An unauthorized transmission of a command interrupts the supply in a wide area.

A malicious third party accesses the firewall from the data historian.

Management of authority

Collecting/analyzing logs

Management of authority

Access control

A malicious third party accesses from the firewall to a data server.

A malicious third party accesses the PLC (master) from the data server.

Some malware accesses the data historian from a monitoring terminal or has it infected with the malware.

A malicious third party accesses from the firewall to a control server.

A malicious third party has the monitor terminal infected with some malware.

Some malware accesses the firewall from the data historian or has it infected with the malware.

Vulnerability

Detecting device errors

1, 2, 3, 8, 9, 10

Objective-execution phases

Measures level

Attack tree

Quick Guide

Information-technology Promotion Agency, Japan
Technology Headquarters
IT Security Center (ISEC)
April 2018
Security Risk Assessment Guide for ICS
Main Guide Book and Supplement

[Contents from Main Guide Book]
Chapter 1. Risk Assessment as Security Measures
Chapter 2. Overview and Work Flow of Risk Assessment
Chapter 3. Getting Ready for Risk Assessment
Chapter 4. Working on Risk Assessment
  4.1. Asset-based Risk Assessment
  4.2. Business Risk-based Risk Assessment
Chapter 5. Interpreting and Making Use of Risk Assessment
Chapter 6. Security Test
Chapter 7. Additional Standards to Specific Measures
Reference and Appendix

Download available at: https://www.ipa.go.jp/security/controlsystem/riskassessment.html
Tactics of Fighting against Cyberattacks
– Importance of Security Risk Assessment –

Sun Wu, a military strategist in the Spring and Autumn Period of China, was the author of "Sun Tzu," in which he said the maxim: "Know thyself, Know thy enemies, Fear not one-hundred battles." In our cyberattack age, we could interpret "enemies" as "threats" (including attackers) and "thyself" as "our organization." Then, the maxim shows us what we should do to be effective for security.

**Security risk assessment** is the art of warfare of the cyberattack age that implements

"Risk assessment" = The process to make clear the business risks with the assessment indices ①, ②, and ③

① The value (importance) of the objects (assets and business) of the assessment, the dimensions of and influence over possible risk
② The possible threats to the objects of the assessment and the probability of the occurrence
③ The acceptability (the vulnerability of the objects of the assessment and the unreadiness to provide measures) at the occurrence of any of the possible threats

**The importance and the effectiveness of risk assessment**

- To realize effective risk mitigation
- **To realize effective security investment** (to add measures, to select efficient test points)
- To provide a base for establishing a PDCA cycle and for **continuing the maintenance and enhancement of security**
Methods of and Challenges in Risk Assessment

Various Methods of Security Risk Assessment and their Features and Challenges –

Methods of risk assessment and their features

<table>
<thead>
<tr>
<th>Assessment method</th>
<th>Labor</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline approach</td>
<td>Small</td>
<td>△</td>
</tr>
<tr>
<td>Informal approach</td>
<td>Small</td>
<td>× ?</td>
</tr>
<tr>
<td>Detailed risk assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset-based</td>
<td>Medium</td>
<td>○</td>
</tr>
<tr>
<td>Scenario-based</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack tree assessment (ATA)</td>
<td>Large</td>
<td>○</td>
</tr>
<tr>
<td>Fault tree assessment (FTA)</td>
<td>Large</td>
<td>○</td>
</tr>
<tr>
<td>Combination approach</td>
<td>Large</td>
<td>◎</td>
</tr>
</tbody>
</table>

Challenges in detailed risk assessment

[Challenge A] **Specific procedures and steps** of the risk assessment are **not clear**.
[Challenge B] You want to avoid it because (it is said that) you need **a huge amount of labor** for risk assessment.

The Guide shows you the answers to these challenges.
Two Types of Detailed Risk Assessment Presented
Asset-based Risk Assessment and
Business Risk-based Risk Assessment

★ Asset-based risk assessment  <Know thyself>

To conduct the risk assessment with the three assessment indices—the importance (value), the possible threats, and the vulnerability—on each of the assets (servers, terminals, communication devices, etc.) among the assets constituting the system you should protect. ⇒ Enable to assess the threats and the state of security comprehensively with respect to assets

★ Business Risk-based risk assessment  <Know thy enemies>

To define the business risk you want to avoid with respect to the business and service having been realized by the system you should protect, and to conduct a risk assessment with the three assessment indices: the level of the business risk at an occurrence, the probability the attack scenario may actually occur, and the vulnerability to the scenario (the acceptability of the scenario)
⇒ Enable to assess the attacks that lead to business
(The strongpoints of ATA and FTA are combined)

⇒ Desktop penetration testing
1. Risk Assessment as Security Measures

The importance and necessity of a risk assessment of control systems are presented.

• The necessity of the security measures on a control system
  – Changes in systems and components
  – Connection with external networks, storage media brought in from the outside
  – Characteristics of control systems
  – Increasing reports on vulnerabilities, targeted attacks, malware infections, and so forth

• The importance of risk assessment
  – The process to make clear the systems you should protect and the levels of the threats and the risk to the business realized by the systems
  – Essential as a security measure
2. Overview and Work Flow of Risk Assessment

The comparison of the methods for risk assessment, the steps of the work, and how to use this guide are presented.

- The overview of risk assessment
  - Baseline approach
  - Informal approach
  - Detailed risk assessment
  - Combination approach

- The work flow of risk assessment
  - Asset-based risk assessment
  - Business risk-based risk assessment

- The composition of this guide and how to use it
  - The composition of this guide
  - A suggestion for conducting security assessment
### 3. Getting Ready for Risk Assessment

#### Analyze your organization and understanding it. = "The most important step to know thyself"

[Preparatory steps and their outputs]

<table>
<thead>
<tr>
<th>Section</th>
<th>Preparation</th>
<th>Output</th>
</tr>
</thead>
</table>
| 3.1     | • Making clear your system configuration  
         | • Making clear your assets and their main functions  
         | • Making clear data flows                                | • A list of assets  
         |                                                            | • System configuration chart  
         |                                                            | • Data flow chart                                    |
| 3.2     | • Defining the criteria for judging the importance of assets  
         | • Determining the importance of assets                        | • Criteria for judging the importance of assets  
         |                                                            | • A list of the importance of assets                  |
| 3.3     | • Defining the criteria for judging business risk levels  
         | • Determining business risk                                    | • Criteria for judging business risk levels  
         |                                                            | • A list of business risk                             |
| 3.4     | • Defining the criteria for judging threat levels  
         | • Reviewing the classification of threats (attacking methods) | • Criteria for judging threat levels                   |
| 3.5     | • Reviewing the relation between the state of security and the vulnerability  
         | • Reviewing security items                                    |                                                            |
3. Getting Ready for Risk Assessment

3.1. Making Clear System Configurations and Data Flows

- Finding assets
- Making clear and modeling your system configuration
  - Determining the scope of assessment
  - Model your system for assessment
  - Organizing assets and their auxiliary information
  - Narrowing down the assets you should analyze (Grouping and excluding)
  - Location
  - Describing the information on the connections among assets
- Making clear data flows
  - Mapping data flows on a system configuration chart
3. Getting Ready for Risk Assessment

3.2. Determining Importance of Assets

- Importance of assets
  - One of the assessment indices in asset-based risk assessment
  - The assessment score (from 1 (lowest) to 3 (highest)) in consideration to the value of system assets, possible business risk caused by attacks, and the influence of the business continuity

[An example of defining the criteria for judging the importance of assets]

<table>
<thead>
<tr>
<th>Assessment score</th>
<th>Judgment criterion</th>
</tr>
</thead>
</table>
| 3                | • If there is an attack on assets, the system may not be running for a long period.  
                   • If assets leak information, a huge amount of loss may occur.  
                   • If there is an attack on assets, a large-scale human suffering and/or environmental damage may occur. |
| 2                | • If there is an attack on assets, the system may not be running for a certain period.  
                   • If assets leak information, a certain amount of loss may occur.  
                   • If there is an attack on assets, a middle-scale human suffering and/or environmental damage may occur. |
| 1                | • If there is an attack on assets, the system may not be running for a short period.  
                   • If assets leak information, a small amount of loss may occur.  
                   • If there is an attack on assets, a small-scale human suffering and/or environmental damage may occur. |
3. Getting Ready for Risk Assessment
3.3. Defining Business Risk and its Level

- Business risk level
  - One of the assessment indices in business risk-based risk assessment
  - The assessment score (from 1 (lowest) to 3 (highest)) in consideration to the business risk caused by threats

[An example of defining the criteria for judging business risk levels]

<table>
<thead>
<tr>
<th>Assessment score</th>
<th>Judgment criterion</th>
</tr>
</thead>
</table>
| 3                | Business damage is large.  
[Example]  
- The damage, if it happens, influences the whole system.  
- Some crucial or permanent damage may occur to the business operation of the company. |
| 2                | Business damage is medium.  
[Example]  
- The damage, if it happens, influences only a part of the system.  
- Some considerable or long-term damage may occur to the business operation of the company. |
| 1                | Business damage is small.  
[Example]  
- The damage, if it happens, influences only a minor part of the system.  
- Some medium or smaller temporary damage may occur to the business operation of the company. |
3. Getting Ready for Risk Assessment
3.3. Defining Business Risk and its Level

- **Business risk**
  - Events and situations that hinder the organization in its stable business operation and business continuity
  - Each business operator defines these based on the scope of risk and the impact on the business operation of the company at an occurrence.

<table>
<thead>
<tr>
<th>Number</th>
<th>Business risk</th>
<th>Overview of Business risk</th>
<th>Business risk level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The supply of XX is suspended in a wide area.</td>
<td>An attack on a XX production facility, XX supply facility, etc. stops the supply in a wide area, influencing the community very much, causing a large amount of loss including the cost for compensation, and degrading the trust in the company very much.</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>The supply of XX is suspended in a limited area.</td>
<td>An attack on a XX production facility, XX supply facility, etc. stops the supply in a limited area, influencing the community, causing loss including the cost for compensation, and degrading the trust in the company.</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>The supply of off-spec XX</td>
<td>An attack on a XX production facility, XX supply facility, etc. alters the system to produce and deliver off-spec XX to the customer, influencing the community, causing loss including the cost for compensation, and degrading the trust in the company.</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>Destruction of facility</td>
<td>An attack on a XX production facility, XX supply facility, etc. destroys the facility and stops the supply, causing causalities (employees and neighbors), influencing the community very much, causing a large amount of loss including the cost for compensation, and degrading the trust in the company very much.</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>Causing a large-scale cost for measures</td>
<td>A cyberattack does not cause any such risk that stops the supply of XX, but it makes clear the vulnerability of the current measures, causing a huge amount of cost for the measures for solution.</td>
<td>1</td>
</tr>
</tbody>
</table>
3. Getting Ready for Risk Assessment
3.4. Defining Threat Levels

- Threat levels
  - One of the assessment indices in two types of risk assessment
  - The assessment score (from 1 (lowest) to 3 (highest)) in consideration to the probability of the occurrences

[An example of defining the criteria for judging threat levels]

<table>
<thead>
<tr>
<th>Assessment score</th>
<th>Judgment criterion</th>
</tr>
</thead>
</table>
| 3                | The probability of occurrence is **high**.  
[Example]  
  - If *an attacker with whatever skills* attempts an attack, the probability of its success is high.  
  - *An occurrence is assumed in the near future*. |
| 2                | The probability of occurrence is **medium**.  
[Example]  
  - If *an attacker or group of attackers with a certain level of skills* attempts an attack, there is probability of its success.  
  - *An occurrence is assumed in the life cycle* of the object of an assessment system. |
| 1                | The probability of occurrence is **low**.  
[Example]  
  - If *nation-state attackers (military forces, intelligence agencies or similar bodies)* attempts an attack, there is probability of its success.  
  - *An occurrence is hardly assumable* in the life cycle of the object of an assessment system. |
# 3. Getting Ready for Risk Assessment

## 3.4. Defining Threat Levels

[Excerpts from the threats (the methods of attacks) against assets (equipment)]

<table>
<thead>
<tr>
<th>#</th>
<th>Threats (methods of attacks)</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| 1  | Unauthorized access                                                                      | To hack into a device via network                                           | • To exploit authentication information having been obtained maliciously (unauthorized login)  
• To hack into a device that does not have any authentication mechanism  
• To exploit vulnerability of a device  
• To exploit defective settings (unnecessary processes are running, unnecessary ports are open, etc.) |
| 2  | Physical intrusion                                                                       | To make an unauthorized intrusion into a restricted zone or area (any location where a device is placed etc.), or  
To unlock a device the access to which is physically limited (a device placed on a rack, in a box, etc.) | • Unauthorized intrusion into premises, an instrument room, or a server room  
• Unauthorized access to a rack or housing box |
| 3  | Unauthorized manipulation                                                                 | To directly manipulate the console of equipment etc. for intrusion and for attacking | • To exploit authentication information having been obtained maliciously (unauthorized login)  
• To hack into a device that does not have any authentication mechanism  
• To exploit vulnerability of a device |
| 4  | Erroneous operation                                                                       | To induce incorrect operation by an internal user (an employee or a business partner with privilege to access the device) for attacking  
To do an act equivalent to an attack as a result of connecting some authorized media or device to a device | • To open an attachment to mail  
• To bring in some authorized media that is infected with malware |
| 5  | Connecting unauthorized media or device                                                    | To bring in some unauthorized media or device (CD/DVD, USV device, etc.) and connect it to a device to attack | • Connecting unauthorized media  
• To import data from media or to export data into media |
| 6  | Executing unauthorized processes                                                          | To make an unauthorized execution of an authorized program, command, service, etc. on the device to attack | • Executing unauthorized programs or commands  
• Unauthorized execution of services |
| 7  | Malware infection                                                                        | To have a device infected with malware (unauthorized program) and to execute the malware to attack the device | |
| 8  | Information theft                                                                        | To steal information stored on a device (software, authentication information, information on configuration settings, encrypted keys, and/or other secret information) | • Stealing control parameters |
| 9  | Falsifying information                                                                    | To falsify information stored on a device (software, authentication information, information on configuration settings, encrypted keys, and/or other secret information) | • To falsify control programs  
• To falsify control parameters |
| 10 | Destroying information                                                                   | To destroy information saved on a device (software, authentication information, information on configuration settings, encrypted key, and/or other secret information) | • To delete control data  
• To forcefully encrypt control data |
| 11 | Unauthorized transmission                                                                 | To send unauthorized commands (to change settings, to cut off power, etc.) or unauthorized data to another device | • To execute an unauthorized control command or data transmission command  
• To falsify transmission data |
| 12 | Shutdown                                                                                  | To shutdown a device                                                       | • To execute an unauthorized shutdown command |
### 3. Getting Ready for Risk Assessment

#### 3.5. Reviewing Security Items

- **Vulnerability level**
  - One of the assessment indices in two types of risk assessment
  - The assessment score (from 1 (lowest) to 3 (highest)) in consideration to the probability of accepting an occurring threat

<table>
<thead>
<tr>
<th>Assessment score</th>
<th>Vulnerability level</th>
<th>Measures level</th>
<th>Judgment criterion</th>
</tr>
</thead>
</table>
| 3                | 1                   | 1              | **The probability of easily accepting** a threat is **high** at its occurrence. **No measures are taken for threats.** The probability of successful attacks is high. [Example]  
  - In past examples, it was confirmed that attacks making use of vulnerability occurred and was successful to cause damage. |
| 2                | 2                   | 2              | **The probability of accepting** a threat is **medium** at its occurrence. **Some measures are taken for threats but are not sufficient.** The probability of successful attacks is medium. [Example]  
  - **General measures are taken.** Whether an attack succeeds depends on the level of the attacker.  
  - In past examples, it was confirmed that attacks making use of vulnerability occurred and that no major damage was caused. |
| 1                | 3                   | 3              | **The probability of easily accepting** a threat is **low** at its occurrence. **Sufficient measures are provided for threats.** [Example]  
  - **Effective measures and multi-layered measures are provided.** The probability of successful attacks is low.  
  - In past examples, no attacks occurred that made use of vulnerability. |
3. Getting Ready for Risk Assessment
3.5. Reviewing Security Items

Measures for threats and security as well as the list of measures are provided.

[Lists of security items (47 items in total)]

[Lists of threats (methods of attacks) and the available technological or physical measures]
4. Working on Risk Assessment
4.1. Asset-based Risk Assessment

The methods of assessment in terms of the assets that compose a control system are described.
—The possible direct threats to the assets and the adequacy of the security measures are assessed.—

- With respect to the assets groups that compose the control system you should protect,
- the levels of the risk (risk value) of each of the assets are calculated from
  - Importance of assets
  - Threat level
    (The probability of threat occurrences)
  - Vulnerability level
    (The probability of accepting a threat at its occurrence)
4. Working on Risk Assessment
4.1. Asset-based Risk Assessment

- The assets that compose the control system you should protect are grouped depending on functions, types, etc.
- With respect to the assets groups:
  - Threats (methods of attacks)
  - State of security

Threats (methods of attacks)
- Unauthorized access
- Malware infection
- Falsifying information
- Suspension of functions, etc.

State of security
- Authentication of the opposite end of communication
- White list
- Authenticating operators
- Management of authority, etc.

Vulnerability level of each threat
### 4. Working on Risk Assessment

#### 4.1. Asset-based Risk Assessment

Asset-based risk assessment sheet

<table>
<thead>
<tr>
<th>Business</th>
<th>Classification of Assets</th>
<th>Target Device</th>
<th>Assessed Index</th>
<th>Threats (methods of attacks)</th>
<th>Threat Level</th>
<th>Vulnerability Level</th>
<th>Importance of Assets</th>
<th>Risk Value</th>
<th>Protection</th>
<th>Detection/Understanding Risk</th>
<th>Business Continuity</th>
<th>Asset Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Information assets</td>
<td>Data server</td>
<td></td>
<td>Malicious attack</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td>C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>3</td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
<td>C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>2</td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>2</td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>2</td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. Working on Risk Assessment
4.2. Business Risk–based Risk Assessment

The means for scenario–based detailed risk assessment are described by using an attack tree.

• Attack scenario
  – The scenarios that embody a point of attack, target and final attack that may cause a business risk an organization wants to avoid

• Attack tree
  – The steps of a series of attacks that embody an attacker, an entry point and attack path to realize an attack scenario in addition to a point of attack, target and final attack included in the attack scenario

• The levels of the risk (risk value) of each attack tree are calculated from
  – Threat level (The probability of threat occurrences)
  – Vulnerability level (The probability of accepting a threat at its occurrence)
  – Business risk level (The severity of business risk)
4. Working on Risk Assessment

4.2. Business Risk-based Risk Assessment

ATA Approach

FTA Approach

ATA: Attack Tree Analysis
FTA: Fault Tree Analysis

Main Guide
Book pp.148-231

Copyright © 2018 Information-technology Promotion Agency, Japan
### 4. Working on Risk Assessment

#### 4.2. Business Risk-based Risk Assessment

**Business Risk-Based Risk Assessment Sheet**

<table>
<thead>
<tr>
<th>Number</th>
<th>Attack scenario</th>
<th>Assessment index</th>
<th>Measures</th>
<th>Measures level</th>
<th>Attack tree number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>An unauthorized transmission of a command interrupts the supply in a wide area.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Point of intrusion = Monitoring terminal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>A malicious third party has an unauthorized access to the monitoring terminal on the information network.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>A malicious third party accesses the data historian from a monitoring terminal.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>A malicious third party accesses from the firewall to a data server.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>A malicious third party stops a wide-area supply from the PLC (master) by sending an unauthorized supply-stop command and the supply is suspended in a wide area.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>A malicious third party accesses from the firewall to a control server.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>A malicious third party stops a wide-area supply from the control server (by sending an unauthorized supply-stop command) and the supply is suspended in a wide area.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>A malicious third party accesses from the firewall to a data server.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>A malicious third party accesses the PLC (master) from the data server.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>A malicious third party stops a PLC (master) by sending an unauthorized supply-stop command and the supply is suspended in a wide area.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>A malicious third party has the monitor terminal infected with some malware.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Notes:**
- Attack scenarios are detailed in the table above.
- Measures include protective and detection steps.
- Risk assessment is based on threat level and vulnerability level.

---

**Copyright © 2018 Information-technology Promotion Agency, Japan**
5. Interpreting and Making Use of Risk Assessment

There are new steps for enhancing the security of control systems.

- Interpreting and utilizing the result of a risk assessment
  - To find the security weak points and mitigate the risk of cyberattacks, lower the risk values obtained as the result of the assessment as much as possible

- Making use of risk values
  - Understanding risk values
  - Picking up and selecting the points of improvement
  - Mitigating risks
  - Confirming the effectiveness of risk mitigation
  - Picking up and identifying test points (where to test the current measures in a security test)

- The difference in the usage and the relation between the two types of risk assessment

- Practicing continuous security measures (PDCA cycle)
6. Security Test

The secureness and the effectiveness of the state of security and the robustness against threats are verified.

- Objectives and effectiveness of security tests
  - Using actual machines to confirm the result of a risk assessment of a control system
  - Investigating the current situation of a control system

- The types, objectives, and targets of a security test

<table>
<thead>
<tr>
<th>Objectives</th>
<th>Target of test</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Network</td>
</tr>
<tr>
<td>Detecting known vulnerability</td>
<td>• Vulnerability inspection</td>
</tr>
<tr>
<td></td>
<td>(System security inspection)</td>
</tr>
<tr>
<td>Detecting zero-day vulnerability</td>
<td>• Fuzzing</td>
</tr>
<tr>
<td>Verifying the possibility of intrusion</td>
<td>• Penetration testing</td>
</tr>
<tr>
<td>Inspecting suspicious communications</td>
<td>• Packet capture test</td>
</tr>
<tr>
<td>Investigating unauthorized network devices</td>
<td>• Network discovery</td>
</tr>
<tr>
<td></td>
<td>• Wireless scanning</td>
</tr>
</tbody>
</table>
7. Additional Requirements from Security Standards

The state of the implementation of specific security measure items is confirmed and assessed further in detail.

- Selecting encryption techniques and their usage standards
- Measures for targeting type attacks
- Measures against internal threats
- Various settings on the firewall
- Security measures for external storage media

- Providing assessment items in various additional standards as a check list
  - Assessment items and security requirements
    - Setting "required" or "recommended"
  - Reference
    - Related international standards, industry standards and other referential points
  - Assumed respondent/business division (Check list for "measures for internal threat check list" only)
  - Answer column

Not limited to control systems, applicable to information systems.
Appendix

- How to use firewalls for security zone segmentation
  - Definition of firewalls
  - Classification of firewalls
  - Architecture to implement firewalls
- Check list for specific security measures
  - Check list to use encryption techniques
  - Check list for measures for targeted attacks
  - Check list for measures for internal misconducts
  - Check list for firewall configuration
  - Check list for measures for external storage media
- Control system incidents (case studies)
- Glossary
**Examples of Conducting Risk Assessment on ICS**

Security Risk Assessment Guide for ICS – Supplement

Here are examples of conducting perfect risk assessment on exemplary model systems.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>System configuration</td>
</tr>
<tr>
<td>2</td>
<td>A list of assets</td>
</tr>
<tr>
<td>3</td>
<td>Data flow chart</td>
</tr>
<tr>
<td>4</td>
<td>Criteria for judging the importance of assets</td>
</tr>
<tr>
<td>5</td>
<td>A list of the importance of assets</td>
</tr>
<tr>
<td>6</td>
<td>Criteria for judging business risk levels</td>
</tr>
<tr>
<td>7</td>
<td>A list of business risk</td>
</tr>
<tr>
<td>8</td>
<td>Criteria for judging assets levels</td>
</tr>
<tr>
<td>9</td>
<td>Asset-based risk assessment sheet</td>
</tr>
<tr>
<td>10</td>
<td>Attack scenarios</td>
</tr>
<tr>
<td>11</td>
<td>Business risk-based risk assessment sheet</td>
</tr>
<tr>
<td>12</td>
<td>Results of the risk assessment of control systems (Measures for improvement to mitigate risk)</td>
</tr>
</tbody>
</table>

Download all risk assessment sheets (Excel files) at:
https://www.ipa.go.jp/security/controlsystem/riskassessment.html
Conclusion
"Security Risk Assessment Guide for ICS"

This is a risk assessment guide for enabling the overall enhancement of control system security.

- Enhancing the understanding of risk assessment and promoting it
- Presenting specific procedures and guidance for conducting security assessment

• Explaining two types of detailed risk assessment methods
  - Asset-based, business risk-based

• Providing materials for risk assessment
  - Risk assessment sheet (formats, examples of actual cases)
  - Lists of threats (methods of attacks) and measures
  - Detailed check lists for specific security measures

• Presenting the examples of how to utilize the results of risk assessment
  - How to improve measures to mitigate risk
  - Guidance to consider security tests