guidance documents for our system

[2] ν SAFE is in the process of being registered as a trademark of Hitachi, Ltd

architects, design engineers and test engineers, in order to provide these professionals with the essence of the security derivation process and security management process for their respective system development activities.

These guidance documents are also intended to be compatible with major standards in order to meet the requirements of customers who need compliance with these standards. **Figure 4** outlines the development process of these guidance documents. First, Hitachi investigated the requirements in the major international standards documents such as NIST SP 800 Series, IEC 62443 Series, and NERC CIP. These requirements were then classified as related to the development phase or target component (or function) and requirement level. These requirements were also cross-coordinated with our own design guidelines for the design of high reliability systems.

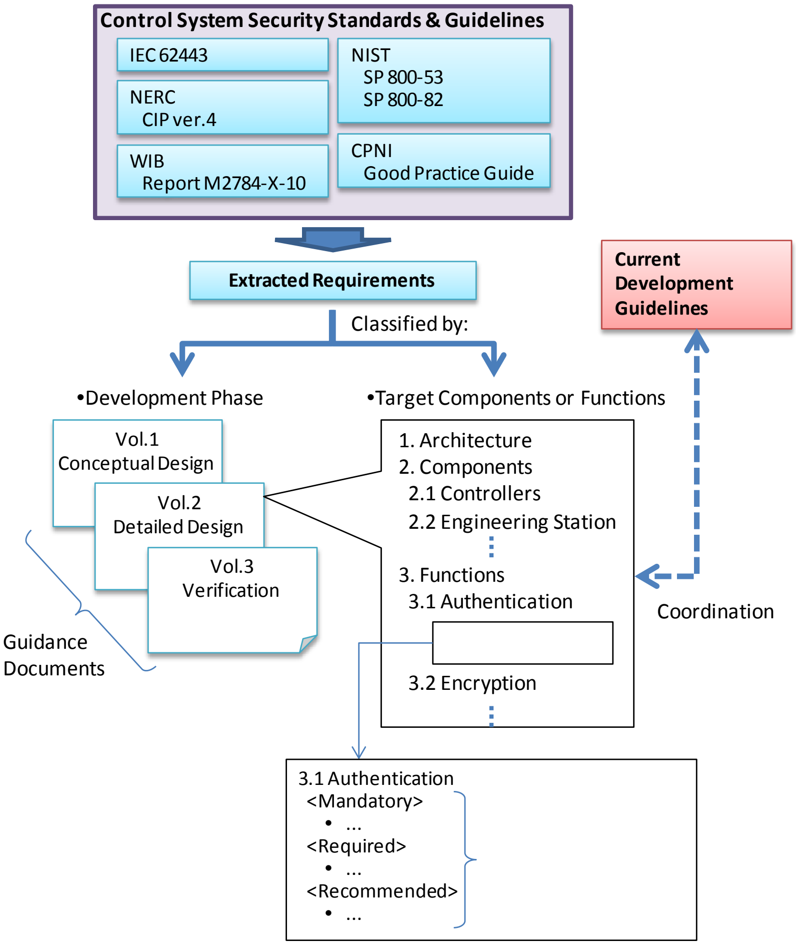

Figure 4 Development of Integrated Guidance Documents for Design

4.2 System Components Employing Embedded Security Technologies

Besides integrating equipment following strict security requirements, improving control system security requires the development of inherently more robust control equipment. Due to the requirement for real-time operation and the fact of limited computing resources, implementing such increased security functionality into equipment such as general-purpose computers (i.e., PCs) will be a significant challenge.

Another problem to implementation of more sophisticated security techniques to existing control systems is backward compatibility and interoperability with newer devices and software. In order to address these problems, Hitachi has been developing security technologies optimized for existing embedded control equipment thanks to our technological background and experience in key security-related areas such as IT systems and fault-tolerant computer systems. Hitachi also has embedded system technologies that enable us to provide high reliability components in those areas.

One technology example is "Enocoro", the lightweight and high throughput cipher algorithm suitable for embedded control equipment, which has been proposed for ISO/IEC 29192-3 by Hitachi [12][13]. Enocoro is optimized for embedded systems with software implementation in small memory footprint or hardware implementation with small circuit size. Short encryption latency by this feature enables equipment such as controllers and control servers to exchange encrypted messages with each other without interfering control functionality.

4.3 Applying Embedded Security Technologies to Control Systems

The embedded security technologies noted above should be coordinated appropriately to fit in the system architecture and target phase in the system life cycle, which are considered in the security derivation process and security management process.

For example, encryption functionality may be required in some part of control communication among the controllers and servers to prevent important control data from eavesdropping or unauthorized change. In this case, implementation of cipher algorithm such as Enocoro should be carefully chosen because the encryption functionality introduces some increase of system load and communication latency.

If the target equipment is newly developed controller or server with powerful CPU and sufficient memory, it will be possible to implement the cipher algorithm with software because the increase of system load and communication latency will not be significant. On the other hand, it is not feasible to implement the cipher algorithm if the target is an existing controller without enough computing resources or a controller manufactured by other companies. Alternatively, external encryption adapters or gateways which support the cipher algorithm by the hardware will be the best solution.

5. Conclusion

Since control systems are tightly coupled with the real world, protecting them from malicious influences is the main objective of control system security. Security measures should be carefully chosen to blend intelligently protection with functionality so that the system can continue its operations as much as possible and so maintain service integrity. One should not separate security and functionality when designing for maximum capability. The best solution is to design the system and its security measures as a unified whole in order to identify the safe system states and so develop maximally secure and dependable control systems.

Security measures should be derived to assure that the system stays within the defined safe states against any assumed threat and through the system's lifetime. The "2-Aspects and 3-Dimensions" security assurance model is proposed so that security measures can be rationally chosen and managed over the system life cycle. A security development program has also been introduced to support development of secure control system per Hitachi's proposed security concept.

This paper is a first step in stimulating discussion on and improvement of Hitachi's security concept and development program in view of its inclusion in the ISO/IEC 29192-3 international standard. This security concept for control systems will contribute to safe and dependable operation of Canadian nuclear systems throughout their lifetime, as well as any other infrastructure systems.

6. References

[1] Nicolas Falliere et al., "W32.Stuxnet Dossier", http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, 2010

[2] North American Electric Reliability Corporation (NERC), "Critical infrastructure protection (CIP)", Reliability Standards, http://www.nerc.com/page.php?cid=2%7C20, 2009-2011

[3] National Institute of Standards and Technology (NIST), "NIST special publication 800-82: Guide to industrial control systems (ICS) security", http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, 2011

[4] National Institute of Standards and Technology (NIST), "NIST special publication 800-53 (Rev.3): Recommended security controls for federal information systems and organizations", http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf, 2010

[5] PA Consulting Group and Centre for the Protection of National Infrastructure, "Good practice guide – process control and SCADA security", http://www.cpni.gov.uk/documents/publications/2008/2008031-gpg_scada_security_good_practice.pdf

[6] International Electrotechnical Commission (IEC), "IEC 62443: Industrial communication networks - Network and system security", 2008-2010

[7] Yoshio Maruyama et al., "Development of comprehensive monitoring and control system for power plants", *Hitachi Review*, Vol.60, No.7, 2011

[8] Chikashi Komatsu et al., "Development and commercialization of new digital protection and control equipment", *Hitachi Review*, Vol.60, No.7, 2011

[9] Tetsuya Ogawa et al., “Convergence of Information Technology and Control Systems in Railway Transportation Service Systems”, *Hitachi Review*, Vol.60, No.3, 2011

[10] Hitoshi Tomita et al., “People- and Environment-friendly Urban Development Utilizing Geospatial Information”, *Hitachi Review*, Vol.60, No.2, 2011

[11] V. Gomez et al., “Application of DCS to New Build CANDU® Designs using the G-HIACS ν SAFE Platform,” Proceedings of the 32nd Annual Conference of Canadian Nuclear Society, June 2011

[12] D. Watanabe et al., “Enocoro-80: A Hardware Oriented Stream Cipher,” Second International Workshop on Advances in Information Security, 2008

[13] D. Watanabe et al., “Update on Enocoro Stream Cipher,” 2010 International Symposium on Information Theory and its Applications (ISITA), 2010