Japan Computer Emergency Response Team Coordination Center

JPCERT CC®

J-CLICS Guidance

STEP 2

For ICS Engineers and Administrators

Japan Computer Emergency Response Team Coordination Center

March 27, 2013

About This Guide

This guide is provided as a supplement to J-CLICS (Check List for Industrial Control Systems of Japan). Its purpose is to clarify and explain the measures referred to in each checklist question.
This guide explains the meaning (background and purpose) of the questions listed on the checklist and how to implement specific countermeasures, so you can use it to more accurately judge whether you should mark each question with a ✓ or a X as well as to design and implement effective measures for the questions you mark with an X.

Content of This Guide

This guide has been prepared so that the sections for each question can be read independently of one another. Rather than reading the entire guide, you may read only those sections necessary for you to understand particular questions.
The guide uses the following format to provide information to help you obtain a deeper understanding of each question:

Background and Purpose
An explanation of the background and purpose of the J-CLICS question.

Potential Risks
Examples of potential risks if what the J-CLICS question asks is not met. You can eliminate or reduce these risks by implementing the measures described in the next section (Explanations and Implementation Examples).

Explanations and Implementation Examples
A detailed explanation of the J-CLICS question and examples of countermeasures you can take to fulfill the requirements described in the relevant question. Provided measures are strictly generalized examples. Using them as a guide, you must consider which measures are best for each work site.

References
Information sources related to the J-CLICS question, such as books, papers, and websites that you may use to better understand the question.

Supplement
Supplementary information pertaining to the J-CLICS question that may be useful when reviewing or implementing measures. This supplement appears at the end of each question.

Acknowledgments

J-CLICS was created through the cooperation of the SICE/JEITA/JEMIMA Security Working Group (WG) and the Joint Council of J-CLICS Users based on the items in the Japanese version of SSAT (SCADA Self-Assessment Tool), which is freely distributed by the JPCERT Coordination Center.

People Who Collaborated in the Creation of J-CLICS
(Affiliations as of the publication of this guide, titles omitted)

Takayuki Arai	Yokogawa Electric Corporation (JEMIMA)
Yuuji Umeda	Toshiba Corporation (JEMIMA)
Hiromichi Endo	Hitachi, Ltd. (JEMIMA)
Shirou Kitaura	The Japan Gas Association
Takushi Kitagawa	The Federation of Electric Power Companies of Japan
Satoshi Kubo	Fuji Electric Co., Ltd. (JEMIMA)
Satoshi Kuboya	Azbil Corporation (JEMIMA)
Yoshiaki Shimizu	Fuji Electric Co., Ltd. (JEMIMA)
Hiroyuki Sugitani	Mitsubishi Chemical Engineering Corporation
Kenji Takatsukasa	Fuji Electric Co., Ltd. (JEITA)
Naoto Takamune	Mitsui Chemicals, Inc.
Seiji Takita	Japan Electric Measuring Instruments Manufacturers' Association
Tsutomu Yamada	Hitachi, Ltd. (SICE)
Hidehiko Wada	Yokogawa Electric Corporation (JEITA)
Souichi Watanabe	Mori Building Company

Japan Electric Measuring Instruments Manufacturers' Association (JEMIMA)
The Japan Electric Measuring Instruments Manufacturers' Association (JEMIMA) PA/FA Measurement and Control Committee Security Research Work Group researches and studies the future impact of and initiatives on security in the manufacturing sector, and provides feedback and valuable information to JEMIMA member companies.

Japan Electronics and Information Technology Industries Association (JEITA)
The Japan Electronics and Information Technology Industries Association (JEITA) Control and Energy Management Technical Committee researches and studies issues and solutions in order to disseminate and promulgate industrial control system security measures, and defines and proposes visions for safe, secure factory and plant operation.

The Society of Instrument and Control Engineers (SICE)
The Society of Instrument and Control Engineers (SICE) Technical Committee on Instrument and Control Networks in the Technical Division on Industrial Applications researches and studies the implementation of the latest IT technologies, standardization activities, and industrial control system security technologies at industrial sites in order to coordinate information concerning the industrial control systems field.

Table of Contents

Introduction

About This Guide 2

Acknowledgments 3

1. Understanding of the System and Business

Question No. 1 5

2. Understanding of Threats

Question No. 2 8

3. Network Architecture

Question No. 3 11

4. Firewall

Question No. 4 13

5. System Monitoring

Question No. 5 16

6. Measures for Viruses

Question No. 6 19

7. Security Patches

Question No. 7 22

8. System Enhancement

Question No. 8 25

9. Backup and Recovery

Question No. 9 28

10. Processes for Transferred Personnel

Question No. 10 31

Appendix A

Information Security Reference Materials 33

1. Understanding of the System and Business Risks

Question No. 1

Do you understand the configuration of the industrial control system and manage its latest state, including the change history?

In order to grasp and reduce the business risks related to the industrial control system, it is important that you understand the system configuration. Management of the latest system state, including the change history, is important for quickly identifying the causes of failures and implementing countermeasures.

1

1.Understanding of the System and Business Risks Question No. 1

Background and Purpose

Possible business risks associated with industrial control systems include interruption of operations and provision of services due to disasters such as power failures, malfunctions, earthquakes, and fires; physical accidents, including those involving the loss of human lives triggered by losing control of equipment; and business-related confidential information leaks.

To reduce business risks associated with industrial control systems and quickly respond to incidents that do occur, it is vital to accurately analyze and evaluate the factors behind such risks as well as to consider and implement appropriate countermeasures. To this end, understand the configuration of the industrial control system as well as make and periodically update an inventory of the industrial control system (including the operating system ("OS") and installed software) and reevaluate its security risks. It is important to create a management ledger that includes the details of existing systems, their functions, critical operations/security, locations, owners, and support personnel, and to manage the systems' latest state.
Managing the systems' latest state minimizes business risks by enabling support personnel to quickly respond to possible impacts and understand the procedure for rapid recovery.

Potential Risks

If no management ledger is created for the industrial control system or if it is not kept up-to-date (changes to the system configuration are not reflected therein), countermeasures against the various failures and disasters mentioned above (not only natural disasters, but also human-caused disasters such as cases of unauthorized access) may be insufficient and business itself may be significantly affected due to unexpected side effects resulting from system configuration changes, delays in determining the root causes of troubles, missing countermeasures, and so on.

1.Understanding of the System and Business Risks

Question No. 1

Explanations and Implementation Examples

To manage the configuration of the industrial control system, you can implement the following measures.

(A) Create and maintain a management ledger.

Create a management ledger that records the assets that constitute the industrial control system, and identify the personnel responsible for managing each asset. Understand the threats to each piece of equipment and software as well as the vulnerabilities that lead to threats as well as the effects on business should such threats and vulnerabilities cause a failure.

Below are some examples of items to be recorded in the management ledger of assets that constitute the system. When creating a management ledger, identify all pieces of equipment and software related to the industrial control system, and understand their levels of importance. The following are some items to record in the management ledger.

- Personnel responsible for managing the equipment or software (names of asset owners, administrators, etc.)
- Type of equipment or software (format, backup media, license, etc.)
- Connection status of the equipment or software (interface used, names of connected devices, connection diagram, VLAN*1 setting information, etc.)
- Change logs for the equipment or software (changes to settings, upgrades, etc.)
- Installation (storage) status
- Installation (storage) location
- Installation (storage) period
- Use cases
- Range of users
- List of system account owners
- Method of disposal
- Information necessary to recover from a disaster
- Dependencies on other systems, etc.
- Network configuration diagram

*1 Virtual LAN: A function to subdivide a single network into multiple networks within the switching hub. Clarify the configuration information with respect to how the network has been subdivided.

Managing the latest status of the industrial control system by reflecting changes to the system configuration in the management ledger and by periodically reviewing the ledger will help you understand the industrial control system and identify threats and vulnerabilities (see Question No. 2).

References

- Information-technology Promotion Agency (IPA): Information Security https://www.ipa.go.jp/security/english/index.html
- ISMS User Guide (Risk Management) https://www.isms.jipdec.or.jp/english/isms/index.html
- ISO/IEC 27001:2007 A.7.1.1 Inventory of assets
- ISO/IEC 27001:2007 A.7.1.2 Ownership of assets

2. Understanding of Threats

Question No. 2

Do you understand the possible threats to each component of the industrial control system?

In order to avoid business risks related to the industrial control system, it is important to understand what kind of attacks and failures each component of the control system may experience and to consider countermeasures against such threats.

2. Understanding of Threats
Question No. 2

Background and Purpose

The industrial control system administrator understands the threats to the system and its vulnerabilities, and assesses possible risks. Countermeasures against the occurrence of such risks must be considered.
For example, understand what kinds of threats the industrial control system may experience (power outages, unauthorized access, etc.), which vulnerabilities exist (insufficient maintenance of power supply equipment, improper password management, etc.), and their severity (high or low), and after that, consider countermeasures. Consideration of countermeasures leads to their prioritization per component.

Potential Risks

If the threats to components of the industrial control system and their vulnerabilities are not understood or if measures against risks are not taken, the business itself may be significantly impacted.

2. Understanding of Threats

Question No. 2

Explanations and Implementation Examples

To manage the configuration of the industrial control system, you can implement the following measures.

(A)Understand threats.

Identify threats for each component of the industrial control system.

In this guidance, a "threat" refers to the cause of an accident that results in the loss of or damage to the industrial control system, organization, or business. Extract existing threats (earthquakes, floods, fires, power failures, theft, dust, deterioration of recording media, software failures, unauthorized access, and information leak), and identify and classify the security-related items among such threats. Threats are classified into intentional, accidental, and environmental threats.

Examples of Threats and Countermeasures

- Intentional threats
  An example of an intentional threat is information leak by an insider. In this case, a countermeasure would be an educational campaign.
- Accidental threats
  Examples of accidental threats are input and operational errors. In this case, countermeasures would be to require double input and to add a check flow.
- Environmental threats
  Examples of environmental threats are earthquakes and fires. Installation of a seismic isolation floor, decentralized management of backup media, and duplication of the industrial control system are possible countermeasures to environmental threats.

(B) Analyze and respond to threats.

Based on the classification of threats described in (A) above, consider and implement risk assessment and risk management (appropriate countermeasures against the loss of power supply, unauthorized access, etc.) Also, based on individual threats and classified threats, consider the priorities of risks and take measures that take into consideration such priorities.

For example, risks arising from the threat of "unauthorized access" include "unauthorized operation" and "falsification of data." Countermeasures against such risks include "installation of a firewall," "strengthening of access restrictions," and so on.

Though it is ideal to implement countermeasures against all such threats, it is important to prioritize effective measures by taking into account the budget and implementation timing.

Regarding "unauthorized access" and "viruses," understand what is asked in the questions about the "Network Architecture" of the industrial control system, and install a firewall and/or implement antivirus measures.

Reference

- Information-technology Promotion Agency (IPA): Information Security (Countermeasures against viruses, bots, unauthorized access, etc.)

https://www.ipa.go.jp/security/english/index.html

3. Network Architecture

Question No. 3

Do you understand the communication specifications and connection specifications for all equipment connected to the industrial control system?

Create a management ledger that describes the communication specifications and connection specifications for all equipment connected to the industrial control system in order to understand the system's status. To do so, it is more efficient to add the items related to communication and connection specifications to the management ledger created in Question No. 1. Integrating several management ledgers into a single ledger can simplify asset management.

3

Background and Purpose

To ensure network security for the industrial control system, it is important to first understand the system's communication specifications and connection specifications. Understand the name, purpose, administrator, communication specifications, connection specifications, and so on of the equipment connected to the industrial control system and create a management ledger. The management ledger can be used to assess security risks and to consider countermeasures. It is also helpful for auditing unauthorized system changes. Understanding the system' s normal connection and communications status can assist in analyzing a system failure or evaluating a security incident.

Potential Risks

When the communication specifications and connection specifications for equipment connected to the industrial control system are unknown, the normal system status may not be correctly understood, and system malfunctions may not be adequately detected.
For example, the connection of unauthorized equipment or changes to communication configuration may go unnoticed. This could result in virus infections, opening up of intrusion routes, or unexpected failures, which may lead to serious situations such as operational shutdown.

Explanations and Implementation Examples

Create a management ledger that covers the communication specifications and connection specifications of all equipment connected to the industrial control system. When creating this ledger, it is recommended to contact the vendors involved in system construction and have them submit management ledgers that contain the most up-to-date information.

Example of Items to Track in the Management Ledger

- Name of communication
- Purpose of communication
- Name of protocol used
- Port number used
- Timing of usage (e.g., during operation or maintenance)

Use the management ledger to audit the connection status and consider security measures. During audits, re-examine the necessity of connections, and abolish unnecessary connections and communications instead of leaving them in place (disconnect unnecessary connections and close communication ports that do not need to be open).

Reference

- Information-technology Promotion Agency (IPA): Information Security
  https://www.ipa.go.jp/security/english/index.html

4. Firewall

Question No. 4

Is a firewall set up at the boundary between the industrial control system and other networks to block unnecessary communication?

In order to prevent unauthorized access to the control equipment connected to networks and to prevent virus infections, set up a firewall at the boundary between the industrial control system and other networks to block unnecessary communication.

4

4. Firewall
Question No. 4

Background and Purpose

Though connecting to networks is a necessary means of communication, it may also provide an intrusion route for attacks and viruses.
For this reason, it is safer not to connect the industrial control system network to external networks, such as an intranet or the Internet. If operational requirements necessitate connecting the industrial control system network to other networks, set up a firewall at the boundary of the networks and allow only necessary communications to pass through.

Potential Risks

A network connected to external networks without a firewall in place is open to attacks from outside and virus infections.

4. Firewall Question No. 4

Explanations and Implementation Examples

Although firewalls are useful for improving security, improperly configured or operated firewalls may cause abnormal system behavior or fail to provide the expected effects.
When setting up and configuring a firewall, it is important to thoroughly consider how to do so in advance. Contacting the industrial control system vendor for consultation and advice can be helpful. The following are some implementation examples based on the above explanation.

(A) Examine the necessity of connection to other networks.

Connecting the industrial control system network to other networks such as an intranet or the Internet may expose the industrial control system to risks of attack or intrusion from such networks. If communicating with other networks, re-examine the necessity of connection, abolish unnecessary connections and communications instead of leaving them in place, and disconnect unnecessary connections.

(B) Set up a firewall.

If connecting to other networks, set up a firewall at the boundary and allow only necessary communications to pass through. Keep the following points in mind when setting up a firewall.

(1) Ask the control equipment vendor about the recommended configuration and settings.

If passing control equipment-related communications through the firewall, ask the equipment vendor about the equipment's communication specifications and use the recommended firewall equipment and settings, if any.

(2) Protect the firewall against unauthorized access.

Allow only the administrator to modify the firewall settings and connections. Additionally, physically protect the firewall by storing it in a locked rack or similar location, and use configuration features over the network as infrequently as possible. Since using the default administrator password makes the firewall easier to attack, it is recommended to change it. This helps prevent modification of settings in the case of unauthorized access.

Reference

- Information-technology Promotion Agency (IPA): Information Security
  https://www.ipa.go.jp/security/english/index.html

5. System Monitoring

Question No. 5

Do you regularly check and analyze the industrial control system’s operating status and logs even during normal times?

To quickly find abnormalities in the industrial control system, it is important to recognize the system's normal state by regularly checking and analyzing the system's operating status and logs even during normal times.

5

Background and Purpose

It is important to check and analyze the industrial control system’ s operating status and logs so that abnormalities in the industrial control system due to virus infections or equipment failures can be promptly found. Impacts on operations may be minimized if abnormalities can be noticed before they impact the industrial control system’ s operation and information to facilitate a quick response can be collected together with support personnel when trouble occurs. To this end, an eye must be kept on CPU usage, memory consumption, free HDD space, the industrial control system's network communication status, logs output by the industrial control system’ s OS, and so forth during normal operation as well as to have an organization in place and a practice of awareness to quickly find signs of abnormalities.

Potential Risks

If you do not regularly check the operating status of the industrial control system during normal times, it is impossible to accurately determine whether the system's status is normal or abnormal, and you may miss signs of abnormalities. As a result, abnormalities could remain unnoticed until they impact the industrial control system's operation, ultimately leading to a serious situation such as operational shutdown.

5. System Monitoring
Question No. 5

Explanations and Implementation Examples

Check logs and the system's operating status daily to promptly discover system abnormalities. Check and analyze the usage rate and amount of space particularly for the following items.

- CPU usage
- Memory consumption
- Free HDD space
- Network connection status
- System logs
- Operating status of processes and services
- Login/logout records

Recording these items and checking their statuses help to grasp the system’ s tendencies during normal times. If a tool is to be used, it is convenient to choose one that keeps historical records in addition to displaying the system's operating status. Operating status records are also valuable when analyzing abnormalities.
The industrial control system's status can be checked in the following ways.

(A) Method recommended by the industrial control system vendor

If the industrial control system vendor recommends a method for checking, analyzing, and recording the system's operating status, use that method.

(B) With tools provided with the OS

Tools included in the OS (e.g., Windows Task Manager) can be used to obtain information on the system's operating status.

(C) With dedicated tools

It is also possible to monitor the system using commercially available tools. When using such monitoring tools, install them after testing the impact that they exert on the industrial control system. It is effective to choose a tool that keeps historical records in addition to displaying the system's operating status.

Reference

- Information-technology Promotion Agency (IPA): Information Security
  https://www.ipa.go.jp/security/english/index.html
- ISO/IEC 27001: A.10.10 Monitoring

6. Measures for Viruses

Question No. 6

Are antivirus measures in place for the industrial control system?

To prevent damage to the industrial control system caused by virus infections as much as possible, implementing antivirus measures is recommended.

6. Measures for Viruses

Question No. 6

Background and Purpose

In recent years, the risk of virus infections has increased due to the introduction of general purpose OSes to industrial control systems and due to connection to other networks for business requirements (e.g., data sharing between the industrial control system and other systems). Virus infections may lead to abnormal system behavior and/or shutdowns, which is why antivirus measures are needed.
Because some antivirus measures can affect system behavior, when planning and implementing antivirus measures, contact the industrial control system vendor in advance and follow the recommended method.

Potential Risks

When the industrial control system is infected by a virus, it may malfunction, exerting a significant impact on operations and business.

6. Measures for Viruses

Question No. 6

Explanations and Implementation Examples

In order to prevent virus infections, it is important to carry out management so as not to bring in viruses from outside.
An effective way to reduce the chance of infection by viruses and such is to isolate the industrial control system from other networks as much as possible. If the industrial control system is connected to other networks for business requirements, prevent virus infections by setting up a firewall or similar to restrict unnecessary communications. In addition, it is recommended to take measures such as performing virus scans of external storage media such as USB memory devices when using them to share data with the industrial control system. Some industrial control system products provide enhanced system configurations and/or additional software as antivirus measures.
On the other hand, some industrial control systems do not allow measures such as antivirus software to be introduced. In addition, some industrial control systems may not be easy to stop or restart, which makes it difficult to modify them by applying patches, updating software, and so on. In such cases, it is possible to isolate and manage the industrial control system itself without installing antivirus software.

Various kinds of antivirus measures prevent infections over networks, via brought-in media, and on the industrial control system PCs. Because some antivirus measures can adversely affect system behavior, when planning and implementing antivirus measures, it is recommended to contact the industrial control system vendor and follow the recommended method.

(A) Measures against infections over networks

Measures to prevent virus infections over networks include elimination of unnecessary network connections, disconnection (e.g., turning off network equipment) of networks that are not regularly used, installation of a firewall, and configuration enhancement.

(B) Measures against infections via brought-in media

Measures to prevent virus infections via brought-in USB memory devices and/or PCs include placing restrictions on brought-in media, deletion of unnecessary files on such media, and virus scanning upon bringing such a device in.

(C) Measures on the industrial control system PCs

Measures to prevent virus infections on the industrial control system PCs include locking up of equipment, blocking of unnecessary connection ports (USB ports and network ports), disconnection (e.g., powering off) of equipment that is not regularly used, installation of antivirus software, enhancement of the OS and software configurations (hardening *2), and installation of security software to restrict program launching, etc.
*2 See Question No. 8 for details.

Reference

- Information-technology Promotion Agency (IPA): Countermeasures on Computer Virus
  https://www.ipa.go.jp/security/english/virus/antivirus/shiori-e.html

7. Security Patches

Question No. 7

Do you have an established procedure to apply patches to the industrial control system and applications running on it based on vendor-provided information, and does this procedure take into consideration the adverse effects on your business that may result from applying such patches?

Prompt application of security patches is essential to keep industrial control systems safe from cyberattacks. Clarify how to obtain information on security patches, the timing for applying patches, and the work procedure for doing so. When establishing a patch application procedure, it is recommended to develop a plan that enables restoration of the latest state from a backup in consideration of the unlikely case in which a security patch exerts adverse effects.

7. Security Patches
Question No. 7

Background and Purpose

When a vulnerability (i.e., a weak point that could be exploited in an attack) or a problem is found in an industrial control system, the system vendor releases a security patch or takes other measures. In order to keep the system safe, it is vital to promptly obtain countermeasure information and respond to the problem. Always be familiar with how to obtain information and the procedure for responding when a security patch is released, even during normal times. In addition, develop a procedure to back up the system before starting work and apply patches while confirming normal system operation to several units at a time, not to all units at once, in consideration of the possibility that a virus infection and/or malfunction may occur during the work.

Potential Risks

If security patches are not applied, the system may succumb to attacks and/or system behavior may not be as expected. Additionally, if security patches are not applied using the correct procedure, there is a risk of virus infection during patch application as well as a risk of the system operating abnormally due to a glitch in a security patch itself. Problems may persist even after applying security patches.

7. Security Patches

Question No. 7

Explanations and Implementation Examples

Keep the following points in mind when considering and applying security patches.

(A) Check with the industrial control system vendor on how to obtain security patch information.

Check with the industrial control system vendor on how to obtain security patch information so that such information can be quickly obtained when security patches are released. When security patch information is released, check the necessity and effects of patch application.

(B) Check with the industrial control system vendor regarding the patch application procedure.

Check with the industrial control system vendor regarding the procedure to apply patches to the industrial control system and become familiar with the recommended procedure, if any.

(C) Consider risk measures when applying security patches.

Applying patches may cause the industrial control system to operate abnormally, so consider the following points as precautions.

(1) Run a virus scan on the recording media and/or PC to use to apply security patches.

In order to prevent virus infections during patch application, run a virus scan on the recording media (CD, DVD, etc.) and memory device (USB memory device, USB hard disk drive, etc.) to use. For PCs to be used to apply patches, run a virus scan before connecting them to the industrial control system.

(2) Back up the system before applying security patches.

A failure during patch application work or a bug in a security patch itself may induce abnormal system behavior. Before applying patches, back up the system as a precaution so that it can be restored to the previous state if something goes wrong.

(3) Apply security patches to equipment sequentially starting with the equipment that has the least impact on operation.

In consideration of the risk that the system may operate abnormally due to applying a patch, apply security patches to equipment sequentially starting with the equipment having the least impact on operation; check that operation is normal before proceeding to the next piece of equipment instead of applying patches to all equipment at once.

References

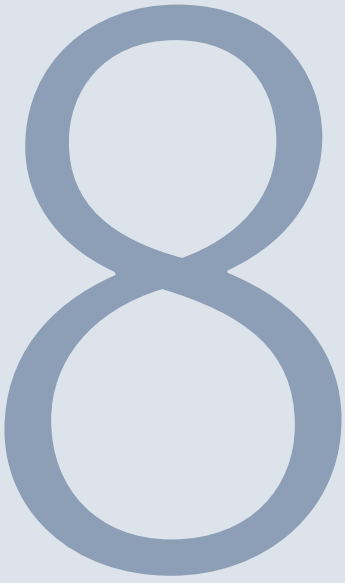
• Information-technology Promotion Agency (IPA): Information Security
https://www.ipa.go.jp/security/english/index.html

8. System Enhancement

Question No. 8

Do you suspend or disable unused OS services and communication ports upon initially installing or upgrading the OS and applications used on the industrial control system?

To reduce vulnerabilities, suspend or disable unused services (e.g., those of the OS) and communication ports on the industrial control system.



8. System Enhancement Question No. 8

Background and Purpose

Services over the network and communication ports are possible intrusion routes for attackers (vulnerabilities). To reduce vulnerabilities, suspend or disable unused services (e.g., those of the OS) and communication ports on the industrial control system.

Potential Risks

Attacks that exploit the vulnerabilities of functions of OS services (e.g., ftp and telnet) and communication ports may cause unstable or abnormal system behavior, leading to operational shutdown.

8. System Enhancement Question No. 8

Explanations and Implementation Examples

Suspending unnecessary system functions to improve security is known as "fortifying" or "hardening." Although hardening is effective for improving security, improper configuration can cause system abnormalities. When implementing hardening, check with the industrial control system vendor in advance and use the recommended method and settings, if any. When configuring settings on one's own, it is still recommended to seek advice from the industrial control system vendor regarding settings.

When implementing hardening, take the following into account.

(A) Uninstall unnecessary applications.

Uninstall unused applications from the system. Do not install unnecessary applications.

(B) Delete unnecessary accounts.

Leaving unnecessary accounts on the system may increase the system's vulnerabilities. Delete unused accounts.

(C) Allow only the minimum number of necessary users to access files and folders.

Check that access rights to files and folders are appropriate and give only the minimum necessary permissions (e.g., write, read, execute) to the minimum number of necessary users.

(D) Disable unused functions.

Disable unused OS functions (e.g., shared folders, printer sharing, auto-play).

(E) Render unused ports (e.g., USB, IEEE1394, and network ports) physically unusable.

Block ports on the industrial control system that will not be used with a jig or seal (such that removal can be detected) so that the ports cannot be used without permission.

Reference

- Information-technology Promotion Agency (IPA): Information Security
  https://www.ipa.go.jp/security/english/index.html

9. Backup and Recovery

Question No. 9

Do you back up the data necessary to restore the industrial control system as recommended by the vendor?

It is necessary to back up the data that is required to restore the industrial control system.

Background and Purpose

As a precaution, it is necessary to regularly back up the data required to restore the industrial control system (e.g., parameters and operation data) and to verify such backup data (by checking that the data is not corrupted). Therefore, be sure to store data in the vendor-recommended way.

Potential Risks

The industrial control system may malfunction and need to be restored for recovery.
In this case, the most recent data before the malfunction is necessary. If regular backups are made at short intervals, restoration using data that is almost the same as the data at the time of the malfunction becomes possible.
Having no backup of data may significantly impact business due to the longer time required to recover to normal operation.

9. Backup and Recovery Question No. 9

Explanations and Implementation Examples

It is recommended to consider the following items when making backups.

(A) Frequency of backups

Consider the timing for making backups by considering how recent backup data is needed when restoring the system. If the system data is updated online every day, make a backup every day. On the other hand, if the system data is updated less frequently, make a backup before changes are made to the system or monthly. Backup frequency must be determined based on the characteristics of system operations.

(B) Generation management of backup data

Determine the retention period for backup data in line with the frequency of backups discussed in (A) above. Generation management of backup data allows for the restoration of data from several generations before if, for example, some trouble is discovered some time after the system has been modified. In order to ensure the validity of the restored system, the number of generations to keep and the retention period for backups must be adequately determined.

(C) Remote management of backup data

In order to make recovery possible even when a disaster such as a fire or flood occurs, backup data must be stored not only locally but at a remote location.

(D) Method of backup

Backups can be made as a whole or differentially in order to shorten the time required to make each backup. Operational efficiency can be improved by considering the backup method as well.
Additionally, to avoid the risk that backup data may not be able to be read due to defects in the recording media, verify the data upon making a backup and carry out the backup procedure again if the backup is incomplete.

Reference

- Information-technology Promotion Agency (IPA): Information Security
  https://www.ipa.go.jp/security/english/index.html
- ISO/IEC 27001: A.10.5.1 Information back-up

10. Processes for Transferred Personnel

Question No. 10

Do you document and implement procedures for account addition/deletion and password changes in the event of personnel transfers, including making changes to the roles or responsibilities of personnel registered in the system?

When the members authorized to operate the system or their roles and responsibilities are changed, the system administrator must add or delete the relevant member accounts or change the passwords of administrative accounts.

10

10. Processes for Transferred Personnel

Question No. 10

Background and Purpose

The system administrator grants operation permissions for the industrial control system only to those who need them. In addition, the system administrator must regularly carry out reviews to ensure that the permissions of accounts to which operation permissions have been granted are appropriate. When members who are granted industrial control system operating permissions change due to new hiring or retirement, and also when members' roles and responsibilities change, permissions must be reviewed.

Potential Risks

If accounts and passwords are not properly managed, business interference or information leak could occur due to unauthorized access by retired members or members who should no longer have operation permissions, leading to a major impact on the business itself.

Explanations and Implementation Examples

Considering the fact that some of the incidents affecting industrial control systems reported overseas involve cases of unauthorized access from outside by a retired member of an organization, operational countermeasures must be taken in addition to technical and physical countermeasures.
Examples of operational countermeasures include granting the minimum necessary industrial control system operation permissions to the minimum number of necessary personnel and deleting accounts as soon as possible once accounts are no longer required in order to create an environment that prohibits misuse or destruction of the system as well as prohibits bringing information out.
It is critical to document these procedures in the security implementation procedure manual or similar document, regularly change passwords, check the system login history for unauthorized access, and construct and implement a mechanism for promptly reporting transfers and retirements. It is also necessary to regularly review whether or not the current procedure is appropriate.

Reference

- Information-technology Promotion Agency (IPA): Information Security
  https://www.ipa.go.jp/security/english/index.html

Appendix A

Information Security Reference Materials

Information Security Reference Materials

The following lists documents and websites where you can learn more about information security.
(Website information (URLs) is current as of January 2013.)

1. References on Information Security

- JPCERT/CC website

https://www.jpcert.or.jp/english/cs/controlsystemsecurity.html
https://www.jpcert.or.jp/english/
Regarding industrial control system security, the following kinds of helpful information on incident response are available.

Guidelines, standards, and similar documents
Related tools
Presentation materials
Information introducing the information sharing community and other communities
Security alerts
Vulnerability-related advisory
Other information

You can also use the website to submit a request for consultation from JPCERT/CC on how to respond in the case of an incident.

- JPCERT/CC Information on Industrial Control System Security

https://www.jpcert.or.jp/ics/ics-community.html (Japanese)
Information that JPCERT/CC collected and organized, news and trend on the control system security, examples of threats, reference information on standards and rules, etc. are provided to participants of the industrial control system security community.

- Information-technology Promotion Agency (IPA) Website

http://www.ipa.go.jp/index-e.html
The IPA website provides information on emergency responses related to information security, materials on information security measures, seminar and event information, notifications and consultation information, and information on software engineering.

- IPA Control System Security

http://www.ipa.go.jp/security/controlsystem/index.html (Japanese)
Information on the security of industrial control systems used in critical infrastructure can be found here.

2. Standards and Guidelines

- Information Security Management Guide—JIS X 5080:2002 (ISO/IEC 17799:2000) (Japanese)

Co-authored by Yoshiyuki Hirano, Masahiro Mizumoto, Kenichiro Yoshida, and the Japanese Standards Association.

- ISO/IEC 17799: 2005 (JIS Q 27002: 2006) Code of Practice for Information Security Management (Japanese)

Co-authored by Koji Nakao, Yoshiyuki Hirano, Kenichiro Yoshida, Hatsumi Nakano, and the Japanese Standards Association.
This is the handbook to ISO/IEC 17799: 2005 on information security management. The handbook discusses measures that should be carried out for information security management.

- GOOD PRACTICES GUIDE - PROCESS CONTROL AND SCADA SECURITY

Prepared by the Center for Protection of National Infrastructure (CPNI). Translated by JPCERT/CC.
https://www.jpcert.or.jp/ics/information02.html (Japanese)
In outlining the need for process control and SCADA system security and revealing the difference between process control or SCADA system security and IT security, this guide demonstrates the seven stages to handle process industrial control system security and the principles behind good practices in each stage.

• Japanese Version of SSAT (SCADA Self-assessment Tool)

Developed and created by the Centre for Protection of National Infrastructure (CPNI). Japanese version developed by JPCERT/CC.

https://www.jpcert.or.jp/ics/ssat.html (Japanese)

JPCERT/CC has developed a security self-assessment tool that is focused on monitoring and industrial control systems using SCADA developed by the UK-based CPNI. You can use this tool in conjunction with the Good Practices Guide - Process Control and SCADA Security to obtain a deeper understanding of industrial control system security.

3.Vulnerability Information

• Vulnerability countermeasure information portal site: JVN (Japan Vulnerability Notes)

https://jvn.jp/en/

JVN stands for "the Japan Vulnerability Notes." It is a vulnerability information portal site designed to help ensure Internet security by providing vulnerability information and their solutions for software products used in Japan.

• Common Vulnerabilities and Exposures (CVE)

http://cve.mitre.org

This is the vulnerability information website operated and managed by the US-based MITRE Corporation that administers CVE. The website provides information on vulnerabilities found in software. Each vulnerability is assigned a CVE-ID; these IDs are used internationally.

• Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

http://www.us-cert.gov/control_systems/ics-cert/

Operated by the US Department of Homeland Security (DHS), ICS-CERT is an incident response organization that focuses on industrial control systems. The ICS-CERT website provides newsletters, advisories, reports, and other information on industrial control system security.

4.Information on Information Security Policies

• Ministry of Economy, Trade and Industry

http://www.meti.go.jp/policy/netsecurity/index.html (Japanese)

This website provides information on security policies from METI. Information on government security policies, various reports, guidelines, and so forth are posted here

• National center of Incident readiness and Strategy for Cybersecurity (NISC)

http://www.nisc.go.jp/eng/index.html

The website of the National center of Incident readiness and Strategy for Cybersecurity posts various conference materials, security-related investigation reports, and information on relevant laws.

• Ministry of Internal Affairs and Communications

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html (Japanese)l

Investigation reports, public relations documents, and other information pertaining to security can be viewed at the information security policy website.

• National Police Agency

http://www.npa.go.jp/cyber/ (Japanese)

On its cybercrime countermeasures website, the NPA posts information on its efforts to prevent and crack down on cybercrime, cybercrime statistics, and how to contact it for a consultation on cybercrime as well as other information.

Copyright Notice