IPA Better Life with IT

Guidance for Practice Regarding "IoT Safety/Security Development Guidelines"

IoT High Reliability Functions

Software Reliability Enhancement Center (SEC),
Technology Headquarters, Information-technology Promotion Agency (IPA)

Introduction

Countries around the world are taking on IoT (Internet of Things)-related initiatives, and an increasing number of corporations are placing the creation of value through interconnectivity of IoT devices and relevant systems (IoT devices and systems) as one of their major business strategies. If IoT becomes popular in a specific sector, we can expect it to spread to other sectors for increased convenience and cost reduction. However, it does not mean that the IoT-related initiatives are completed and flawless just by connecting all IoT devices and systems, sharing information, and controlling these devices and systems. It is necessary to give careful consideration to safety/security/reliability, with due deliberation given to new risks and threats that may arise from this interconnectivity. Also, when developing IoT devices and systems intended for just a specific sector, their lifespans may be shortened for several reasons, including having to redesign the IoT devices and systems, unless if there is a design or road map for future use in other sectors.

Assuming that IoT would become more popular, IPA has compiled the *IoT Safety/Security Development Guidelines* and published it in March 2016, to support the development of trustworthy products and IT systems that satisfy the safety/security/reliability standards. The *IoT Safety/Security Development Guidelines* focuses on prevention of accidents and incidents caused by the interconnectivity. Each guideline consists of "points," "description," and "example measures," and provides a comprehensive view of factors to be considered when developing products and IT systems to ensure their safety/security/reliability. We have received suggestions that specific examples are needed when developing systems based on the *IoT Safety/Security Development Guidelines*. As a result, this document provides detailed descriptions on functional levels for achieving higher reliability, regarding the technical requirements described in the *IoT Safety/Security Development Guidelines*.

This document introduces the functions that can contribute to achieving safety/security/reliability, and is intended for those who are planning to develop IoT devices and systems. Specifically, this document presents the high reliability requirements for IoT and summarizes the functional requirements and functions needed to satisfy these requirements. Examples of risk assessments regarding the coordination of IoT between different sectors are also provided in this document. The developers should be able to utilize this information when developing their own IoT devices and systems.

When using this document, do not attempt to implement all IoT high reliability functions. Instead, conduct a risk assessment of the target IoT devices and systems, select the necessary IoT high reliability functions, and then implement them. We hope this document will contribute to the safety/security/reliability of IoT.

[Word Usage in This Document]

(1) Definitions

See the table below for the definitions of terms used in this document. See *IoT Safety/Security Development Guidelines* for the definitions of terms not included in this table.

Table 1. Definitions of Terms Used in This Document

Term	Definition	Note
Safety/security/ reliability	A condition where the safety, security, and reliability of the target equipment and system are ensured.	*IoT Safety/Security Development Guidelines*
Fault	An abnormal condition that leads to degradation or loss of capability of a function that executes a request.	JIS X 0014:1999
Failure	An inability of a function to execute a request.	Same as above.
Security abnormality	A condition that is not normal caused by a fraudulent or negligent act.	
Risk assessment	A process that consists of risk identification, risk analysis, and risk evaluation.	JIS Q 31000
Erase	Files that are deleted or initialized (e.g., by formatting a USB flash drive) may be restored in some cases, but erasure is an act that renders the data completely unreadable.	
Log	A record of events that occur in a system or network.	NIST SP800-92 *Guide to Computer Security Log Management*
Log collection	A process that consists of generating, transferring, saving (storing), and discarding logs. Log analysis is part of the monitoring process.	
Trustworthiness	Whether you can trust the information or another person's act.	
Trust assurance level	Level of trustworthiness.	

(2) Abbreviations

The abbreviations used in this document are as follows:

Table 2. Abbreviations

Abbreviation	Term in full
ATM	Automatic Teller Machine
AV	Audio Visual
CSA	Cloud Security Alliance
CSMS	Cyber Security Management System
C2C-CC	CAR 2 CAR Communication Consortium
CRYPTEREC	Cryptography Research and Evaluation Committees

Abbreviation	Term in full
CRSS	CVSS based Risk Scoring System
CVSS	Common Vulnerability Scoring System
DoD	United States Department of Defense
EoL	End of Life
FIRST	Forum of Incident Response and Security Teams
GPS	Global Positioning System
GW	Gateway
HDD	Hard Disk Drive
HEMS	Home Energy Management System
IEEE	The Institute of Electrical and Electronics Engineers, Inc.
ID	Identification
IIC	Industrial Internet Consortium
IIRA	Industrial Internet Reference Architecture
I/F	Interface
IoT	Internet of Things
ISMS	Information Security Management System
JSAE	Society of Automotive Engineers of Japan
NC	Numerically Controlled
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
OWASP	Open Web Application Security Project
PKI	Public Key Infrastructure
PM	Particulate Matter
POS	Point of Sales
POST	Power on Self Test
PV	Photovoltaics
RSMA	Risk Scoring Methodology for Automotive systems
SIAT	System Invariant Analysis Technology
USB	Universal Serial Bus
VPP	Virtual Power Plant

Table of contents

Chapter 1 Background and Purpose of This Document

This chapter explains the background of why a detailed implementation guide became necessary for the *IoT Safety/Security Development Guidelines* [1], the purpose of this document, and the positioning of this document in relation to the *IoT Safety/Security Development Guidelines*.

1.1 Background

International standards and guidelines are currently being compiled in each sector for the forthcoming IoT era. As the objective of international standards and guidelines is to indicate the requirements that should be satisfied, the developers need to consider specific functions and functional layouts that would meet these requirements. In reality, however, this sort of detailed public information is rare.

If international standards and guidelines are established and IoT becomes popular in the target sector, we can expect it to spread to other sectors for increased convenience and cost reduction.

In such situations, we need a grand design, including interconnection between different sectors, creation of a road map, conception of a future-proof design, for not just when developing devices and systems based on joining of different sectors, but also for when developing them according to the standards and guidelines for a certain sector. This requires the developers to understand the need for a function (IoT high reliability function) that ensures safety/security/reliability when connecting the IoT devices and systems, and be aware of the important factors in terms of their functional requirements and functional definitions.

Among the guidelines described in the *IoT Safety/Security Development Guidelines*, this document focuses on ones that require technical actions. We expect this document to be used as a guide for identifying specific issues and considering how the issues can be resolved, not just for the engineers involved in development and operation of equipment, systems, and services that already require IoT support, but also for developers involved in development of equipment and systems that would require IoT support in the future. We hope this document will help the developers formulate a future-proof design and help strengthen global competitiveness.

1.2 Purpose of This Document

This document provides detailed descriptions on technical requirements described in the *IoT Safety/Security Development Guidelines* at the functional levels that are implementable, and is meant to be used as a guide for those working on-site. We hope this document will contribute to the safety/security/reliability of IoT.

This document provides the life cycle, functional layouts, and other factors for developers who are planning to create IoT high reliability functions, and at the same time introduces functional requirements of IoT high reliability functions and specific functions that are supported. In addition, we are hoping that setting the sights on coordination of IoT between different sectors, where IoT is expected to become popular in the near future, will lead to development of competitive IoT devices and systems with long lifespans.

The following methods are used to provide specific descriptions to the readers.

(1) Specific examples of IoT high reliability functions and functional requirements that these functions should satisfy are explained. This should help the readers understand the associations between these factors.

(2) The life cycle of IoT devices, IoT systems, and services, and functional layouts, such as edge, fog, and cloud are explained. This should provide a comprehensive image of implementations and necessary functions to the readers, and help them consider their realistic economic rationality and lifespans.

(3) The use cases that span different sectors discussed by the expert members of each sector in the working group, and specific examples of risks, threats, functional definitions, and functional layouts are included in the document. This should help the readers list expected risks and threats with regards to what they are developing and examine possible measures for these risks and threats.

1.3 Positioning of This Document

The *IoT Safety/Security Development Guidelines* summarizes the important factors that should be recognized by the developers for a safe, secure, and reliable IoT from the perspective of life cycles. The *IoT Safety/Security Development Guidelines* provides examples of measures for 17 guidelines, but does not go into details of what functions should be implemented. For events that may occur when the IoT devices and systems are actually used, this document describes the IoT high reliability requirements and functions that should be taken into consideration when designing the maintenance and operation aspects in detail and divides them into five categories. The implementation locations are also taken into consideration in this document.

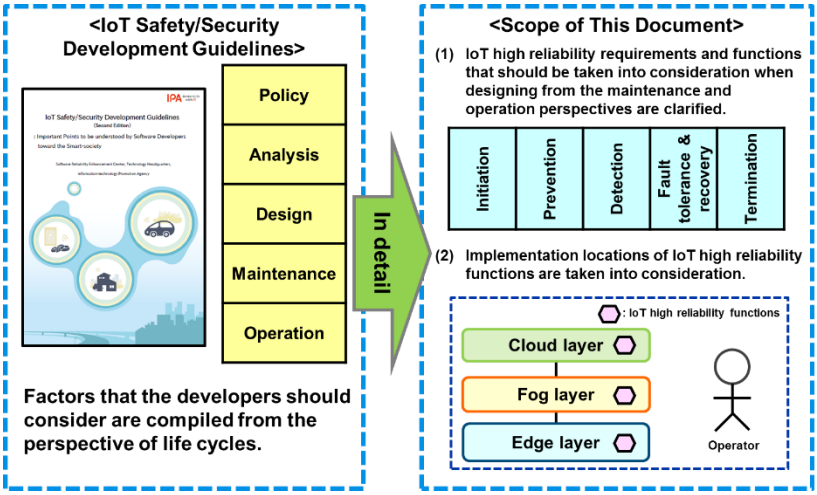


Figure 1-1. Positioning of this document

Chapter 2
Regarding High Reliability of IoT

What is necessary to make IoT more reliable is to anticipate potential threats and hazards that may arise when IoT devices and systems are connected and then introduce countermeasures for them. We are expecting to see an increasing number of cases where the IoT systems will be coordinated between different sectors, but because there are not that many cases at the present time, more considerations are necessary.

This chapter explains the threats and hazards related to IoT, based on the *IoT Safety/Security Development Guidelines*. On the assumption that the coordination of IoT between different sectors needs deep inspection, we created and analyzed five use cases. The measures are focused on the technical measures to identify the necessary functions. As conditions for identifying and selecting the necessary functions, the definitions of IoT high reliability functions are also clarified. In terms of what the developers should take into consideration for these selected functions, this chapter explains how to organize them by focusing on the aspects of maintenance and operation.

The IoT high reliability requirements described in this document are intended to be implemented mainly in software, but they can also be implemented in hardware or implemented partly with the support of an operator.

2.1 IoT High Reliability Functions

In the *IoT Safety/Security Development Guidelines*, the objects to be protected in the IoT devices and systems are classified as: IoT functions, Intrinsic functions, Information, and Others. (See 2.4.) Making just the connection function more reliable is insufficient for a highly reliable IoT. Functions including the "intrinsic" functions must be reliable as well. Otherwise, an abnormality in the section that is not reliable may cause a problem in another area. This document assumes that the IoT high reliability functions are necessary for ensuring safety/security/reliability in environments where IoT devices and systems are interconnected, and that these functions should be implemented in the IoT functions and Intrinsic functions.

■ **IoT High Reliability Function**
Functions needed to ensure safety/security/reliability in an environment where IoT devices and systems are coordinated (interconnected).

Figure 2-1 shows how the IoT high reliability functions are implemented. (See Chapter 3 for more details.)

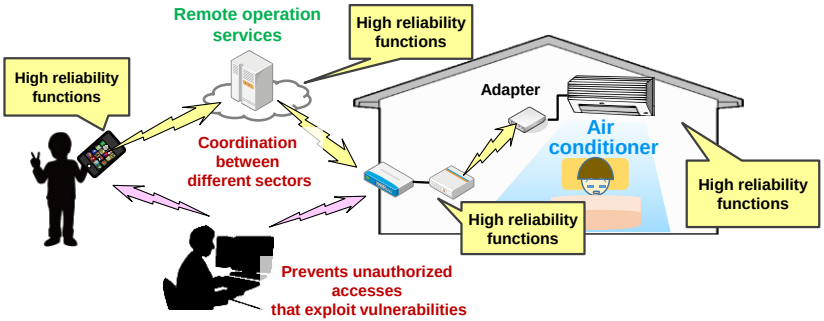


Figure 2-1. How IoT high reliability functions are implemented

2.2 Identification and Selection of IoT High Reliability Functions

The necessary IoT high reliability functions are identified and selected in the four steps shown in Figure 2-2.

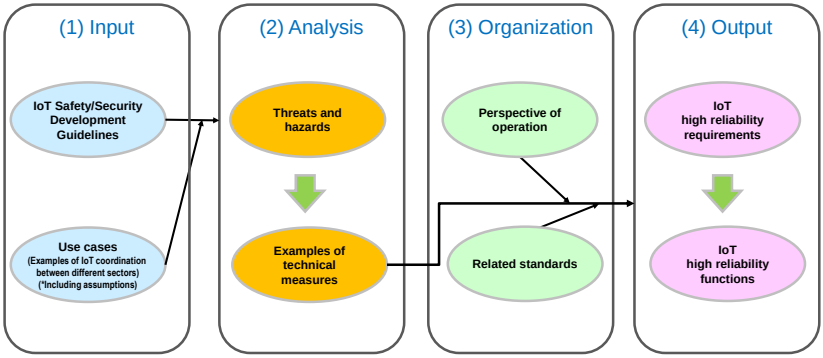


Figure 2-2. Steps to identify and select IoT high reliability functions

(1) Input

For input, in addition to the *IoT Safety/Security Development Guidelines*, the use cases (see Appendix A) of IoT coordination between different sectors, in particular, are used.

(2) Analysis

For the potential threats and hazards with regards to IoT and measures against them, an analysis is conducted based on the example measures described in the *IoT Safety/Security Development Guidelines* and use cases of IoT coordination between different sectors. See Appendix B for the potential threats, hazards, and examples of technical measures.

(3) Organization

The necessary technical measures identified as a result of analyzing the potential threats and hazards are individual threats. Thus, the situations where they are needed and the necessities of these measures are difficult to understand. The IoT high reliability functions become necessary in the maintenance and operation. As such, we organized the measures for the operation, to incorporate during the design phase, the functions that a developer would view as necessary in maintenance and operation (see 2.3).

As IoT-related standards already exist, we studied them and made sure our work does not deviate from them (see Appendix B).

(4) Output

For the selected technical measures, we compiled the IoT high reliability requirements that are based on the perspective of operation and IoT high reliability functions for satisfying these requirements (see Chapter 3).

The necessary IoT high reliability functions are selected based on the example measures included in the *IoT Safety/Security Development Guidelines* and use case analyses. The functions deemed as necessary during considerations are also included.

2.3 Analysis and Organization Regarding High Reliability of IoT

2.3.1 Basic Model Assumption

We created an assumption of an IoT basic model (IoT configuration) for analyzing the potential threats and hazards using use cases and for studying the implementation of technical measures (Figure 2-3).

This document classifies the basic model of IoT high reliability functions into three layers: Edge, Fog, and Cloud layers [2] (see Appendix A for more information on coordination). In the Edge layer, there are individual platforms where edge servers are distributed and placed near the users to shorten the distance between them, thereby reducing the data amount and distance. There is no data processing (accumulation and analysis), but real-time capabilities may be necessary in certain cases. The Fog layer is a distributed processing environment between the Cloud and Edge layers. Data processing devices are distributed and placed near the Edge layer, and its overall network structure is designed based on a unified Internet Protocol. Real-time capabilities may be necessary in certain cases. The word "Fog" is used because fog is closer to the ground than clouds. The Cloud layer conducts data processing (accumulation and analysis), and real-time capabilities may not be important.

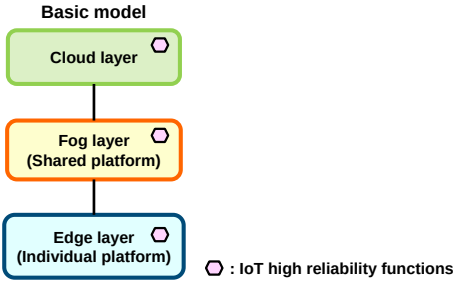


Figure 2-3. IoT basic model in this document (IoT configuration)

The IoT high-reliability functions are placed in the Edge, Fog, or Cloud layer, according to the needs of the target IoT devices and systems. For example, if a high-load function cannot be placed in the Edge layer that has less resources, we can have the Fog or Cloud layer support this function, so that the IoT high reliability functions will be incorporated as a whole.

In the IoT era, we are expected to design comprehensively, the optimum placement of the IoT high reliability functions. Should they be placed in the Edge, Fog, or Cloud layer? Coordination between automotive and home devices, coordination between industrial robots and power management, and other coordination examples are described in Appendix A. Refer to these examples as a reference for determining how the IoT high reliability functions should be placed in each situation.

2.3.2 Organization of Requirements in Terms of Maintenance and Operation

It is important to incorporate the IoT high reliability functions that are necessary in terms of maintenance and operation during the design phase. For example, the functions necessary when a system failure occurs during operation are those related to detection and recovery. These functions should be included in the design phase.

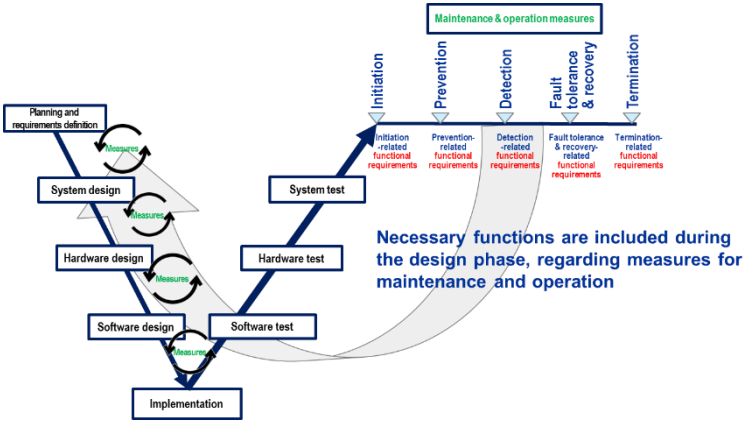


Figure 2-4. Diagram of IoT high reliability in terms of operation

To provide the IoT high reliability functions, the Prevention, Detection, and Fault tolerance & recovery measures are necessary for maintenance and operation. [3] Additional measures are also needed for the start of service, connection, end of service, and destruction, as the environments and configurations for the IoT devices and systems change constantly. Therefore, Initiation and Termination measures are added. In total, the measures are divided into five categories: Initiation, Prevention, Detection, Fault tolerance & recovery, and Termination.

(1) Initiation measures

To allow a safe, secure, and reliable connection when a service is started, we need to check when making the connection whether the initial settings match the objectives of the IoT devices and systems and whether the users are permitted to start using the service. The meaning of "Initiation" is described in section 2.3.3.

(2) Prevention measures

To prevent abnormalities during operation, we need to take preemptive actions, including grasping predictive signs of failure beforehand for stable operation of IoT devices and systems, protecting functions and assets, and running software updates.

(3) Detection measures

Early detection of abnormalities during operation requires having the functions to detect and notify the fault/failure in IoT devices and systems, security abnormalities, and conflicts. It is necessary to log the detected information for later determination of the cause of the abnormalities.

(4) Fault tolerance & recovery measures

Functions are required for minimizing the damage in the event of an abnormality in the IoT devices and systems, and for recovering from the abnormality. The fault tolerance & recovery measures can be divided into configuration information management, temporary evasion, recovery, and full-scale investigation into the cause and actions to deal with the problem.

(5) Termination measures

Functions are required for protection in case the IoT devices and systems are left unattended and for prevention of information leakage through secondhand sales or disposal. The meaning of "Termination" is described in section 2.3.3.

2.3.3 Meanings of Initiation and Termination

In the five categories, Initiation and Termination can have several meanings. This section clarifies what they mean. For example, Initiation can be when a service of a system that was developed first starts after a cutover, or when a user first starts using a service after signing a subscription agreement. Other examples are when the shared PCs in business and schools (e.g., college, etc.) are first used, or when rental cars and other IoT devices and systems that are shared among the general public are first used. The premise in this document is that there are multiple layers for Initial and Termination measures. This section will not define their exact meanings. However, please remember to consider them in multiple layers.

<Meanings of Initiation>

[1] When a service provider or user obtains a system/equipment.

[2] When a service provider or user develops a system and makes initial settings.

[3] When a user starts using a service.
(Including start of a daily service provided by a service provider.)

<Meanings of Termination>

[4] When a user terminates the use of a service.
(Including termination of a daily service provided by a service provider.)

[5] When a system is made unavailable to a service provider or user (including when a system is dismantled).

[6] When a service provider or user discards a system/equipment.

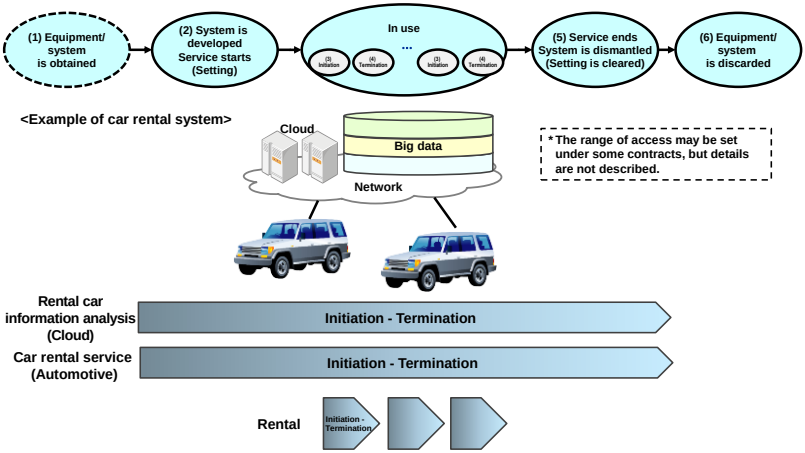


Figure 2-5. Meanings of Initiation and Termination

2.4 Utilization of IoT High Reliability Functions

The IoT high reliability functions described in this document are those that are needed to make IoT more reliable so that they will be introduced widely in each sector, assuming that these functions can be utilized across different sectors. (See Chapter 3.) We are assuming that when these IoT high reliability functions are introduced, a risk assessment is conducted for the target IoT devices and systems and the IoT high reliability functions that requires measures are selected, before they are implemented. Prior to the introduction of these functions, you need to consider and select which IoT high reliability functions are necessary, including where in the three layers of the basic model, described in 2.3.1, they should be implemented.

The details of how the functions are introduced are described in Chapter 4.

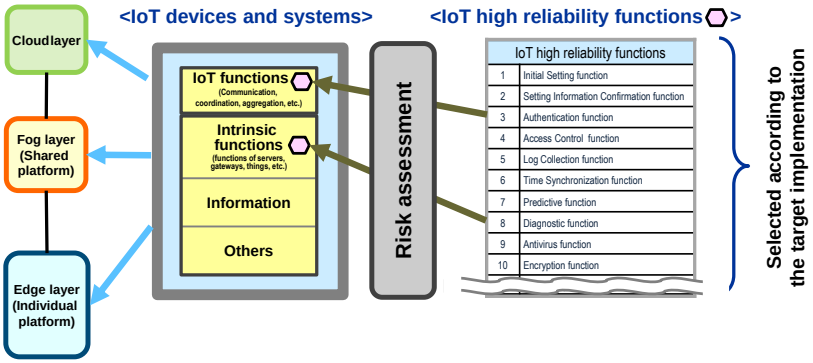


Figure 2-6. Introducing IoT high reliability functions

Chapter 3
IoT High Reliability Functions

This chapter describes in detail in the functional level the IoT high reliability requirements described in Chapter 2 in terms of maintenance and operation, functional requirements for achieving highly reliable IoT, and IoT high reliability functions that can be utilized during implementation. Other considerations regarding implementation are also described, such as wide-range spreading of faults/abnormalities, which is the characteristic of IoT, a large number of connections between users/devices, and long usage of IoT devices and systems.

The IoT high reliability function requirements should be considered when implementing IoT devices and systems. Be sure to select the necessary IoT high reliability functions.

The IoT high reliability functions described in this document are those that are deemed as the minimum necessary. More functions may be needed in the future due to technological advances or specific needs in certain areas.

3.1 IoT High Reliability Requirements and Functional Requirements

Table 3-1 shows the list of IoT reliability requirements and functional requirements and Table 3-2 shows the IoT high reliability functions. The details of IoT high reliability functional requirements are described in 3.1 and details of IoT high reliability functions are described in 3.2. In this chapter, the phrases "is necessary" and "is recommended" indicate how you should prioritize things when considering what is necessary in your situation ("is necessary" is more important than "is recommended"). Whether to implementation a measure should be determined based on the result of risk assessment.

Table 3-1. List of IoT high reliability requirements and functional requirements

IoT high reliability requirement		Functional requirement for a highly reliable IoT	Corresponding IoT high reliability function number
Initiation	[Requirement 1] Safety/security/reliability are attained when the target IoT is introduced or when the use of IoT is started.	[Functional requirement 1] Initial settings are configured properly, and are confirmed as appropriate.	1, 2
		[Functional requirement 2] Can confirm that permission is granted when beginning to use the service.	3, 4
Prevention	[Requirement 2] Abnormalities during operation can be prevented.	[Functional requirement 3] Predictive signs of abnormalities can be identified.	5, 6, 7, 8, 9
		[Functional requirement 4] Functions and assets that should be protected can be protected.	4, 5, 6, 10
		[Functional requirement 5] Preparations can be made for abnormalities.	11
Detection	[Requirement 3] Early detection of abnormalities during operation is possible.	[Functional requirement 6] Occurrences of abnormalities can be monitored and notified.	12, 13
		[Functional requirement 7] Events can be logged for identification of causes of abnormalities.	5, 6
Fault tolerance & recovery	[Requirement 4] Operation can be continued and early recovery is possible even when there is an abnormality.	[Functional requirement 8] Configurations can be identified.	14
		[Functional requirement 9] Operation can be continued even when there is an abnormality.	8, 15, 16, 17
		[Functional requirement 10] Early recovery is possible when there is an abnormality.	11, 18, 19, 20
Termination	[Requirement 5] Safety/security/reliability can be ensured even when the use of system/service is terminated or when the system/service is no longer available.	[Functional requirement 11] Use of system/service can be terminated autonomously or suspended.	18, 21, 22
		[Functional requirement 12] Data can be erased.	23

Table 3-2. List of IoT high reliability functions

IoT High Reliability function			
1	Initial Setting function	13	State Visualization function
2	Setting Information Confirmation function	14	Configuration Information Management function
3	Authentication function	15	Isolation function
4	Access Control function	16	Degenerate function
5	Log Collection function	17	Redundant Configuration function
6	Time Synchronization function	18	Suspend function
7	Predictive function	19	Recovery function
8	Diagnostic function	20	Fault Information Management function
9	Antivirus function	21	Operation Protection function
10	Encryption function	22	Lifetime Management function
11	Remote Update function	23	Erase function
12	Monitoring function		

[Requirement 1] Safety/security/reliability are attained when the target IoT is introduced or when the use of IoT is started

(1) Outline

In January 2016, a website was found that allowed users to peep into Internet-connected security cameras that had no passwords set. [4] As this case shows, information leakage may occur if the initial settings, which are related to safety/security/reliability, of equipment or system are not configured properly when deployed. Therefore, it is necessary to have a function that supports confirmation of whether the necessary settings are configured and a function that supports confirmation of whether the user is permitted to use the service or whether access to the device is permitted when the user first starts using the service.

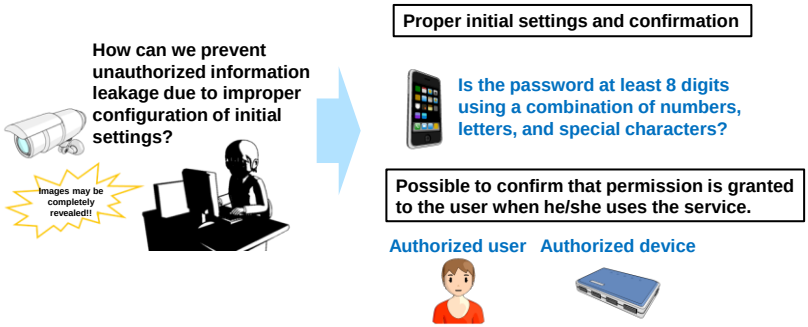


Figure 3-1. Why initial settings are necessary

(2) Required functions

[Functional requirement 1] Initial settings are configured properly, and are confirmed as appropriate.

When a system is developed or when a service is started, a function is necessary to make sure the initial settings, which are related to safety/security/reliability, are configured properly, and that they can be confirmed as correct. With IoT, a vast amount of equipment needs to be set, and it is necessary to have a notification method that considers various installation environments. It is also necessary to allow confirming of the initial settings to ensure safety/security/reliability. Furthermore, in addition to a general password setting function for administrators, it is recommended to have a function that issues a warning when initial settings of a device or system are not configured, and a function that provides current setting information for the whole system that is easy to understand.

[IoT high reliability functions] Initial Setting function(1), Setting Information Confirmation function(2)

[Functional requirement 2] Can confirm that permission is granted when beginning to use the service.

To prevent unauthorized access and data tampering, it is necessary to have a function that confirms if the user or device is authorized to use the service when the user or device makes a connection and permits its use according to the set criteria, and a function that restricts its use if the user or device is not authorized to use the service. Some examples of these functions are: Assigning IDs to each function in the devices and authenticating them (in some cases, multiple types of sensors are installed on a single device at the same time, and their IDs may be different), and using access control that limits the usage. If a high level of security is required, then it is recommended to have a PKI authentication or biometric authentication function, or a function that checks the mutual trust assurance level and determines whether to permit the connection.

[IoT high reliability functions] Authentication function(3), Access Control function(4)

(3) Implementation considerations

[1] Handling an increase in number of connected devices

The number of IoT devices are expected to increase to 50 billion in the year 2020. If the number of connected devices increases and the management table size and other management information exceed the system capacity, the performance of the service may deteriorate or the service may become uncontrollable. This could become a serious problem, in particular, if the IoT devices and systems are related to the life of a person, property, or social infrastructure. Therefore, when designing the size of the management table and other system capacity-related settings, it is necessary to consider the expected increase in the number of connected devices.

[IoT high reliability functions] Initial Setting function(1)

[2] Permission setting based on risk level

With IoT, we need to protect not just information assets, but also those that may affect the life of a person or property. Therefore, it is necessary to set the access permission based on the risk level.

[IoT high reliability functions] Authentication function(3), Access Control function(4)

[3] Considerations when a conflict can be expected

When the currently used IoT devices and systems is newly connected to a different service, and a conflict can be expected to occur with the current environment, it is necessary to consider the function for resolving the conflict. (See Requirement 3: Implementation considerations-(2))

[4] Checking trust assurance level when making connections

In addition to the Authentication function and Access Control function, it may be necessary to check the connection destination's trust assurance level and determine the scope of services based on the trust assurance level. For example, when introducing a never-before-used device in a factory line, checking the trust assurance level can help avoid adverse effects on the entire factory line. The trust assurance level can be checked when a service is started or when a new connection is made. Some examples of trust assurance level are: quality assurance level, security level, functional safety level, and information provided by an accreditation organization within the industry. Trust assurance level is also being discussed in C2C-CC. [5]

[IoT high reliability functions] Authentication function(3), Access Control function(4)

[Requirement 2] Abnormalities during operation can be prevented

(1) Outline

If there is an abnormality in the IoT devices and systems, it can be expected to spread to other IoT devices and systems that are connected. To maintain stable operation of the IoT devices and systems, it is important to predict that an abnormality may occur and to prevent it from happening. To do so, it is necessary to make assumptions on events that might be predictive signs of abnormalities, collect information necessary for identifying these signs, determine whether a measure (e.g., replacing a device) is necessary based on decision criteria, and share the results. Particularly with regard to IoT, a wide range of people, including the user, are involved. Therefore, it is necessary to consider how, when, and to whom it should be notified.

It is also necessary to identify what should be protected and guard it to prevent data tampering and information leakages.

For IoT devices and systems that are expected to be used for a long period, it is recommended to fix bugs, vulnerabilities, and other existing issues beforehand.

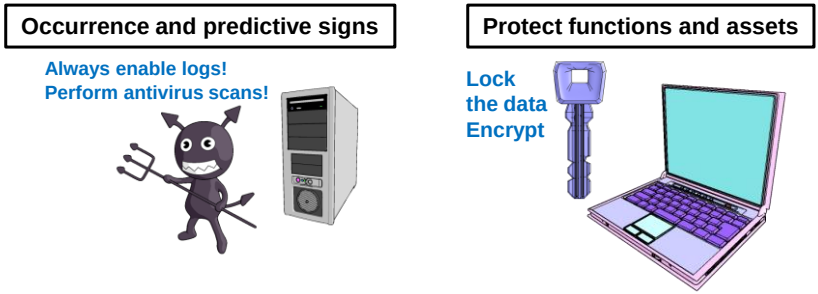


Figure 3-2. Identifying predictive signs and protecting functions and assets

(2) Required functions

[Functional requirement 3] Predictive signs of abnormalities can be identified.

It is necessary to have a function for identifying events that might be predictive signs of abnormalities, collecting and analyzing information necessary for grasping these signs, predicting abnormalities based on decision criteria, and sharing the results. Some examples of these functions are: Logging various information during operation of the IoT devices and systems, and determining whether there is hardware deterioration that may lead to failure, depletion of resources, or security abnormality, and issuing a warning before an abnormality occurs.

Other recommended functions for actively checking that the chances of abnormality occurring are not high are: Periodic diagnosis for checking the proper operation of hardware, boot diagnostics (POST) for IoT devices and systems, and Antivirus function for preventing security abnormalities.

[IoT high reliability functions] Log Collection function[5], Time Synchronization function[6], Predictive function[7], Diagnostic function[8], Antivirus function[9]

[Functional requirement 4] Functions and assets that should be protected can be protected.

Functions are necessary for identifying what should be protected from the safety and security perspectives, protecting them, and checking that they are being protected. For examples of what should be protected, the *IoT Safety/Security Development Guidelines* categorizes them into: IoT functions, Intrinsic functions, Information, and Others (cash in ATMs, products inside vending machines, etc.). Some examples of Information are: User information, images, device information, and setting information. The IoT functions are connected to networks. Therefore, examples of network protection measures are firewalls and encrypted communication. Valid measures for protecting functions and data regarding intrinsic functions and Information are: memory protection, encryption, and access restriction to information. For others, measures such as the use of physical keys and alarms when opened (tamper resistant measures) are necessary. Additionally, because the capability of checking that the subjects of protection are being protected is important, it is recommended to consider implementing this capability using the Log Collection function.

[IoT high reliability functions] Access Control function[4], Log Collection function[5], Time Synchronization function[6], Encryption function[10]

[Functional requirement 5] Preparations can be made for abnormalities.

To maintain the IoT devices and systems in a healthy state, it is necessary to deal with hardware deterioration and poor performance, existing software bugs, security vulnerabilities, and other issues as soon as possible. Hardware replacement, resource enhancement, and software updates are necessary, to solve the problems of life spans and known issues for the IoT devices and systems. It is recommended that the software update, in particular, be executed using the Remote Update function that allows you to fix the software from a remote site. As the update data itself may be tampered with, additional consideration is necessary to introduce (secure update) measures using, for example, digital signatures. It is recommended to keep track of the parts that were fixed.

Remote update is positioned as a preventive measure against abnormalities, but it can also be positioned as a recovery measure, as it is about fixing software.

[IoT high reliability functions] Remote Update function[11]

(3) Implementation considerations

[1] Actions to take when identification of predictive signs is difficult

For some IoT devices and systems, identification of predictive signs may be difficult, for example, because they are not connected at all times or the environment keeps changing (e.g., mobile environment). It is necessary to connect the IoT devices and systems periodically if they are not connected at all times, and consider several environment patterns if the environment changes constantly.

[IoT high reliability functions] Log Collection function[5]

[2] Considerations to make fixes possible

For example, fixing the IoT devices and systems may not be possible due to depletion of resources, such as insufficient memory/disk space, when vulnerability fixes are conducted repeatedly over a long period. When fixing the IoT devices and systems, it is recommended to leave some room for necessary resources (e.g., work area for bug fixes) and issue a warning before the resources are depleted.

[IoT high reliability functions] Predictive function[7], Remote Update function[11]

[3] Considerations regarding performance impact

1) Load for identifying predictive signs

Large amounts of logs, antivirus scans, and periodic diagnostics for IoT devices and systems could lead to increased workloads. It recommended to consider implementing measures such as: Setting logging intervals, scheduling antivirus scans and periodic diagnostics at periods when usages are low, and implementing a priority control measure that gradually lowers the process execution priorities.

[IoT high reliability functions] Log Collection function[5], Diagnostic function[8], Antivirus function[9]

2) Load for fixing

As remote updates can impose a high load on target devices, measures for reducing impacts on execution of intrinsic functions are necessary, similar to the measures described in 1). Additional considerations are necessary regarding the distribution method, which accommodates the increase in load on the networks used. For example, the distribution server can manage the number of target devices, controlling the number of updates sent simultaneously to prevent an overload on certain networks.

[IoT high reliability functions] Remote Update function(11)

3) Performance regarding log aggregation and predictive sign identification

For IoT devices with less resources (e.g., sensors), it may be difficult to have these devices analyze the logs. Therefore, the logs can be aggregated in an aggregation device and have it analyze the logs to identify the predictive signs of abnormalities. In this case, it is recommended to set the number of devices for identifying predictive signs and amount of logs on the aggregation device, and limit the number of predictive signs to be identified at the same time.

[IoT high reliability functions] Log Collection function(5), Predictive function(7)

[Requirement 3] Early detection of abnormalities during operation is possible

(1) Outline

IoT systems usually have complex configurations, consisting of multiple sensors and other IoT devices and providing services that link with other IoT systems. In these complex configurations, faults/failures or security abnormalities with some of the IoT devices may impact all connected systems. Thus, early detection of abnormalities and locating suspected abnormalities are vital. To do so, it is necessary to always monitor the system and collect activity logs for troubleshooting the causes of abnormalities.

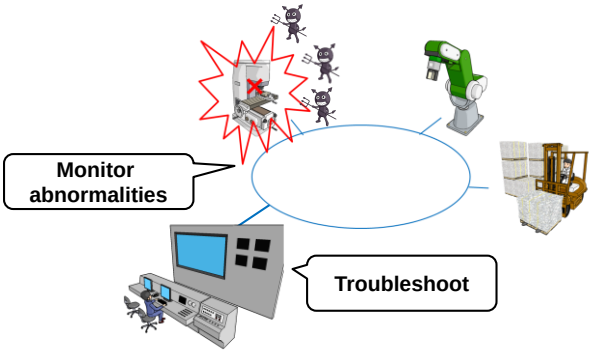


Figure 3-3. Monitoring and troubleshooting

(2) Required functions

[Functional requirement 6] Occurrences of abnormalities can be monitored and notified.

When designing the monitoring of IoT devices and systems, it is necessary to determine the capabilities of each component in the system of monitoring faults/failures and security abnormalities, and make sure the whole system is monitored thoroughly. It is also necessary to clarify what should be monitored and introduce a State Visualization function that allows you to check the status in certain sequence. When monitoring IoT devices, a function to monitor not just faults/failures and security abnormalities in IoT devices and systems, but conflicts between control functions of these IoT devices and systems also needs to be introduced. Detection of control conflicts are described below.

[IoT high reliability functions] Monitoring function[12], State Visualization function[13]

[Functional requirement 7] Events can be logged for identification of causes of abnormalities.

As many IoT devices and systems have complex configurations, logs are necessary for analyzing the faults/failures and security abnormalities. When IoT devices consist of those made by different manufacturers or when the IoT system is linked with other systems in different sectors, analyzing the failure when a fault/failure or security abnormality occurs may be difficult. Therefore, a logging function is necessary to prove that there is no problem with the IoT devices and systems in your company. As the log data itself may be tampered with, it is also necessary to introduce protection measures, such as encrypting log data.

Because a wide array of IoT devices may be connected in an IoT system, there may be cases where the timestamps in logs do not match due to inconsistent clock settings on the IoT devices, making the log analysis impossible. Thus, it is necessary to have a function for time synchronization.

[IoT high reliability functions] Log Collection function(5), Time Synchronization function(6)

(3) Implementation considerations

[1] When individual abnormality detection is not possible

For example, when many sensors are connected in a system, monitoring of individual sensor for failure can be challenging. In such a case, it may be possible to guess a sensor abnormality by comparing sensor values sent from multiple sensors and look for outliers (values that are way off from others in statistics). As such, if IoT device abnormalities cannot be detected individually, values other than abnormality information and other information to guess the existence of abnormalities.

[IoT high reliability functions] Monitoring function(12)

[2] Considerations regarding conflicts

With IoT, there may be a case where various services are linked in a complex configuration, and IoT devices and systems may receive conflicting instructions at the same time from multiple services. In a house, for example, the "Comfort" service may send an instruction to open the windows because the temperature has risen, while the "Home Security" service may send an instruction to close the windows, thereby creating a conflicting situation. The key is being able to detect a conflict. Examples of conflicting situations include not just when there are multiple valid instructions, but also when there is a single invalid instruction.

Measures to take when a conflict is detected can be divided into user's judgment and automatic judgment. For the automatic judgment, priority control based on scenarios that consider the environment condition may be valid.

[IoT high reliability functions] Monitoring function[12]

[3] Analyzing security attacks

It is necessary to give considerations to checking login failures using administration privileges (IDs) and the number of attacks, and issuing warnings when abnormal values are detected.

[IoT high reliability functions] Monitoring function[12]

[4] Checking changes in IoT configuration

It is necessary to give considerations to checking unexpected installation, connection, and losing of IoT devices and systems, and issuing warnings.

[IoT high reliability functions] Monitoring function[12], Configuration Information Management function[14]

[5] Measures regarding false positives

To prevent the system from stopping by mistake due to a false positive detection of abnormal event regarding important data, it may be better to combine data when detecting abnormalities. However, because combining data from all available information and analyzing it can lead to higher cost, one possible solution is to focus on detecting abnormalities in important data.

[IoT high reliability functions] Monitoring function[12]

[6] When there are large amounts or many types of logs

When the IoT devices consist of those made by different manufacturers, you may not be able to analyze the logs because there are no logs, even when they are necessary to determine the causes of abnormalities. Log designs require determining what kind of logs are necessary for what purpose, and considering which log collection method ensures that the necessary logs do not get deleted. When there are many devices from which the logs are collected, you might run out of space for storing these logs. In such a case, it is recommended to rotate the logs or specifically select and store important information, such as the latest failure information. When there are many types of logs, it is recommended to make sure the important ones, such as failure and security abnormality logs, are saved. The failure logs can be compressed if the same event occurs frequently. In some cases, the information that cannot be acquired from the target device or system can be acquired from the other devices or connected systems.

[IoT high reliability functions] Log Collection function[5]

[Requirement 4] Operation can be continued and early recovery is possible even when there is an abnormality

(1) Outline

Some IoT devices and systems are used in traffic monitoring systems, disaster monitoring systems, and other social infrastructure systems, and a high system operation rate may be required in these cases. If the IoT devices and systems fail, measures are necessary for continuing the system operation and measures for recovering from severe failures, including system outage. Measures for preventing the damage from spreading to other connected IoT devices and systems are also necessary. Examples of measures for continuing the system operation include: Switchover, degeneration, or isolation of the failed section and network isolation. Examples of recovery measures include: Resetting, rebooting, recovering data on, and rolling back the settings and data on target devices and systems. As the system configuration of IoT systems tends to change frequently, it is necessary to grasp the latest system configuration.

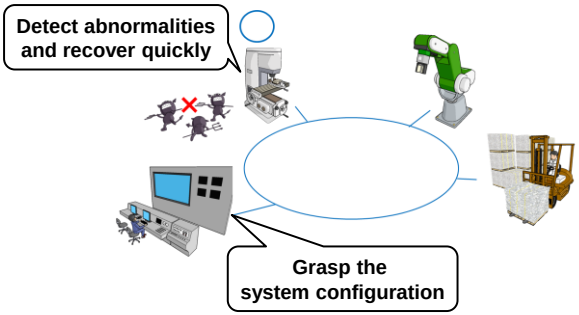


Figure 3-4. Detection and early recovery

(2) Required functions

[Functional requirement 8] Configurations can be identified.

IoT systems can be expected to change on a daily basis. Therefore, it is necessary to manage the configuration information to enable the continuation of system processing when a failure occurs, by switching over or degenerating, or to recover from the abnormality (including automatic recovery) and do a root cause analysis. Managing the connection information requires managing the types, versions, connection information, and state information of the hardware and software in the system. Particularly in a system where many IoT devices are

connected or in an autonomous decentralized system, it is recommended to be able to acquire the configuration information automatically and periodically.

[IoT high reliability functions] Configuration Information Management function[14]

[Functional requirement 9] Operation can be continued even when there is an abnormality.

It is necessary to have functions for continuing the processes by separating parts of the IoT devices and functions or isolating the application or IoT devices where the security abnormality occurred. Critical systems must be secure against faults and failures. Therefore, it is necessary for these systems to have the functions for continuing the processes by employing redundant configurations. It is recommended to periodically check the operation of functions and devices that are not used normally. The examples of this are standby functions and devices in a redundant configuration.

[IoT high reliability functions] Diagnostic function[8], Isolation function[15], Degenerate function[16], Redundant Configuration function[17]

[Functional requirement 10] Early recovery is possible when there is an abnormality.

If a failure occurs and continuing the processes is difficult, it is necessary to have functions to automatically stop the target IoT devices and systems, manually stop or use a monitoring server to stop the target IoT devices and systems, and separate them from the network. Quick recovery is required if the IoT devices and systems stop or if they are separated from the network. Functions for rebooting and reconnecting to the network are necessary for the recovery. For IoT devices and systems in remote locations, it is recommended to be able to reconnect them with remote operation. Additionally, it is recommended to have a function for checking if the data is corrupted and a function for rolling back the data as necessary. It is necessary to have a function for backing up important information about the failure, prior to performing the recovery, to be able to determine the cause of the failure.

In addition to these temporary measures, another function is necessary to fix the software, through remote update or other means, if a bug is found in the software as a result of the root cause analysis.

[IoT high reliability functions] Remote Update function[11], Suspend function[18], Recovery function[19], Fault Information Management function[20]

(3) Implementation considerations

[1] Handling changes in configuration information

The configuration of IoT systems is likely to change and it may be difficult to grasp the configuration information in some cases. Thus, it is necessary to consider using a function that allows you to not just manage the configuration information statically, but also manage the information dynamically.

[IoT high reliability functions] Configuration Information Management function(14)

[2] Considerations regarding degenerate operation

As there are many people involved in IoT systems, including multiple vendors, system developers, and service providers, information sharing between these parties is important during degenerate operation or recovery from the degenerate operation. Thus, it is recommended to consider introducing a mechanism for communicating to others when the system is in the degenerate operation mode. It is also recommended to give similar consideration to situations when recovering from the degenerate operation.

[IoT high reliability functions] Degenerate function(16)

[3] Considerations pertaining to synchronization checks during recovery

During recovery, it is necessary to not just launch the systems and applications, but also execute many other processes, including data recovery and user state recovery. In some cases, considerations must be given to synchronization of launch order and data integrity. For example, if there is a large-scale failure in a system with many IoT devices and it needs to be recovered starting from powering on the system, the power-on procedure may fail when many devices are turned on at the same time and the power required exceeds the available power supply capacity. It is recommended to estimate the power supply capacity, and power on the devices in a certain order and group.

[IoT high reliability functions] Recovery function(19)

[4] When the recovery partially fails

When recovering an IoT system and there are many relevant IoT devices, some of these devices may not start up properly. When a recovery is completed, it is necessary to check that all managed IoT devices start up properly and that they are usable. If the system is linked with another system, it is recommended to check that the systems are linked properly from both sides.

[IoT high reliability functions] Recovery function(19)

[Requirement 5] Safety/security/reliability can be ensured even when the use of system/service is terminated or when the system/service is no longer available

(1) Outline

When a user terminates the use of a service, the user may forget to give a proper termination instruction. In such a case, accidents or information leakage may occur, due to oversight regarding operable devices and theft. Therefore, it is necessary to make the proper termination procedure easy to remember for the users and make sure security is maintained even when they forget the procedure and the IoT devices and systems are left unattended in operable condition.

In cases where users change frequently, for example when there are shared terminals, security abnormalities may occur if IDs, passwords, and other settings and information are left stored in the devices. Thus, it is necessary to have a measure that decides which information should be erased, to ensure the information is erased. When the IoT system is dismantled and the IoT devices are handed down for secondhand sales or to a disposal company, there is a risk of information leakage. A measure is necessary for completely erasing stored information.

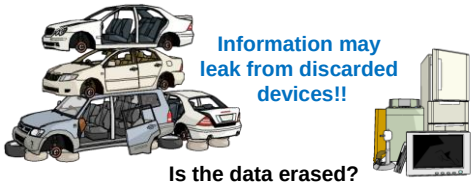


Figure 3-5. Why data erasure is necessary

(2) Required functions

[Functional requirement 11] Use of system/service can be terminated autonomously or suspended.

The IoT devices and systems are likely to be operated remotely, and they may remain operable even when the user exits, due to an operation mistake or communication error. For example, an air conditioner unit might be kept powered on. Smartphones can be operated improperly by a third person, if they are misplaced or stolen. To prevent these incidents, it is necessary to have a function to exit autonomously when a device is left operable for a long period and an operation protection (e.g., remote lock) function to make a device unusable

temporarily if the device is misplaced or stolen. Additionally, it is recommended to have a function to notify the usage time of the IoT devices and systems or end of operation time.

[IoT high reliability functions] Suspend function(18), Operation Protection function (21), Lifetime Management function(22)

[Functional requirement 12] Data can be erased.

IoT may be used as second-hand mobile devices or shared with other users. Because the user changes in these cases, for example car rentals, the information in the device needs to be erased when the user ends its use. Also, if a user stops using an IoT service or decides to dispose of an IoT device, the stored information needs to be erased.

[IoT high reliability functions] Erase function(23)

(3) Implementation considerations

[1] Considerations regarding unconditional implementation of autonomous termination/suspension

Autonomous termination and suspension are useful in maintaining safety, but they can also have the opposite effect. Thus, a function is necessary for setting the conditions.

[IoT high reliability functions] Suspend function(18)

[2] Complete data erasure

Data could in some cases be recovered, even when the settings are initialized or when the data is deleted. For example, normal deletion of data in HDD only clears the file allocation table. Because data recovery is still possible, a function is necessary to erase data based on how the IoT devices are used, such as random overwriting of data. Regarding data erasure, the locations and information leakage risks also needs to be taken into consideration.

[IoT high reliability functions] Erase function(23)

[3] Considerations regarding usage time and operation time

The IoT devices and systems consist of various sensors, and because their numbers may increase or decrease daily and they have long life cycles, lifetime management can be cumbersome. To solve this problem, a function is necessary to have the IoT devices perform lifetime management on their own, including the usage time and operation time, and notify the users of their lifetime information.

[IoT high reliability functions] Lifetime Management function(22)

3.2 IoT High Reliability Functions

This section provides the descriptions regarding IoT high reliability functions that can be used to satisfy the IoT high reliability functional requirements. (See Table 3-2 above for the whole list.)

(1) Initial Setting function

Purpose	To configure the necessary settings when developing/connecting a system or starting to use a system.
Description	The Initial Setting function has the following features: • Range settings of various information. • Password settings for administration privilege and user permission (Including a Help function that encourages changing the default password and using stronger passwords.) • Access control settings • Closing/stopping unnecessary ports and services • Software update settings • Trust assurance level information settings The system cannot be used unless these settings are configured.
Reference	

(2) Setting Information Confirmation function

Purpose	To check the device/system settings.
Description	The Setting Information Confirmation function has the following features: • Warn if the initial settings of devices and systems are not configured properly when the system is developed/connected or when the use of the system is started. • Provides easy-to-understand checking capability regarding the settings in the whole system.
Reference	

(3) Authentication function

Purpose	To uniquely identify users and devices and check their identities.
Description	The following authentication methods are used with this function: • Prevention of spoofing connected IoT devices. - IoT device identifier authentication - Client certificate authentication - Message authentication • Prevention of spoofing users - ID & password authentication - Possession-based authentication (e.g., smart cards) - Biometric authentication • Prevention of spoofing connected systems/services - Mutual authentication with connected systems/services, using keys and digital certificates There are also other methods, such as multi-factor authentication, which combines the above methods. There is also a function to lock the authentication capability, when the authentication failures exceed a certain threshold.
Reference	• IoT Security Guidelines (IoT Acceleration Consortium) http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf • Security Guidance for Early Adopters of the Internet of Things (IoT) (CSA) https://www.cloudsecurityalliance.jp/newsite/wp-content/uploads/2016/02/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things_J_160224.pdf • Guidebook for e-Government recommended ciphers (CRYPTREC) http://www.cryptrec.go.jp/report/c07_guide_final.pdf

(4) Access Control function

Purpose	To restrict access to the objects to be protected, and protect these objects.
Description	The Access Control function allows or denies access to the objects to be protected, based on the ID used in the authentication process. The following access control methods are used: • Discretionary access control (DAC) • Mandatory access control (MAC) • Role-based access control (RBAC)
Reference	

(5) Log Collection function

Purpose	To accumulate event information to allow tracking of events that occurred on the devices and systems possible.
Description	The Log Collection function has the following features: • Logging records related to certain events. • Transferring logs securely to other devices when there are low-resource IoT devices. • Saving logs - If available resources are low, the logs can be saved by rotating them or backing them up to prevent loss of log data. - Some examples of ways to protect logs are: Access control, encryption, and allowing only the appending of logs. • Discarding unnecessary logs Examples of events to be recorded • For security analysis: Attacks, user authentication, data access, configuration management information updates, execution of application, starting/stopping of logs, communication, opening/closing of door, checksum, and move history. • For safety analysis: Failure information (hardware and software) • For reliability analysis: Results information, status information, operating environment information (temperature, humidity, CPU load, network load, resource usage, etc.), and software updates.
Reference	SP800-92 Guide to Computer Security Log Management (NIST) http://www.ipa.go.jp/files/000025363.pdf

(6) Time Synchronization function

Purpose	To synchronize the time settings between devices and systems.
Description	There are two ways to synchronize the time settings: Setting the time based on absolute time, which is used as the reference time, and setting the time relatively between the connected devices and systems to prevent having time setting differences. • Setting the time based on absolute time - NTP with an accuracy of about 10ms. • Setting the time relatively - PTP (IEEE1588) with an accuracy of 1μs. - TSF (IEEE 802.11) for time synchronization in wireless LANs
Reference	- NTP http://www.ntp.org/ - IEEE 1588 PTP (Precision Time Protocol) - IEEE 802.11 TSF (Timing Synchronization Function) - IEEE 802.1 TSN（Time Sensitive Networking） - IEEE 802.15.4 Time-slotted communication model These documents can be purchased at https://standards.ieee.org/

(7) Predictive function

Purpose	To predict abnormalities that may occur in the near future and encourage taking action even when the indicators are still within the normal range.
Description	The events that should be identified as signs of abnormalities are defined, necessary information is acquired and analyzed, and occurrence of abnormality is predicted and notified based on decision criteria. Machine learning and other methods are used for the prediction. For example, the following conditions are checked: • Changes in trend of cyclic activities. • Changes in trend of state transitions • Changes in relationship between multiple conditions that have strong correlation.
Reference	• Real-time Monitoring Solution to Detect Symptoms of System Anomalies (http://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol52-4/paper04.pdf) • Power Plant Fault Sign Monitoring Solution Based on System Invariant Analysis Technology (SIAT) http://jpn.nec.com/techrep/journal/g14/n01/pdf/140126.pdf

(8) Diagnostic function

Purpose	To use tests and other methods to actively check that the chances of any abnormality occurring are not high.
Description	The Diagnostic function has the following features: • Boot analysis that launches a device or system before the device or system is online, and checks that the hardware is functioning properly. • Periodic diagnosis that periodically checks the proper operation after the device or system is online. Diagnosis of parts that are not used normally, such as those in redundant configurations, should also be considered.
Reference	Approaches for Embedded System Information Security (IPA) http://www.ipa.go.jp/files/000013968.pdf

(9) Antivirus function

Purpose	To prevent damage caused by virus infections.
Description	Antivirus measures consist of detection (including detection of intrusion, execution, and hiding) and removal. The following methods are used for detection: • Whitelisting - With low-resource IoT devices, you can allow just the whitelisted software to be executed to prevent execution of unknown computer viruses. • Blacklisting - Antiviruses use pattern files that contain signatures of known computer viruses to detect intrusion, execution, and hiding of computer viruses. Use of blacklisting may be difficult with low-resource IoT devices.
Reference	What is "Antivirus Whitelisting"? A Device Protection Technique for Control Systems http://monoist.atmarkit.co.jp/mn/articles/1404/07/news004.html

(10) Encryption function

Purpose	To use encryption technologies to encrypt or digitally sign data stored in devices and systems and data transmitted over networks.
Description	The details of the encryption function are described in the reference documents below. When encrypting, it is necessary to use secure encryption algorithms, proper key lengths, and proper key management. Lightweight cryptography, which can be used in devices with limited resources, is also available. The Encryption function can also be used for authentication and tampering detection.
Reference	• Security Design Guide for IoT Development (IPA) https://www.ipa.go.jp/files/000052459.pdf • Guidebook for e-Government recommended ciphers (CRYPTREC) http://www.cryptrec.go.jp/report/c07_guide_final.pdf • Cryptographic Techniques Study WG (Lightweight Cryptography) Report https://www.cryptrec.go.jp/estimation/techrep_id2406.pdf

(11) Remote Update function

Purpose	To update software from a remote location and fix software bugs and vulnerabilities.
Description	The Remote Update function has the following features: • Encrypt or digitally sign update files. • Keep track of parts that were fixed (Log Collection function). • Schedule updates. • Set update priorities. • Update the version, or downgrade the version if the update fails. Not all software updates are executed remotely, but IoT devices and systems are expected to require maintenance in remote locations. This is the reason for the focus on the Remote Update function.
Reference	

(12) Monitoring function

Purpose	To detect abnormalities in devices and systems.
Description	The Monitoring function has the following features: • Detection of abnormalities - Detection of faults/failures (including log analysis function). - Detection of security abnormalities (Including log analysis function). - Detection of control conflicts. • Notification of detected abnormalities
Reference	

(13) State Visualization function

Purpose	To display the operation status of devices and systems.
Description	The State Visualization function has the following features: • Display the latest operation status. • Display the time line of operation status. * This function is considered as part of the Monitoring function in some cases.
Reference	

(14) Configuration Information Management function

Purpose	To manage the components of devices and systems.
Description	The Configuration Information Management function manages the following information: • Hardware type and version. • Software type and version. • Update status of certificates for devices in the systems. • Connection information (Network configuration, power supply, etc.). • Enabled/disabled status and other information.
Reference	Technical Reference Model (TRM), Chapter 5. Descriptions of Technological Domain (IPA) https://www.ipa.go.jp/files/000025495.pdf

(15)Isolation function

Purpose	To isolate applications or devices/systems in the location where an abnormality occurred from other applications and devices/systems that have no problems.
Description	The Isolation function has the following features: • Isolation of applications - An application is isolated and its execution is prevented if a virus infection is detected. (See the Antivirus function section.) • Isolation of devices/systems - Devices are separated when they do not follow the Security Policy or when an abnormality is detected, and the relevant network is quarantined in some cases.
Reference	Methods to Create Quarantine Networks (Nikkei BP) http://itpro.nikkeibp.co.jp/article/lecture/20070522/271750/

(16)Degenerate function

Purpose	To prevent system operation from completely stopping, even if there is a failure in parts of the system, by limiting their functions and performance.
Description	The Degenerate function has the following features: • In a system composed of multiple devices, the processes are continued even if one of these devices fails, by separating the failed device. - For example, when many sensors are connected in a system, a sensor is separated if it is deemed as abnormal. • Processes are continued even by resorting to limiting the performance - For example, if the network performance deteriorates, the network mode is switched automatically to low-speed mode, to allow the network communication to continue.
Reference	Research Regarding Measures to Improve the Safety of Internet Servers (IPA) https://www.ipa.go.jp/security/fy14/contents/high-availability/guide.html

(17)Redundant Configuration function

Purpose	To maintain the overall functional and performance level even if a failure occurs in a device or system, by preparing multiple systems or devices in the system.
Description	The Redundant Configuration function has the following features: • Configure a certain function not with a single device, but with multiple devices, including standby devices. • Make a decision to switch to using standby devices when there is an abnormality. • Changeover to standby devices. • Revert back to the original devices.
Reference	Research Regarding Measures to Improve the Safety of Internet Servers (IPA) https://www.ipa.go.jp/security/fy14/contents/high-availability/guide.html

(18)Suspend function

Purpose	To stop the devices and systems if continuation of processing is dangerous due to existence of unattended devices/systems or if continuation of processing is difficult due to an abnormality.
Description	The Suspend function has the following features: • Autonomous suspension - Autonomous suspension of devices/systems under certain conditions if the devices/systems should have been stopped but were not. • Suspension by a person or from a monitoring device (Including sending Suspend instructions remotely) - Forced suspension when there is a security abnormality or fault/failure.
Reference	

(19)Recovery function

Purpose	To recover the devices/systems so that processing can be continued, when an abnormality occurs and processing cannot be continued.
Description	The Recovery function has the following features: • Reboot - Rebooting by a device/system or rebooting of devices/systems by a person or from a monitoring device. • Network reconnection • Data rollback - Recovering of data at a certain point in the past when the device/system was working properly.
Reference	

(20)Fault Information Management function

Purpose	To collect and manage information necessary for analyzing a failure.
Description	The Fault Information Management function has the following features: • Map failure type information and information collected when a failure occurred. • Back up failure information regarding devices/systems when a failure occurs. - If rebooting is necessary after the failure, failure information should be backed up to a non-volatile memory space and collected after rebooting, assuming that rebooting has higher priority than the analysis. • Manage failure history.
Reference	Technical Reference Model (TRM), Chapter 5. Descriptions of Technological Domain (IPA) https://www.ipa.go.jp/files/000025495.pdf

(21) Operation Protection function

Purpose	To prevent devices/systems from being operated, if they are misplaced or stolen and there are risks of improper operation.
Description	The Operation Protection function has the following features: • Locking/unlocking the operation - The device/system is locked autonomously, or the device/system is locked by a person or from a monitoring device. - The device/system is locked through direct operation or locked remotely. - Unlocking of the above locks. • Obfuscation - Display information and other information are made unclear or difficult to understand by anyone other than the user.
Reference	Security Design Guide for IoT Development (IPA) https://www.ipa.go.jp/files/000052459.pdf

(22) Lifetime Management function

Purpose	To prevent use of devices/systems past their intended operation hours period or lifetime.
Description	The Lifetime Management function has the following features: • Operation hours management - Management of cumulative operation hours for preventing use that exceeds maximum operation hours. • Lifetime management - Management of keeping track of warranty periods set by the manufacturers. • Advance notice of EOL - Notice sent prior to the cumulative operation time reaching its maximum or end of lifetime date. * This applies to both the hardware and software.
Reference	

(23)Erase function

Purpose	To prevent the information from leaking when devices or systems are discarded.
Description	Files that are deleted or initialized (e.g., formatting USB flash drive) may be restored in some cases, using special methods. The act of erasing, in this case, pertains to making the data completely unreadable. The Erase function erases the setting information and saved data. The Erase function needs to completely erase information that was magnetically saved, and the following erasing methods are available: • NSA method • DoD method • Peter Gutmann method
Reference	• NSA/CSS Policy manual 9-12 https://www.nsa.gov/resources/everyone/media-destruction/assets/files/storage-device-declassification-manual.pdf • DoD 5220.22-M http://www.dss.mil/documents/odaa/nispom2006-5220.pdf • Secure Deletion of Data from Magnetic and Solid-State Memory https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

<Column 1> Healthcare and IoT

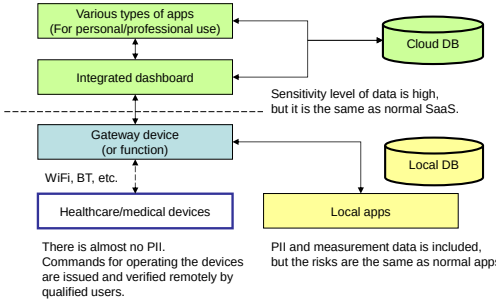
Hiroyuki Kazuma, Japan Electronics and Information Technology Industries Association

[Let's Think About Wearable Healthcare Devices]

Healthcare is a broad term for looking after medical and health aspects. But in Japan, there is a big difference in restrictions imposed on medical devices and healthcare devices. In this column, I would like to talk about IoT for healthcare devices and services that are easy to imagine.

When we talk about IoT for healthcare, the first thing that may come to your mind is probably a wearable healthcare device. These wristband-type devices have the function to measure your amount of activity, number of steps you took, activity patterns, and sleep. With some of these devices with no display function, the measured data is sent to a smartphone or other devices and is managed on an app. If we widen the definition of the term "healthcare device" to include devices that send measured data to smartphones/PCs for management, then we can add blood pressure monitors, body composition monitors, thermometers, and other familiar devices to this mix. There may be a dedicated app that manages this data, but in most cases, there are applications that manage all the data sent from these different devices. One caveat for this type of management is that the data sent from these devices may be sent or saved in unexpected places. Personally identifiable information is rarely saved inside these devices. Therefore, the risk of leakage of private information is low, even though transmission mistakes and data loss caused by attempting to correct the mistake can happen.

Next, let's consider how this integrated data will be used. In a common IoT environment, the aggregated data is automatically analyzed and usually used for some type of feedback. However, in the healthcare field, the situation is slightly different. Because of the complexity of human beings, regarding the person who is the target of the feedback, and restrictions due to not being regarded as a medical procedure as defined in the Medical Practitioner's Law, the mainstream applications are to stop at the analysis stage or issue various control commands after the data is checked by a qualified person. This line of thinking can be observed also in places where health guidance, which is close to medical guidance, is provided and in systems for preventing severity of patients with chronic diseases.

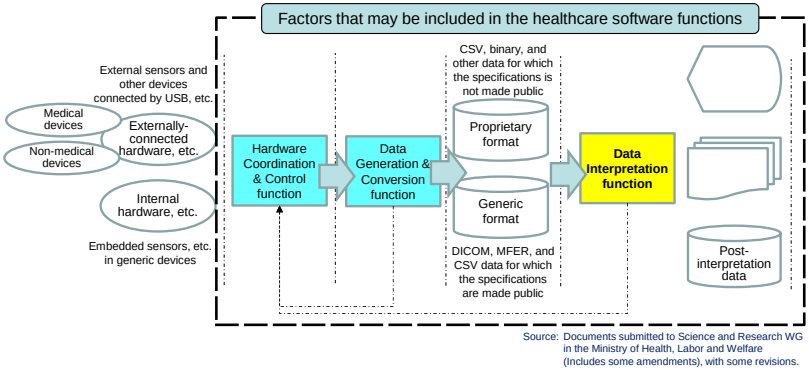


Management of Healthcare Data

[Expected Risks]

Software used on smartphones/PCs in conjunction with healthcare devices is called healthcare software. Healthcare software mainly consists of three functions: Hardware Coordination & Control function, Data Generation & Conversion function, and Data Interpretation function. Data Interpretation is the most valuable function in this software, but risks can be identified in each of these functions as shown below.

Hardware Coordination & Control function	- An incorrect instruction may be issued to a sensor (e.g., medical device). - An instruction issued to a medical device may affect the main function of the device.
Data Generation & Conversion function	- Information sent from a sensor may degrade when data is generated, and cause an error in the interpretation in the next step. - Data loss may occur. (Except when there is a special instruction.)
Data Interpretation function	- Interpretation results may have medical implications. - It may have a negative effect when a message based on an interpretation result is sent to a user (patient).



Source: Documents submitted to Science and Research WG in the Ministry of Health, Labor and Welfare (Includes some amendments), with some revisions.

Functions of Healthcare Software

Chapter 4
Applying IoT High Reliability Functions

Chapter 3 summarized requirements and functions a highly reliable IoT. This chapter describes how these IoT high reliability requirements and IoT high reliability functions can be applied when IoT devices and systems are developed. This consists of the four steps below.

(1) Mapping the IoT devices and systems to be developed to the basic model (see Figure 2-3)

(2) Risk assessment

(3) Determining measures against risks

(4) Measures using IoT high reliability functions

4.1 Procedure of Application to IoT Devices and Systems

4.1.1 Mapping the IoT Devices and Systems to be Developed to the Basic Model

This document is based on the assumption of using the basic model described in Figure 2-3, which consists of three layers: Cloud, Fog, and Edge. When applying the IoT high reliability functions to the IoT devices and systems, it is necessary to map these IoT devices and systems to be developed to the basic model, as determining which layers these functions are implemented to become important.

4.1.2 Risk assessment

A risk assessment needs to be conducted from the safety and security perspectives, for the IoT devices and systems mapped to the basic model in section 4.1.1. Figure 4-1 shows the risk assessment procedure (From *Identification of the objects to be protected* to *Risk evaluation*) described in the *IoT Safety/Security Development Guidelines*.

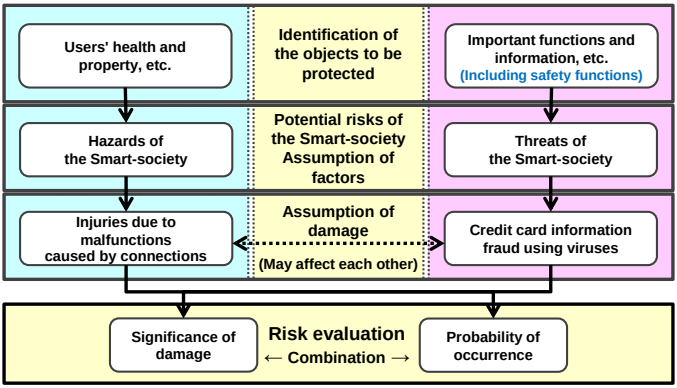


Figure 4-1. Risk assessment procedure

(1) Identification of the objects to be protected

Use Guideline 4 in *IoT Safety/Security Development Guidelines* as a reference to identify the objects to be protected. The examples of objects to be protected are those described in Guideline 4 and examples described in Appendix A (use case analysis that goes into the details of Guideline 4).

(2) Potential risks of the Smart-society and assumption of damage

Use Guidelines 5 through 7 in *IoT Safety/Security Development Guidelines* as a reference to identify the potential risks in the Smart-society, risks that may spread

because of the connections in the Smart-society, and physical risks. Use the basic model and the configuration of IoT devices and systems in *IoT Safety/Security Development Guidelines* as references to identify the applicable coordination model, connection method, target devices and systems, and risks.

When identifying risks, you need to take various usage environments and methods into consideration. For example, you need to assume that the devices and system may be installed on an island or in a remote area, where it is difficult to visit and maintain them.

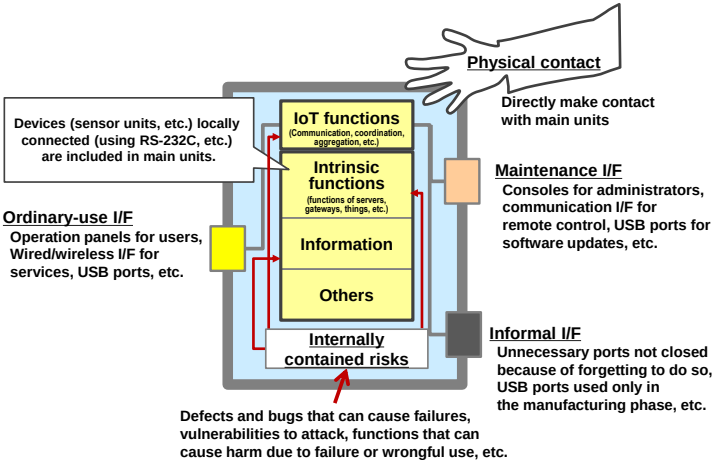


Figure 4-2. Examples of risk locations

(3) Risk evaluation

Evaluate the identified risks from the perspectives of scale of damage and probability of occurrence. For more information on risk evaluation, see Column 2.

The *IoT Safety/Security Design Tutorial* may be helpful in terms of specific hazard analysis and threat analysis methods. [6]

4.1.3 Determining Measures Against Risks

For the risks identified in section 4.1.2, consider what measures can be taken. When doing so, you need to set a policy beforehand on to what extent you want to implement the measures. Then, based on this policy, determine the measures regarding requirements 1 through 5 of the IoT high reliability requirements described in Table 3-1.

These measures can include software implementation (measures using IoT high reliability functions), hardware implementation, and actions taken by operators. It is possible to not implement any measures, if the expected damage is small or occurrence probability is low (risk acceptance). The measures to be implemented need to be decided based not just on the scale of damage and occurrence

probability, but also other priorities as well, including cost, organizational policies, and technical feasibility.

You need to consider the measures not individually, but with the consistency as a whole. If it turns out that the hardware resources (CPU, memory, network, etc.) of IoT devices and systems are limited and IoT high reliability functions are not implemented, or that the IoT high reliability functions are not implemented on devices and systems to which you are planning to connect, you need to consider a configuration that can protect these devices and systems.

4.1.4 Measures Using IoT High Reliability Functions

In 4.1.3, the measures against risks were categorized as: Software implementation (measures using IoT high reliability functions), hardware implementation, and actions taken by operators. This section describes the software implementation (measures using IoT high reliability functions).

When deciding on the software measures, you need to consider the functional requirements for the applicable software. These need to satisfy the software measure requirements in the IoT high reliability functional requirements described in 4.1.3. These are the requirements for the IoT high reliability functions. The examples of main functions that satisfy these requirements are described in Table 3-2. Use this table to select the necessary functions.

4.2 Examples of Considerations Regarding IoT High Reliability Functions

Among the use case analysis examples described in Appendix A, this section provides the example of considerations regarding IoT high reliability functions for coordination between automotive and home systems (UC1). The mapping to the basic model, identification of the objects to be protected in the risk assessment, identification of risk factors, and assumption of damage are conducted in UC1. Below is an example of conducting a risk evaluation based on this information and proceeding to the next step of considering measures.

(1) Risk evaluation example

Because UC 1 is an example related to automotive systems, we used the CRSS for the risk evaluation method, by referring to the *Security Guidelines for Product Categories*. [7] In Table 4-1, the six risk characteristics (field-specific and common risks, threat classification, connection interface, who connected, whom sustained damage, and where it occurred) regarding the target devices (voice recognition device in homes, voice-operated systems in cars, cloud) are clarified, as a preparation for conducting the CRSS-based evaluation. Table 4-2 shows the result of the evaluation for these characteristics, which were conducted using the base metrics defined in CRSS (Access Vector, Access Complexity, Authentication, Confidentiality Impact, Integrity Impact, and Availability Impact). In this example, the risk evaluation results are indicated in red for those that are critical (i.e., requires measures) and orange for those that are major (requires attention). There were no minor risks (i.e., no immediate action is required).

When conducting a risk evaluation in UC1, it was necessary to consider the possibility of an abnormality in one system affecting other systems, because although the automotive systems, home systems, and cloud servers are separate systems, they can also be connected in some cases. Therefore, we treated them as one system and treated the cars, homes, and cloud as parts of the system. And then, we considered the effects on the whole system, when there is a vulnerability in each of these parts.

Table 4-1. Example of risk evaluation using CRSS (First half)

No.	Expected threat	Expected damage	Target device	Field-specific/common	Threat classification	Connection I/F (Intrusion route)	Who connected	Whom sustained damage	Where it occurred
1	Virus infection on car's voice-operated system (* Of whole system, car is attacked)	Negative influence on the human body from abnormal operation instruction (e.g., high-volume sound)	On-board equipment	Field-specific	Virus infection	USB	User (Intentionally)	Body and/or property	Service interface
2	Abnormal operation instruction from home's voice recognition device (* Of whole system, home is attacked)	Traffic accident (e.g., by stopping the engine)	Customer premises equipment	Common	Unauthorized use	3G/GSM	Attacker	Body and/or property	Service interface
3	Incorrect operation instruction from another home's voice recognition device (* Car of one's own system is attacked from another system)	Traffic accident (e.g., by stopping the engine)	On-board equipment	Field-specific	Unauthorized use	3G/GSM	Manufacturer and its affiliated company	Body and/or property	Service interface
4	Virus infection on home's voice recognition device (* Of whole system, home is attacked)	Abnormal operation that may physically affect people negatively (e.g., excessive light) or lead to disaster for the home/household goods (e.g., fire, theft).	Customer premises equipment	Common	Virus infection	USB	User (Intentionally)	Body and/or property	Service interface
5	Abnormal operation instruction from a car's voice-operated system (* Of whole system, car is attacked)	Same as above.	On-board equipment	Field-specific	Unauthorized use	3G/GSM	Attacker	Body and/or property	Service interface
6	Incorrect operation instruction from another car's voice-operated system (* Home of one's own system is attacked from another system)	Same as above.	Customer premises equipment	Common	Unauthorized use	3G/GSM	Attacker	Body and/or property	Service interface
7	Information leakage of cloud server	Malicious use of personal information	Server	Common	Information leakage	Internet	Attacker	Data	Service interface
8	Service interruption of cloud servers	Interruption of coordination function	Server	Common	DoS Attack	Internet	Manufacturer and its affiliated company	Intrinsic functions	Service interface
9	Tampering of communication data or spoofing	Negative influence on the human body from abnormal operation instruction (e.g., high-volume sound) Traffic accident (e.g., by stopping the engine)	Server	Common	Wire-tapping	Internet	Attacker	Intrinsic functions	Service interface
10	Car theft	Malicious use of personal information	On-board equipment	Field-specific	Information leakage	USB	Attacker	Data	Physical contact
11	Information leakage from disposed car	Malicious use of personal information	On-board equipment	Field-specific	Information leakage	USB	Attacker	Data	Physical contact

Table 4-2. Example of risk evaluation using CRSS (Second half)

			CRSS (application of CVSS)								
No.	Expected threat	Expected damage	AV Access Vector	AC Access Complexity	Au Authentication before access	Ease of Attack	C Confidentiality impact	I Integrity impact	A Availability impact	Impact	Risk value
1	Virus infection on car's voice-operated system (* Of whole system, car is attacked)	Negative influence on the human body from abnormal operation instruction (e.g., high-volume sound)	Local	Low	One-time	3.14	Severe	Severe	Severe	10.00	6.77
2	Abnormal operation instruction from home's voice recognition device (* Of whole system, home is attacked)	Traffic accident (e.g., by stopping the engine)	Adjacent	Intermediate	One-time	4.41	Severe	Severe	Insignificant	9.54	7.04
3	Incorrect operation instruction from another home's voice recognition device (* Car of one's own system is attacked from another system)	Traffic accident (e.g., by stopping the engine)	Network	Intermediate	Multiple times	5.49	Insignificant	Insignificant	Insignificant	6.44	5.36
4	Virus infection on home's voice recognition device (* Of whole system, home is attacked)	Abnormal operation that may physically affect people negatively (e.g., excessive light) or lead to disaster for the home/household goods (e.g., fire, theft).	Local	Low	One-time	3.14	Severe	Severe	Severe	10.00	6.77
5	Abnormal operation instruction from a car's voice-operated system (* Of whole system, car is attacked)	Same as above.	Network	Intermediate	Multiple times	5.49	Severe	Severe	Insignificant	9.54	7.55
6	Incorrect operation instruction from another car's voice-operated system (* Home of one's own system is attacked from another system)	Same as above.	Network	Intermediate	Multiple times	5.49	Insignificant	Insignificant	Insignificant	6.44	5.36
7	Information leakage of cloud server	Malicious use of personal information	Network	High	Multiple times	3.15	Severe	None	None	6.87	4.57
8	Service interruption of cloud servers	Interruption of coordination function	Network	High	Multiple times	3.15	None	None	Severe	6.87	4.57
9	Tampering of communication data or spoofing	Negative influence on the human body from abnormal operation instruction (e.g., high-volume sound) Traffic accident (e.g., by stopping the engine)	Network	High	Multiple times	3.15	Severe	Severe	Insignificant	9.54	6.45
10	Car theft	Malicious use of personal information	Local	Intermediate	One-time	2.70	Severe	None	Severe	9.21	6.00
11	Information leakage from disposed car	Malicious use of personal information	Local	Intermediate	One-time	2.70	Severe	None	None	6.87	4.35

(2) Examples of Reviewed Measures That Use IoT High Reliability Functions

Based on the risk evaluation result described in Table 4-2, we created a policy to review the measures for those that require implementation of measures (C: Critical, indicated in red) and those that require attention (M: Major, indicated in orange). This meant that all items in the table required some kind of measure.

Some of these measures require the use of hardware or manual action, but we focused on the software measures in this phase.

When considering the requirements for the IoT high reliability functions, we mapped the above risk evaluation result and considered the necessary measures, as shown in Table 4-3.

Table 4-3. Application examples of IoT high reliability functions

Requirement for IoT high reliability function	Main risk (Risk No.)	Priority	Measure	Main function that is applicable
[Functional requirement 1] Initial settings are configured properly, and are confirmed as appropriate.	Operation from another home's voice recognition device (3)	M	Configure settings so that legitimacy of access can be confirmed. (Related to measures for Functional requirement 2)	Initial Setting function
	Operation from another car's voice-operated system (6)	M		
[Functional requirement 2] Can confirm that permission is granted when beginning to use the service.	Operation from another home's voice recognition device (3)	M	Confirm if access is legitimate, and if it is not legitimate, cut the communication and notify the user.	Authentication function Access Control function
	Operation from another car's voice-operated system (6)	M		
[Functional requirement 3] Predictive signs of abnormalities can be identified.	Virus infection on a car's voice-operated system (1)	M	Prevent virus infections.	Antivirus function
	Virus infection on a home's voice recognition device (4)	M		
[Functional requirement 4] Functions and assets that should be protected can be protected.	Information leakage (7), Tampering of communication data and spoofing (9)	M	Protect data.	Encryption function Authentication function (Message)
[Functional requirement 5] Preparations can be made for abnormalities.	Abnormal operation from a home's voice recognition device (2)	C	Eliminate vulnerabilities and prevent unauthorized operations.	Remote Update function (Including local update)
	Abnormal operation from another car's voice-operated system (5)	C		

[Functional requirement 6] Occurrences of abnormalities can be monitored and notified.	*	–	Monitor abnormalities.	Monitoring function
[Functional requirement 7] Events can be logged for identification of causes of abnormalities.	*	–	Collect logs.	Log Collection function
[Functional requirement 8] Configurations can be identified.	*	–	Manage the configuration information.	Configuration Information Management function
[Functional requirement 9] Operation can be continued even when there is an abnormality.	Service interruption of cloud servers (8)	M	Separate the failed section or switch to the backup system when there is a failure.	Degenerate function Redundant Configuration function
[Functional requirement 10] Early recovery is possible when there is an abnormality.	*	–	Prepare a function to recover from an abnormal condition.	Suspend function Recovery function
[Functional requirement 12] Use of system/service can be terminated autonomously or suspended.	Cars/theft (10)	M	Lock when stolen.	Operation Protection function
[Functional requirement 12] Data can be erased.	Information leakage when cars are discarded (11)	M	Erase data before any car is discarded.	Erase function

*: Required items for the risks.

<Column 2> Conducting Risk Evaluation Before Implementing the Measures

Kosuke Ito, Connected Consumer Device Security Council (CCDS)

IT systems and services have various risk factors (vulnerabilities). When developing an IT system, analyzing the threats on the target system from the safety and security perspectives is an important task in the design phase, to ensure its high reliability.

Guides and manuals usually tell you to "do a threat analysis first" as part of a security measure, and many of you may have experience identifying the potential threats. So, should you immediately start considering the measures to be implemented to eliminate all identified threats? Dealing with all identified threats is time-consuming and costly, and it leads impossible to start an IoT service.

Risk evaluation allows you to highlight the threats and vulnerabilities that should be addressed with higher priority. Not all threats lead to catastrophic risks for the users and service providers. In the risk evaluation, you make assumptions on the possible risks for the identified threats, highlight significant risks that must be avoided when providing your services, and clarify the priority of addressing these threats.

There are several ways to conduct the risk evaluation, depending on the evaluation perspectives. Here, we introduce two typical methods.

1) CVSS

CVSS (Common Vulnerability Scoring System) is a vulnerability scoring system promoted by a non-profit organization called FIRST (Forum of Incident Response and Security Teams), and is the standard evaluation method in information security. This scoring system allows you to clarify the severity by scoring three metric scores, Base, Temporal and Environmental, for each vulnerability, and then using formulas to get the CVSS scores. CVSS is currently in version 3.

- CVSS calculator: http://jvndb.jvn.jp/cvss/v3/ja.html

Metric	Description
1) Base metrics	The Base metrics measure the confidentiality, integrity, and availability impacts.
2) Temporal metrics	The Temporal metrics measure, for example, the exploit code availability and existence of workarounds.
3) Environmental metrics	The Environmental metrics measure, for example, the secondary damage and use of affected products.

Rating	CVSS Score
Critical	9.0 - 10.0
High	7.0 - 8.9
Medium	4.0 - 6.9
Low	0.1 - 3.9
None	0

CRSS: CVSS for the automotive industry

CRSS was created by the Society of Automotive Engineers of Japan (JSAE) based on CVSS (ver. 2), and considers the impacts on human lives and safety. [7]

2) OWASP Risk Rating Methodology

This risk rating methodology was created by an open community called OWASP for solving issues related to web application security.

- Calculation of risk severity: Risk Severity = (((1) + (2))/2) * (((3) + (4))/2)

Features: The risk factors include not just technical impacts, but business impacts as well, including financial damages (e.g., cash) and reputation damages.

①Threat Agent ①-1:Skill Level ①-2:Motive ①-3:Opportunity ①-4:Size	③Technical Impact ③-1:Loss of confidentiality ③-2:Loss of integrity ③-3:Loss of availability ③-4:Loss of accountability
②Vulnerability ②-1:Ease of discovery ②-2:Ease of exploit ②-3:Awareness ②-4:Intrusion detection	④Business Impact ④-1:Financial damage ④-2:Reputation damage ④-3:Non compliance ④-4:Privacy violation

For automotive systems, there are also other methodologies, including RSMA (Risk Scoring Methodology for Automotive system) that scores the risks based on two parameters, likelihood and impact, and OCTAVE Allegro that takes into consideration additional evaluation criteria categories, such as reputation and productivity. We recommend using multiple methodologies, if possible, for the risk evaluation, to not miss any serious risks. For Example, there was an actual review case in CCDS. The user wanted to focus on reputational damage, but the implemented measures did not reflect any effect, because this user scored the risks using a method not having the reputational damage factor.

Though the task of risk evaluation can be hard work, there are advantages, as shown below.

1) The severity of identified threats can be quantified and visualized.
2) The severity rating of threats that should be addressed facilitates the decision making.
3) The measures against threats can be considered in the early part of the design stage.
4) By conducting the risk evaluation again on the target system after the measures are implemented, you can verify how the measures contributed to reducing the risks (i.e., you can determine the adequacy of the implementation cost of measures).
5) Using the basis of risk ratings, it becomes easier for the developers and those responsible for quality management to have the common perspectives on risks.

As described above, risk evaluation is an important part of the design process for business organizations for determining which security measures are reasonable from the technical and business perspectives.

Conclusion

In the world of IoT, connection of various devices and systems are expected to create a world that is more convenient than ever before. On the other hand, there is also a risk of creating a social chaos unless safety/security/reliability of IoT are ensured. The Software Reliability Enhancement Center, Technology Headquarters, Information-technology Promotion Agency (IPA/SEC) compiled the IoT Safety/Security Development Guidelines for addressing the IoT-related risks and clarified the key factors that the system developers should take into consideration.

While the industrial sectors are pushing the development IoT devices and systems, there were no specific requirements that can be used for the consideration of making IoT more reliable, and the responsibility of setting the requirements were left to the developers themselves. There was a demand for specific functional requirements for highly reliable IoT. In particular, the requirements for high reliability functions necessary for coordination between different sectors, which is one of the features of IoT, were not clarified.

Given such conditions, IPA/SEC decided to compile the common measures for highly reliable IoT for each industrial sector, by presenting requirements for high reliability functions that should be implemented by the developers when developing IoT devices and systems. The perceptions of highly reliable IoT, however, were significantly different between the members in the working group. In an effort to reach a consensus, long hours were spent in the working group to discuss what should be considered when designing from the maintenance and operation perspectives and where the functions should be implemented in the IoT configuration, based on the use cases of coordination between different sectors. This document was compiled as a result of this hard work. We hope that those who are responsible for developing IoT devices and systems follow the *IoT Safety/Security Development Guidelines* and refer to this document when developing the functions for highly reliable IoT.

We will continue to keep track of the relevant standards and new developments in the IoT services and risks, and update this document accordingly.

Lastly, we would like to thank the members in the working group for providing tremendous support to the work of compiling of this document.

Appendix A. IoT Use Case Analysis

As described in 2.2, the IoT high reliability functions in this document were deduced from typical use case analyses (i.e., these are not application examples of IoT high reliability functions, but rather, use cases for deducing the functions).

Various risks may arise when the IoT develops further in the future and when IoT is used to coordinate between different sectors. To illustrate how the IoT is implemented and consider the risks involved in coordination between different sectors, we clarified the coordination models and selected the required IoT high reliability functions based on the identified risks.

(1) Coordination models

To analyze the threats and hazards and consider the implementation of technical measures, we created the Cloud Coordination (CC) model, Fog Coordination (FC) model, and Edge Coordination (EC) model for each layer as models of IoT coordination between different sectors. The Edge Coordination model is coordination between individual platforms. The Fog Coordination model is coordination that works in conjunction with the Fog layer, and while the coordination with the Edge layer is included, the coordination with the Cloud layer is not included. The Cloud Coordination model is coordination that works in conjunction with the Cloud layer, and the coordination with the Fog and Edge layers are included.

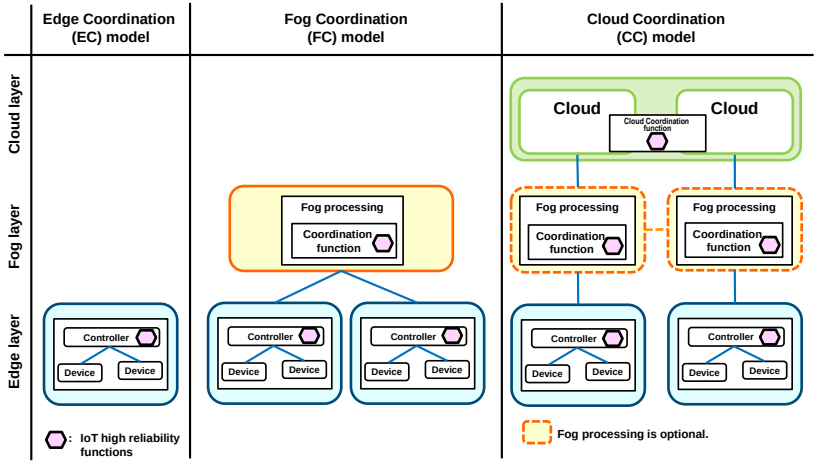


Figure A-1. Coordination models

(2) Relationships between the use cases and coordination models

For the use cases, we created and analyzed five use cases, as shown in Table A-1. These use cases are those that can be implemented now and those that can be expected to be implemented in the future. We will use the term "IoT component" (those among the IoT devices and systems that fulfill their purposes or functions independently), as this analysis is based on the *IoT Safety/Security Development Guidelines*. We found that each of these use cases does not apply to a certain coordination model, but rather, apply to multiple models. Here, we analyzed mainly the risks regarding the coordination function, based on the coordination models that most reflect the characteristics of these use cases.

Table A-1. Relationships between the use cases and coordination models

Use case		EC model	FC model	CC model	Note
UC1	Coordination between cars and home systems			◎	This is a CC model because it utilizes the cloud and real-time processing is not required.
UC2	Coordination between VPP and distributed energy resources monitoring service	○		◎	Coordination between multiple services. There is a model where the HEMS server resides in the cloud and another model where the HEMS server resides within the customer device, and the former is selected as a CC model.
UC3	Coordination between Home Devices	◎			Coordination between HEMS devices or controllers. Fog and cloud are not used.
UC4	Conflict control for door locks	◎	○	○	This is for solving conflicts between multiple control software in home GW or edge servers.
UC5	Coordination between industrial robots and power management	○	◎		This is a Fog Coordination model that coordinates multiple services and where fast judgment response is important.

(○ are those that are applicable to the model and ◎ are those on which analyses were conducted.)

UC1. Risk Analysis on Coordination Between Cars and Homes

Yoshio Nakagaki, Denso Corporation

(1) Target sectors of coordination

Automotive vehicles (cars) and homes

(2) Overview

The driver of a car uses the on-board voice-operated system (by connecting to the cloud-based voice recognition service for the driver's home) to control the lighting, thermostat, and security systems in the home, such as opening/closing the garage door, turning on/off the lighting of the home's entrance, and turning on/off the home security system. The person relaxing on a couch at home uses the home's cloud-based voice recognition service to start/stop the car's engine, lock/unlock the car's door, and check its fuel gauge.

(3) Form of coordination

Cloud Coordination model

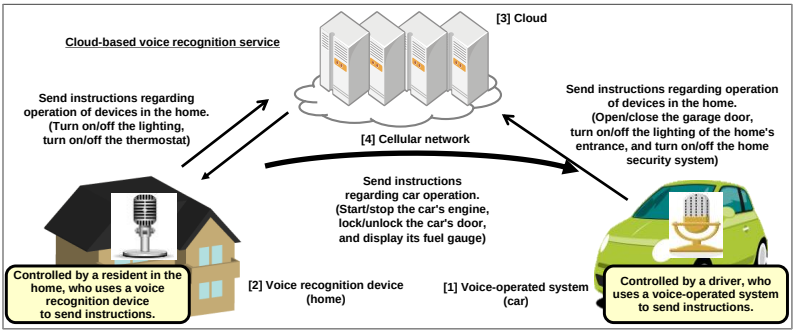


Figure A-2. Form of coordination

(4) Characteristics

The characteristics of this coordination are that this is coordination of services in different sectors (i.e., automotive and home sectors), using a cloud service, like a cellular network. A real-time IoT connection of homes and cars located in different areas allows the user to execute various remote operations.

There are, however, security risks including accidents such as incorrect remote instruction sent to a home from a car causing a fire, and attacks on a car in motion leading to car operation not intended by the driver which could cause serious accidents that may put lives at stake.

(5) Structural analysis of IoT components

As indicated in Figure A-3, the resident in the home can acquire operation information regarding the car's voice-operated system from the cloud, and the driver of a car can connect to the cloud and acquire operation information regarding the home's voice recognition device.

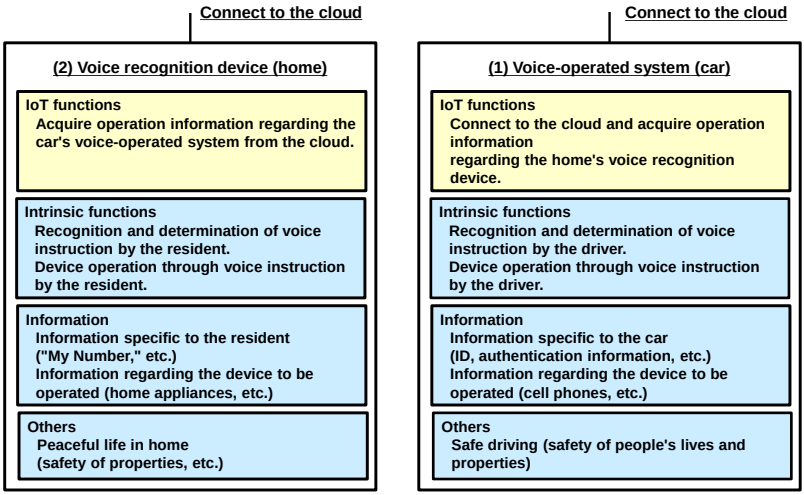


Figure A-3. Structural analysis of IoT components

(6) Expected threats/damage and main factors and issues

The expected risks and main factors are as described below.

Table A-2. Expected threats/damage

Location	Expected threat/damage	Main factors and issues
(1)	Virus infection on car's voice-operated system Abnormal operation that may physically affect the passengers negatively (e.g., high volume sound) or cause accidents (e.g., by stopping the engine).	Vulnerabilities of car's voice-operated system
(1)	Abnormal operation instruction from home's voice recognition device Same as above	Vulnerabilities of home's voice recognition device Vulnerabilities of the network that connects the car and home
(1)	Incorrect operation instruction from another home's voice recognition device Same as above.	No authentication of device that connects to the car's voice-operated system
(1)	Intermittent service interruption of a car's voice-operated system Recognition capability of proper operation information may be hampered, and incorrect operation could physically affect the passengers negatively or cause accidents.	Failure or end of life of the car's voice-operated system
(2)	Virus infection on home's voice recognition device Abnormal operation that may physically affect the people negatively (e.g., excessive light) or lead to disaster for the home/household goods (e.g., fire, theft).	Vulnerabilities of home's voice recognition device
(2)	Abnormal operation instruction from a car's voice-operated system Same as above	Vulnerabilities of car's voice-operated system Vulnerabilities of the network that connects the home and car
(2)	Incorrect operation instruction from another car's voice-operated system Same as above	No authentication of device that connects to the home's voice recognition device
(2)	Intermittent service interruption of a home's voice recognition device Recognition capability of proper operation information may be hampered, and incorrect operation could physically affect the people negatively or lead to disaster for the home/household goods (e.g., fire, theft).	Failure or end of life of the home's voice recognition device
(3)	Service interruption of cloud server or information leakage	Vulnerabilities in the server system
(4)	Tampering of communication data or spoofing	Vulnerabilities of the network

(7) Possible measures

The measures for the expected risks are as described below.

Table A-3. Measures for the expected risks

Location	Expected threat/damage	Measure	Coordination model	Note
(1)	Virus infection on car's voice-operated system	Check the trustworthiness of the device connected via cloud (e.g., car's voice-operated system) and stop the system	CC	Authentication function, Access Control function Monitoring function,

		and notify the user if the device is not trustworthy.		Log Collection function Suspend function
(1)	Abnormal operation instruction from home's voice recognition device	Check if the operation instruction sent from the device connected via cloud (e.g., home's voice recognition device) is a proper instruction and stop the system and notify the user if any abnormality is detected.	CC	Abnormality Detection function Monitoring function, Log Collection function Suspend function
(1)	Operation instruction from another home's voice recognition device	Check the authenticity of the device connected via cloud (e.g., home's voice recognition device) and cut the communication and notify the user if the device is not authentic.	CC	Authentication function, Access Control function Configuration Information Management function Monitoring function, Log Collection function Forced Cutoff function
(1)	Intermittent service interruption of car's voice-operated system	Periodically check if the system is operating properly, manage the cumulative operation hours, and stop the system and notify the user if any abnormality is detected.	CC	Diagnostic function Lifetime Management function Monitoring function, Log Collection function Suspend function
(2)	Virus infection on home's voice recognition device	Check the trustworthiness of the device connected via cloud (e.g., home's voice recognition device) and stop the system and notify the user if the device is not trustworthy.	CC	Authentication function, Access Control function Monitoring function, Log Collection function Suspend function
(2)	Abnormal operation instruction from a car's voice-operated system	Check if the operation instruction sent from the device connected via cloud (e.g., car's voice-operated system) is a proper instruction and stop the system and notify the user if any abnormality is detected.	CC	Abnormality Detection function Monitoring function, Log Collection function Suspend function
(2)	Operation instruction from another car's voice-operated system	Check the authenticity of the device connected via cloud (e.g., car's voice-operated system) and cut the communication and notify the user if the device is not authentic.	CC	Authentication function, Access Control function Configuration Information Management function Monitoring function, Log Collection function Forced Cutoff function
(2)	Intermittent service interruption of home's voice recognition device	Periodically check if the system is operating properly, manage the cumulative operation hours, and stop the system and notify the user if any abnormality is detected.	CC	Diagnostic function Lifetime Management function Monitoring function, Log Collection function Suspend function
(3)	Service interruption of cloud server or information leakage	Use a typical redundant configuration or other similar measures.	-	-

(4)	Tampering of communication data or spoofing	Use a typical encryption method or other similar measures.	-	-

(8) IoT high reliability functions and implementation locations

(1) (Device) Authentication function and Access Control function

Confirmation of trustworthiness and authenticity of devices connected via cloud.

- Car's voice-operated system and home's voice recognition device connect to the cloud.
- Trustworthiness and authenticity of devices connected via cloud are checked.
- The car sets the home's voice recognition device as the connection destination and the home sets the car's voice-operated system as the connection destination.

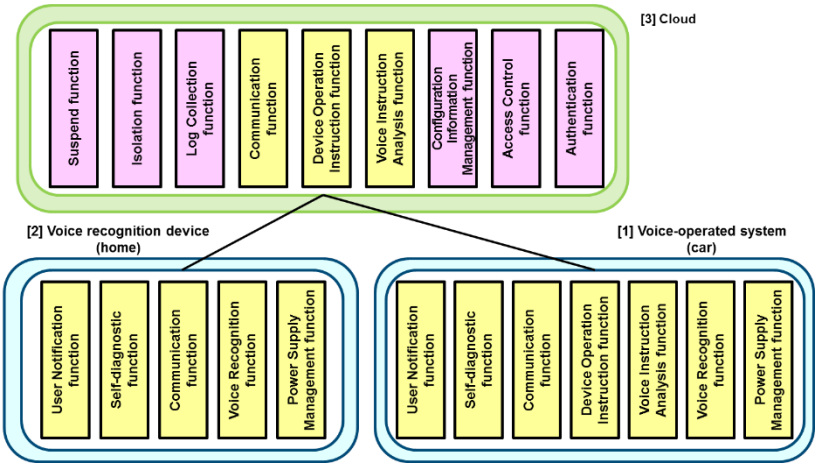


Figure A-4. Confirmation of trustworthiness and authenticity of devices connected via cloud

(2) Monitoring function (Abnormality detection)

Confirmation of trustworthiness of operation information regarding the devices connected via cloud.

- Car's voice-operated system and home's voice recognition device connect to the cloud.
- Trustworthiness of devices connected via cloud are checked.
- The car sets the home's voice recognition device as the connection destination and the home sets the car's voice-operated system as the connection destination.

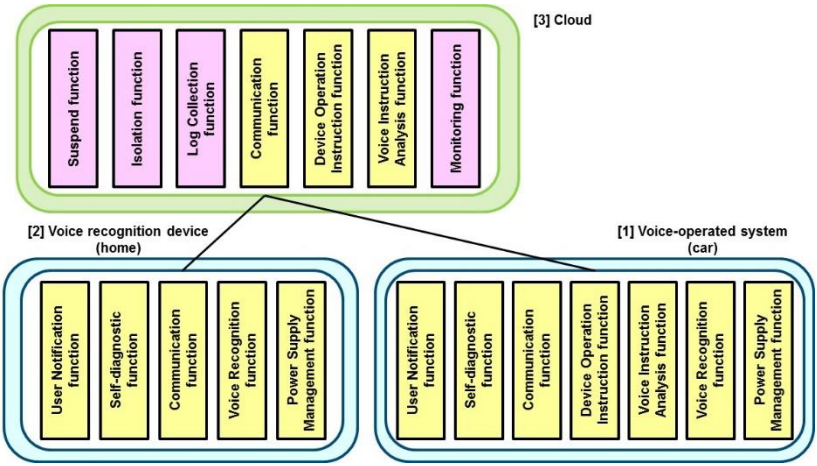


Figure A-5. Confirmation of trustworthiness of operation information regarding the devices connected via cloud

(3) Diagnostic function and Lifetime Management function

Confirmation of trustworthiness of devices connected via cloud.

- Car's voice-operated system and home's voice recognition device connect to the cloud.
- Operation statuses of devices connected via cloud are checked and cumulative operation hours are managed.
- The car sets the home's voice recognition device as the connection destination and the home sets the car's voice-operated system as the connection destination.

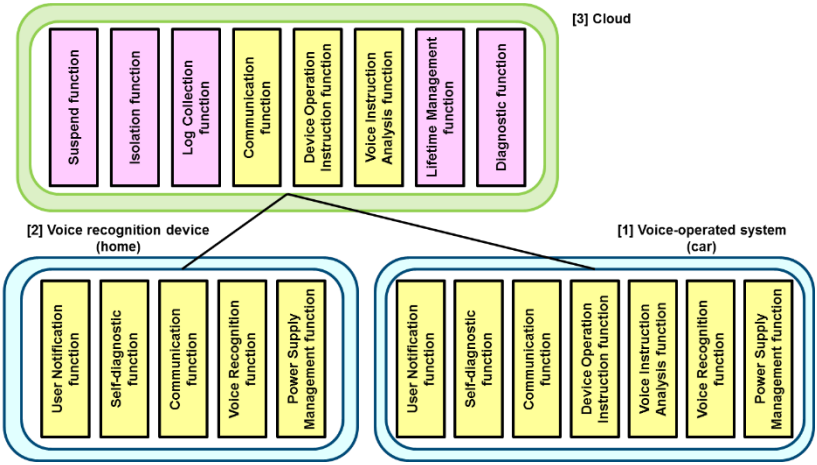


Figure A-6. Confirmation of trustworthiness of devices connected via cloud

UC2. Risk Analysis on Coordination Between VPP and Distributed Energy Resources Monitoring Service

Kazutaka Tsuji, The Japan Electrical Manufacturers' Association

(1) Target sectors of coordination

VPP (Virtual Power Plant) and distributed energy resources monitoring service

(2) Overview

In VPP, an aggregator operates the virtual large-scale power generation facilities or large-scale energy storage systems by controlling the distributed energy resources systems, such as photovoltaic systems, fuel cells, and energy storage systems installed at customers' sites (e.g., homes) via a network, and provides services to the power transmission/distribution operators, such as supplying power when the grid power supply capability is tight and adjusting supply/demand when there is a surplus of energy resources. In this case, HEMS (Home Energy Management System) that consists of an HEMS server and HEMS controller runs the operation of charging/discharging storage batteries and operation of customer devices based on the power generation prediction and battery charge status for the relatively small distributed energy resources in homes, to meet the aggregator's requirement on power supply and power consumption.

The distributed energy resources monitoring service, on the other hand, provides services such as monitoring the generation status of photovoltaic systems or charge/discharge status of energy storage systems, estimating the amount of energy that can be produced based on abnormality notifications and weather forecasts, and checking the charge/discharge capacity of storage batteries.

(3) Form of coordination

Cloud Coordination model

HEMS consists of a function that coordinates with multiple services and the HEMS controller function that collects information from and controls the ECHONET Lite devices installed at customers' sites, and is defined as a system that realizes the coordination with other services and ECHONET Lite devices. [8]

The service coordination function is installed on the server or on the customers' devices. This use case is based on the assumption that the HEMS server is on the cloud and this server is linked with the HEMS controllers at customers' sites.

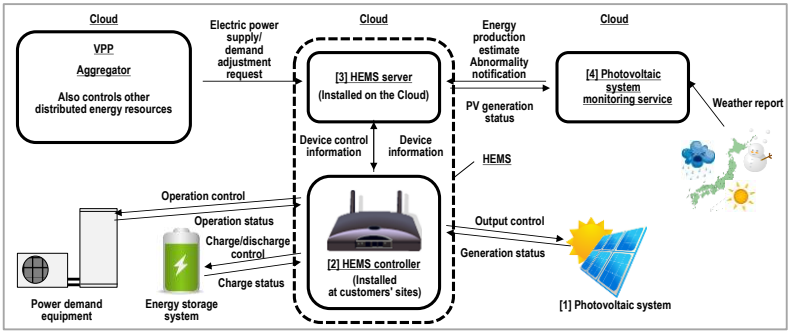


Figure A-7. Form of coordination

(4) Characteristics

The characteristics of this coordination are that this is coordination of services in different sectors (i.e., VPP that controls multiple distributed energy resources and monitoring systems that detects abnormalities in photovoltaic systems and energy storage systems or estimates PV generation amounts), using a cloud service and HEMS through the Internet. This enables, for example, meeting the requirements set by an aggregator on optimizing the control of customers' devices based on the estimates of PV generation amounts and charge/discharge capacity of storage batteries.

However, there are risks of failing to meet the aggregator's requirements or creating conditions that could lead to accidents, such as unnecessary PV system interruption, due to incorrect PV generation amount estimates or device abnormality notification. There may also be risks in particular with VPP that controls numerous distributed energy resources. A serious accident may occur that would hinder stable grid power operation.

(5) Structural analysis of IoT components

This section is based on the coordination between VPP and photovoltaic system monitoring system. As shown in Figure A-8, HEMS acquires the power supply/demand requirement information from the VPP aggregator and PV generation estimate and device abnormality notification from the photovoltaic system monitoring system. Based on this information, VPP controls the PV systems and other ECHONET Lite devices, and the PV system sends the generation status to the monitoring system via HEMS.

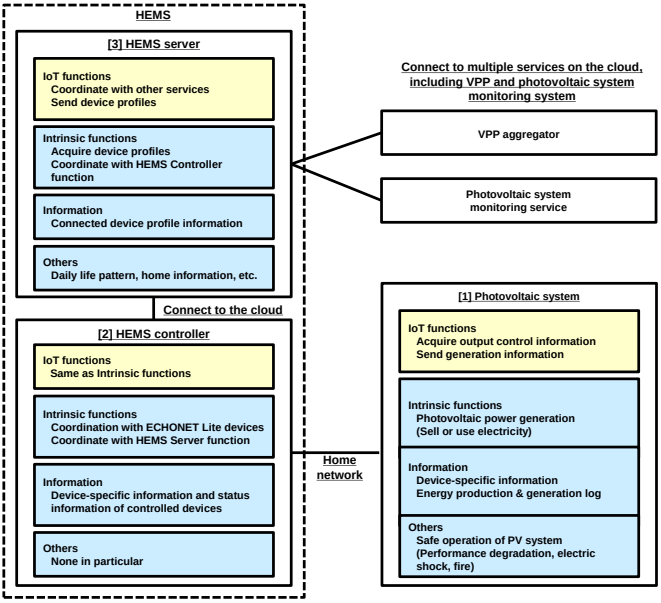


Figure A-8. Structural analysis of IoT components

Appendix

(6) Expected threats/damage and main factors and issues

The expected risks and main factors are as described below.

Table A-4. Expected threats/damage

Location	Expected threat/damage	Main factors and examples of issues
(1)	Malfunction of photovoltaic system Device malfunction due to an abnormal/incorrect control sent from an uncertified app or other controllers. (Unnecessary power generation restriction, failure to meet VPP's requirement)	Vulnerability in the PV system. Connection with an uncertified app or other controllers that are low quality. Priority settings regarding communication destinations are not set.
(2)	Unauthorized access and spoofed access to HEMS controller Unnecessary power generation restriction and failure to meet VPP's requirements due to the use of incorrect device information. Unnecessary power generation restriction and failure to meet VPP's requirements due to the use of incorrect control information.	Vulnerability in the HEMS controller. Unencrypted communication. Not confirming the communication destination.
(2)	Virus infection on the HEMS controller Abnormal device control and failure to meet VPP's requirements. Unnecessary power generation restriction and failure to meet VPP's requirements due to transmission of incorrect device information to the HEMS server.	Vulnerability in the HEMS controller.
(2)(3)	Tampering of communication data	Vulnerability in the

	Unnecessary power generation restriction and failure to meet VPP's requirements due to the use of incorrect device information. Unnecessary power generation restriction and failure to meet VPP's requirements due to the use of incorrect control information.	communication between the server and controller.
(3)	Unauthorized access and spoofed access to the HEMS server Unnecessary power generation restriction and failure to meet VPP's requirements due to the use of abnormal control information. Malfunction of monitoring system due to the use of incorrect device information.	Vulnerability in the communication between the PV monitoring system and HEMS server. Vulnerability in the communication between the HEMS server and controller.
(3)	Virus infection on the HEMS server Abnormal device control and failure to meet VPP's requirements. Malfunction of the monitoring system due to the use of incorrect device information.	Vulnerability in the HEMS server.

(7) Possible measures

The measures for the expected risks are as described below.

Table A-5. Measures for the expected risks

Location	Expected threat/damage	Measure	Coordination model	Note
(1)	Malfunction of photovoltaic system	・ Deny connections from or restrict functions for uncertified apps and controllers, by using device authentication to authenticate the other side and using the shared keys to perform message authentications. ・ Restrict the connections (controllers) by requiring user's approval.	EC	(Device) Authentication function Message Authentication function Access Control function
(2)	Unauthorized access and spoofed access to the HEMS controller	・ Use device authentication to authenticate the other side and use the shared keys to perform message authentications. ・ Deny response to abnormal control instructions related to safety and device failure.	CC	(Device) Authentication function Message Authentication function Monitoring function
(2)	Virus infection on the HEMS controller	・ Update the controller's OS and security software. ・ Confirm the connection destination (device authentication).	CC	(Device) Authentication function
(2)(3)	Tampering of communication data	・ Encrypt communication using SSL/TLS. ・ Collate data using accumulated logs.	CC	Encryption function Log Collection function
(3)	Unauthorized access and spoofed access to the HEMS server	・ Device authentication of coordinated server. ・ Collation of information, and monitoring abnormal instructions and notifying (e.g., bulk failure/maintenance of devices, etc.) by a third-party entity.	CC	(Device) Authentication function Monitoring function Log Collection function

(3)	Virus infection on the HEMS server	・ Update the server's OS and security software. ・ Run security updates on the network devices. ・ Confirm the connection destination (device authentication).	CC	(Device) Authentication function

(8) IoT high reliability functions and implementation locations

(1) Device Authentication function/Message Authentication function/Access Control function

Trustworthiness confirmation of devices connected in the home network.

- Confirm and approve that the device is being connected to the intended device.
- HEMS controller and PV system confirm each other's authenticity.
- Encrypt the communication with other devices and use message authentication.

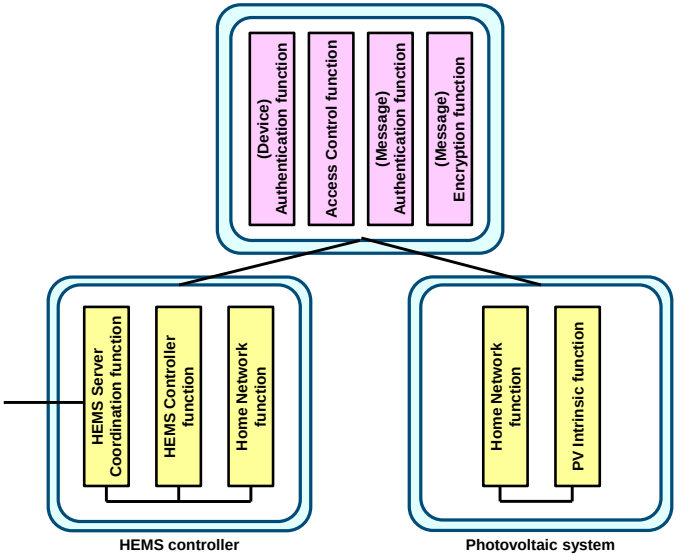


Figure A-9. Trustworthiness confirmation of devices connected in the home network

(2) Device Authentication function/Encryption function/Log Collection function

Trustworthiness confirmation between HEMS server and HEMS controller

- Confirm and approve that the device is being connected to the intended device.
- HEMS server and HEMS controller confirm each other's authenticity.
- Encrypt the communication with other devices.
- Collate the device control information and device operation and analyze the factors that caused the malfunction.

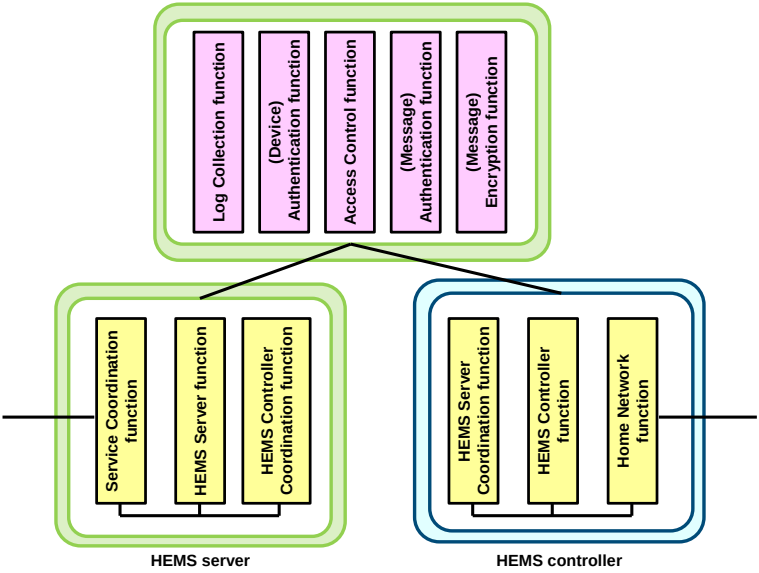


Figure A-10. Trustworthiness confirmation between HEMS server and HEMS controller

UC3. Risk Analysis on Coordination Between Home Devices

Takashi Murakami, ECHONET CONSORTIUM

(1) Target sectors of coordination

Controllers and home devices.

(2) Overview

A relatively low-speed, low-bandwidth, and low-cost facility network that is compatible with conventional domestic appliances, household equipment, and sensor networks will enable the interconnection and systematic operation of a wide assortment of household appliances, sensors, and controllers made by different manufacturers. The result will be a network system that is safe/secure/reliable, comfortable, user-friendly and eco-friendly, in response to challenges including energy conservation, elderly users and home care nursing.

For example, the presence or absence of a resident will be detected and air conditioning and lighting will be controlled efficiently to reduce wasteful energy consumption. Energy from solar power facilities and fuel cells, which are expected to spread in the future, will be stored in batteries or electric vehicles and used at night or during hours when household power consumption is high, thus using natural energy efficiently. By operating facilities for power generation, storage, and consumption efficiently in a network, environment-friendly and efficient energy management systems can be constructed.

(Excerpts from Part I in *ECHONET Lite SPECIFICATION*) [9]

(3) Form of coordination

Edge Coordination model

This is an example of a model where the HEMS controller understands the PV (photovoltaic) power generation status and battery's charge capacity and controls the charging of the batteries, so that the PV-generated energy is consumed inside the home and energy is utilized effectively.

This model is used as shown below.

- The HEMS controller acquires the power generation status from the PV system.
- The HEMS controller acquires the charge capacity from the batteries.
- If electricity is being sold or if power output is being restricted, the HEMS controller sends a charge request to the batteries, so that electricity will be used efficiently by the user.

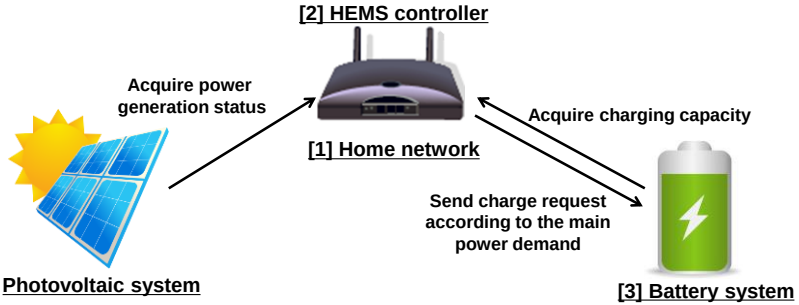


Figure A-11. Form of coordination

(4) Characteristics

The characteristics of this coordination are that users coordinate different devices in their homes, such as photovoltaic systems and energy storage systems, by accessing the HEMS controller via Ethernet, Wi-Fi, and other home networks. In the example for this model, effective use of electricity is accomplished by using the information acquired from the photovoltaic system and controlling the charging of the energy storage system.

ECHONET Lite is a communication specification for interconnecting the HEMS controller with the photovoltaic system and energy storage system. This specification prescribes the *Specification Compliance Certification: ECHONET Lite Certification* for testing the conformance to the communication specifications to ensure the interoperability and the *Specification Compliance Certification: Interface Specification for Application Layer Communication between Smart Energy Meters and HEMS Controllers* for testing the conformance to the specifications that prescribe the detailed applications of ECHONET Lite for each device.

However, because ECHONET Lite is a lightweight and simple communication specification, devices that have not been awarded with the above conformity certifications and have low reliability in terms of interoperability may be released on the market. For this reason, some users are commenting that they "want to operate the devices safely from an HEMS controller with high communication reliability" and some service/device providers are commenting that they "want to provide device operation capability that is more advantageous for the users, by combining devices with high communication reliability."

(5) Structural analysis of IoT components

As shown in Figure A-12, users can operate the devices in their homes through HEMS controllers. They can also obtain status information and device-specific information for these devices.

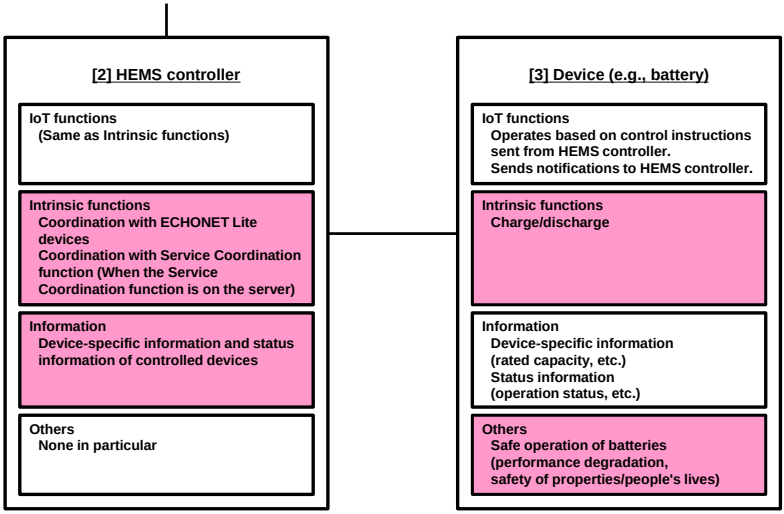


Figure A-12. Structural analysis of IoT components

(6) Expected threats/damage and main factors and issues

The expected risks and main factors are as described below.

Table A-6. Expected threats/damage

Location	Expected threat/damage	Main factors and examples of issues
(2)(3)	Connection from an uncertified app Device malfunction due to an abnormal/incorrect control instruction sent from an uncertified app on PC/smartphone.	Connection with an uncertified app that is low quality.
(2)(3)	Connection from an unauthorized device Device malfunction due to an abnormal/incorrect control instruction or needless control instruction (for the main controller) sent from other controllers.	Priority settings regarding communication destinations are not set. Connection with a low-quality controller.
(2)(3)	Unauthorized control Unintended controlling of a device through unauthorized access or incorrect connection by a third party to the Ethernet/Wi-Fi (including bad packets sent due to an implementation mistake).	Wi-Fi security settings are not configured properly. Communication is not encrypted. Not confirming the communication destination.
(1)	Leakage of private information Interception of private information or device status information through unauthorized access to the Ethernet/Wi-Fi.	Wi-Fi security settings are not configured properly. Communication is not encrypted.

(7) Possible measures

The measures for the expected risks are as described below.

Table A-7. Measures for the expected risks

Location	Expected threat/damage	Measure	Coordination model	Note
(2)(3)	Connection from an uncertified app	· Deny connections from or restrict functions for uncertified apps and controllers, by using device authentication to authenticate the other side and using the shared keys to perform message authentications.	EC	(Device) Authentication function (Message) Authentication function
(2)(3)	Connection from an unauthorized device	· Use access control to restrict the connections (controllers).	EC	Access Control function
(2)(3)	Unauthorized control	· Use access control to prevent incorrect connections. · Use device authentication to authenticate the other side and use the shared keys to perform message authentications.	EC	(Device) Authentication function (Message) Authentication function Access Control function
(1)	Leakage of private information	· Use device authentication to authenticate the other side and use the shared keys to encrypt the messages.	EC	(Device) Authentication function (Message) Encryption function

(8) IoT high reliability functions and implementation locations

(1) Authentication, Access Control, and Encryption functions

Trustworthiness confirmation of devices connected in the home network.

- Confirm and approve that the device is being connected to the intended device.
- HEMS controller and controlled devices mutually confirm the other's authenticity (e.g., awarded or not with the specification compliance certification).
- Encrypt and authenticate (message authentication) the communication with those devices for which the authenticity is confirmed.

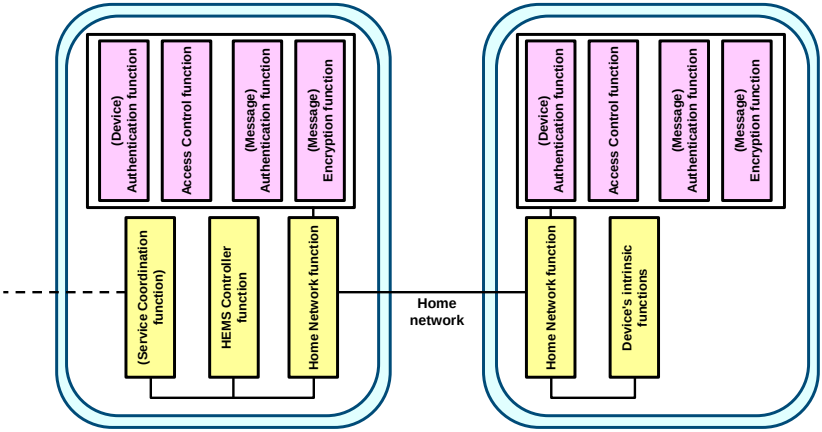


Figure A-13. Trustworthiness confirmation of devices connected in the home network

UC4. Risk Analysis on Conflict Control for Door Locks

Akira Tsuge, YRP R&D Promotion Committee / WSN-ATEC General Incorporated Association

(1) Target sectors of coordination

Homes (Conflicts between multiple systems in homes)

(2) Overview

This use case analysis describes the conflicts between the automatic ventilation system for amenity control, emergency disaster management system, and home security system, as examples of conflicts that may occur when multiple systems inside a home operate simultaneously.

[1] Automatic Ventilation & Window Operation System for amenity control

A/C control and automatic ventilation control that use a temperature & humidity sensor, illuminance sensor, and PM 2.5 sensor.

[2] Emergency Disaster Management System and Home Security System

Disaster management control and home security control that use local weather reports and outdoor intruder sensors.

(3) Form of coordination

Edge Coordination model

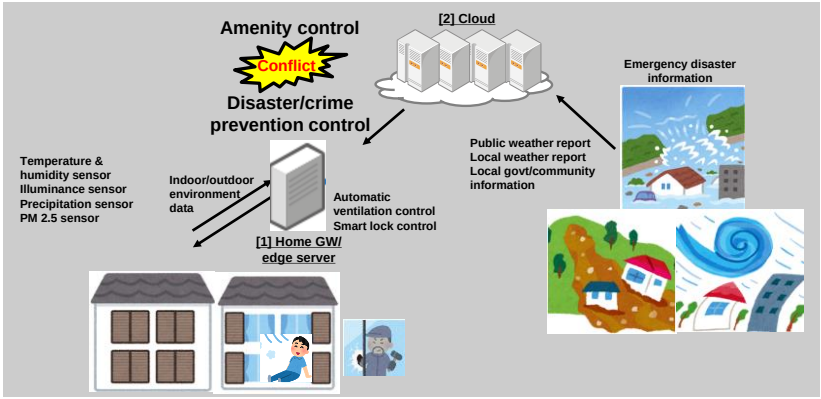


Figure A-14. Form of coordination

A conflict occurs between the amenity control of the Automatic Ventilation System that opens the shutters and windows and the door lock control of the Emergency Disaster Management or Home Security System that closes and locks the shutters and windows. The home's entrance should be unlocked to

allow emergency evacuation during emergency disasters, but this could conflict with the door lock control of the Home Security system.

(4) Characteristics

These are just two examples of conflicts, and there can be many other similar conflicts. For example, a video recording system's instruction to power on an audio/visual device could conflict with a power-saving system's instruction to power off the device. Usually, we have a mix of systems designed individually. When controlling a certain object, these individually-designed systems attempt to control the same object at the same time, and this can create unexpected conflicts.

(5) Structural analysis of IoT components

As shown in the figure below, these are examples of conflicts that occur inside the home gateway or home edge server.

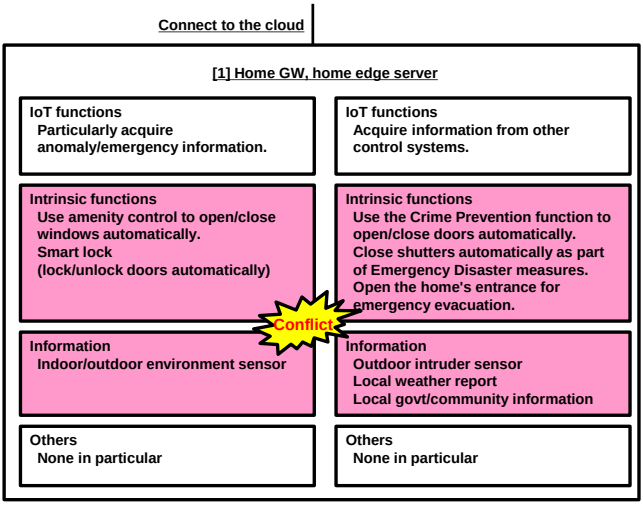


Figure A-15. Structural analysis of IoT components

(6) Expected threats/damage and main factors and issues

The expected threats/damage and main factors and issues for these examples are as described below.

Table A-8. Expected threats/damage

Location	Expected threat/damage	Main factors and examples of issues
(1)	Home GW/edge server The control that opens the windows for amenity and the control that closes the windows and shutters for disaster management and home security conflict and safety/security/reliability is compromised.	Conflicts between multiple control logics
(1)	Virus infection on the home GW/edge server A malicious attack on control software allows the attacker to take over the lock control of windows, shutters, and doors.	Vulnerability in the home GW/edge server
(2)	Service interruption of cloud servers	
(3)	Tampering of communication data	

(7) Possible measures

The possible measures that can be taken in these examples are as described in Table A-9.

Table A-9. Measures for the expected risks

Location	Expected threat/damage	Measure	Coordination model	Note
(1)	Home GW/ edge server	For a situation when a conflict occurs between the control that opens the windows for amenity and the control that closes the windows and shutters for disaster management and home security, add a control function in the upper layer that determines which control has higher priority. Safety/security/reliability is prioritized.	EC	Monitoring function (Conflict-Resolving function)
(1)	Home GW/ edge server	Security measures against attacks from malicious intruders on home GW/edge server's control software.	EC	Monitoring function (Intrusion Prevention function)
(2)	Service interruption of cloud servers	Use a typical redundant configuration or other similar measures.	-	-
(3)	Tampering of communication data	Use a typical encryption method or other similar measures.	-	-

(8) IoT high reliability functions and implementation locations

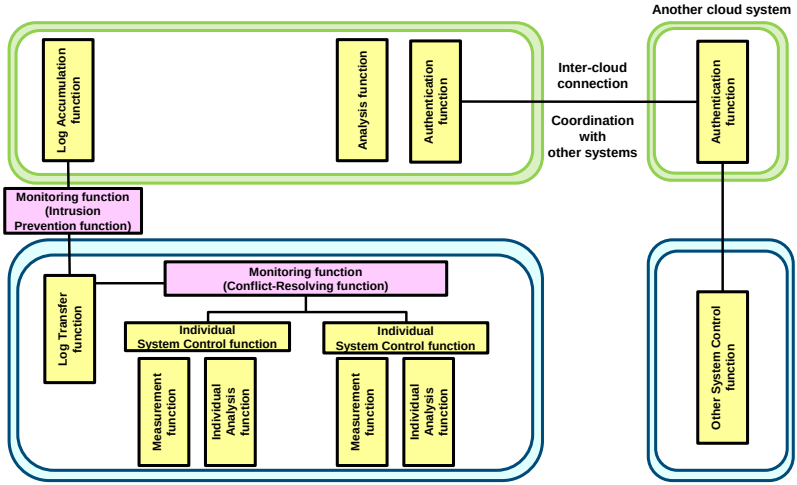


Figure A-16. Resolving conflicts between multiple control systems

If multiple control systems operate in the home at the same time, as shown in the figure above, it is necessary to have a supervisory control system that takes account of the whole situation inside the home and prioritizes the people's lives first and properties second, and applies lower priorities to other elements, such as amenity and entertainment.

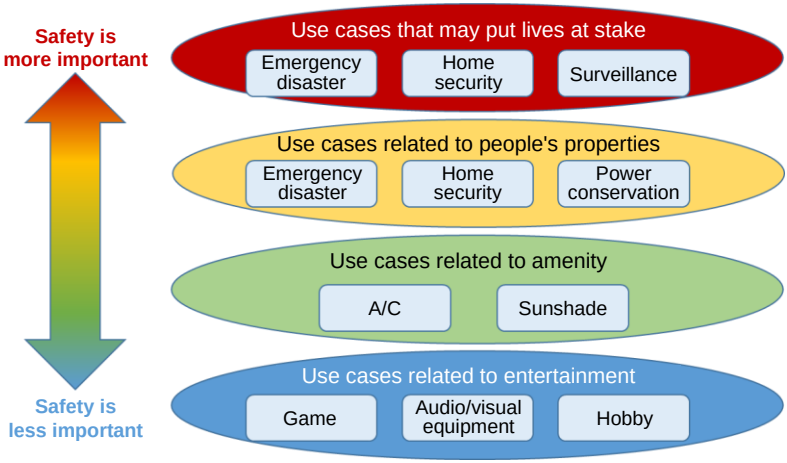


Figure A-17. Prioritization in conflict control

Figure A-18 shows the diagram of the categories of these priorities and the architecture of the home edge server for resolving conflicts. While taking into consideration that new control systems may be added in the future, a system is necessary that can minimize the damage by comprehensively taking into account the priority order of people's lives, properties, amenity, and entertainment, in the order of first to last, in any circumstances. To accomplish this, a supervisory conflict control is necessary that allows you to combine each system as plug-ins and provides optimal capability overall in any system combination.

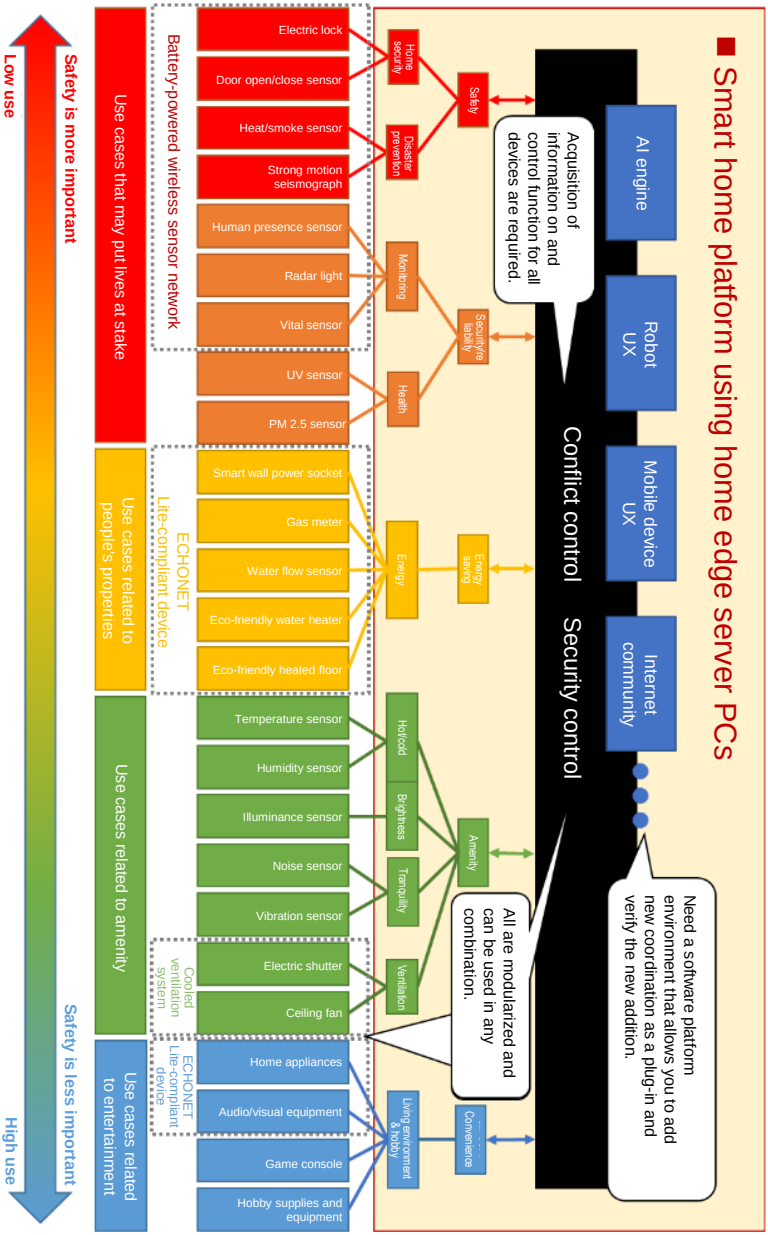


Figure A-18 Diagram of priority categories

UC5. Risk Analysis on Coordination Between Industrial Robots and Power Management

Software Reliability Enhancement Center, Information-technology Promotion Agency

(1) Target sectors of coordination

Industrial Robot System and Power Management System

(2) Overview

This analysis is based on a case where a business owner of a small/medium company is monitoring and operating equipment in a small-scale factory.

In this case, the Production Monitoring System has the functions listed below.

• Abnormality detection

This function coordinates the operation information of the Industrial Robot System and power information of the Power Management System to ensure detection of abnormalities in the Industrial Robot System and Power Management System.

• Factory facility control

This function controls the air conditioning and lighting under the Power Management System, based on the operation status of industrial robots.

(3) Form of coordination

Fog Coordination model

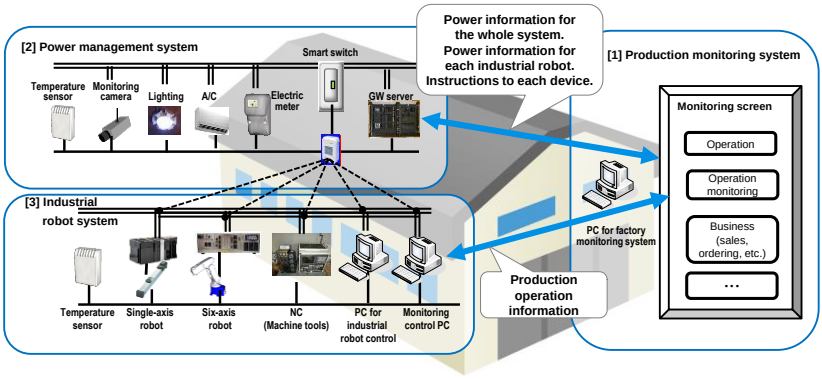


Figure A-19. Form of coordination

(4) Characteristics

This system consists of a Power Management System that monitors the factory's power usage and controls the power consumption, an Industrial Robot System that controls the industrial robots and NC devices to perform machining processes, and a Production Monitoring System that monitors these two systems and performs operations.

The Production Monitoring System coordinates the power information obtained by the Power Management System and production operation information obtained by the Industrial Robot System, and monitors the factory systems for abnormalities and controls these systems to conserve energy.

In this system, spoofing of sensors and other devices or tampering of acquired information for the Power Management System may lead to a malfunction in the factory system's abnormality monitoring or power-saving control. Also, if the individual decisions made by the Industrial Robot System and Power Management System lead to conflicting instructions on the same device, these controls do not succeed in their purposes, and it may also cause malfunctions in the device.

(5) Structural analysis of IoT components

(1) Production Monitoring System

This system obtains power information for the industrial robots from the Power Management System and production operation information from the Industrial Robot System, and then performs abnormality detection by checking their consistencies.

(2) Power Management System

This system controls the power usage as necessary by monitoring it, to keep the power consumption of the whole system below the maximum value.

(3) Industrial Robot System

This system performs machining processes automatically according to the given instructions. While doing so, the system obtains the production operation information for production management.

This system also sends instructions to the A/C devices in the Power Management System, and controls the temperature to maintain it at a level that is suitable for the operation of robots and industrial equipment and for the workers.

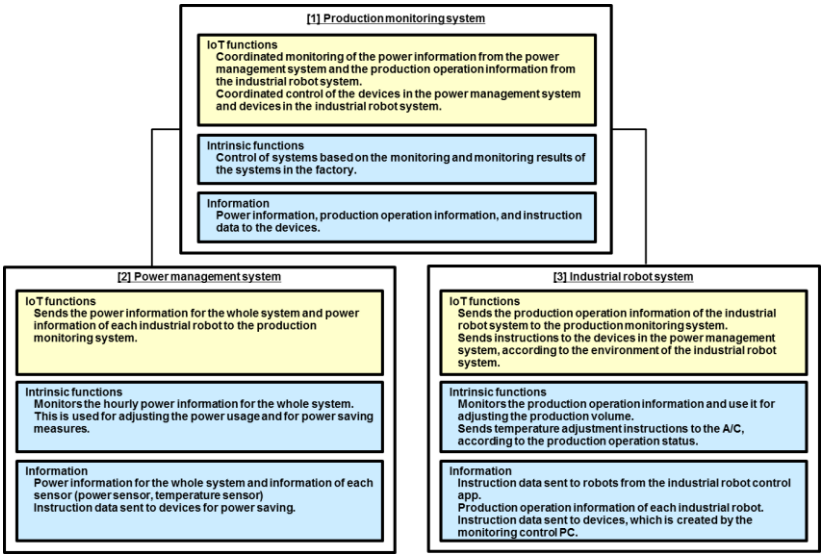


Figure A-20. Structural analysis of IoT components

(6) Expected threats/damage and main factors and issues

The expected risks and main factors are as described below.

Table A-10. Expected threats/damage

Location	Expected threat/damage	Main factors and issues
(1)(2)(3)	Tampering of power information of the whole system or each industrial robot Tampering of production operation information of the Industrial Robot System /System interruption due to failure to detect an abnormality Increase in failure due to unexpected operation continuation Increase in power consumption due to unexpected operation continuation Excess production or underproduction	Low tamper-resistance capability of hardware/software installed on the PC or GW server. Data transmitted on LAN is not protected.
(2)	Spoofing of electric meter or power sensor Connection of a device containing malicious hardware/software /System interruption due to failure to detect an abnormality	No way of checking if the GW server is genuine. No way of checking if the electric meter or power sensor is genuine.
(1)(3)	Tampering or spoofing of monitoring program on the Industrial Robot System /System interruption due to failure to detect an abnormality	No way of checking if the monitoring program is genuine.

(2)(3)	Conflict between contradictory instructions (e.g., instructions to power on and power off the A/C) /Reduced productivity due to A/C failure	Two independent systems may be configured with different priority settings. (Power Control System might prioritize keeping the power consumption below the maximum level, while the Industrial Robot System might prioritize adjusting the temperature to a level appropriate for the workers and devices.)
(1)(2)(3)	Internal fraud or virus that tampers the time settings on PC/GW server /Increase in cost for investigating abnormalities	Inadequate access control for the Time Setting function of the PC and GW server.

(7) Possible measures

The measures for the expected risks are as described below.

Table A-11. Measures for the expected risks

Location	Expected threat/damage	Measure	Coordination model	Note
(1)(2)(3)	Tampering of power information of the whole system or each industrial robot Tampering of production operation information of the Industrial Robot System /System interruption due to failure to detect an abnormality Increase in failure due to unexpected operation continuation Increase in power consumption due to unexpected operation continuation Excess production or underproduction	・ Prevent the tampering of data on memory by strengthening the access control and tamper-resistance capabilities of programs on PCs. ・ Detect tampering by adding message digests or digital signatures on power information and production operation information to check the information's authenticity.	FC	・ Access Control function ・ (Tamper resistant) ・ Monitoring function (Detection of security abnormalities)
(2)	Spoofing of electric meter or power sensor Connection of a device containing malicious hardware/software /System interruption due to failure to detect an abnormality	・ Detect spoofing by having the GW server perform device authentication on electric meters and power sensors.	EC	・ Authentication function (Device authentication) ・ Monitoring function (Detection of security abnormalities)
(1)(3)	Tampering or spoofing of monitoring program on the Industrial Robot System /System interruption due to failure to detect an abnormality	・ Prevent the tampering of programs and data on memory by strengthening the access control and tamper-resistance capabilities of programs on PCs. ・ Detect spoofing by having the Production	FC	・ Access Control function ・ (Tamper resistant) ・ Monitoring function (Detection of security abnormalities) ・ Authentication

		Monitoring System authenticate PC programs and mutually authenticate with the industrial robot control programs.		function (Program authentication)
(2)(3)	Conflict between contradictory instructions (e.g., instructions to power on and power off the A/C) /Reduced productivity due to A/C failure	・ Monitor the instructions sent to the A/C and raise an abnormality alarm if conflicting instructions are sent continuously for a certain period.	FC	・ Monitoring function (Detection of conflicts)
(1)(2)(3)	Internal fraud or virus that tampers the time settings on the PC/GW server /Increase in cost for investigating abnormalities	・ Synchronize the clock settings on all PCs in reasonably short intervals, using NTP, GPS, and other tools.	FC	・ Time Synchronization function

(8) IoT high reliability functions and implementation locations

(1) Access Control, Monitoring, and Authentication functions

As measures against threats on abnormality monitoring, the Access Control function, Monitoring function (detection of security abnormalities), and Authentication function (device authentication and program authentication) are included in the Production Monitoring System, Power Management System, and Industrial Robot System. As a measure for preventing tampering of programs and data for the Monitoring function and functions that control the devices, these functions could also have tamper-resistance capabilities.

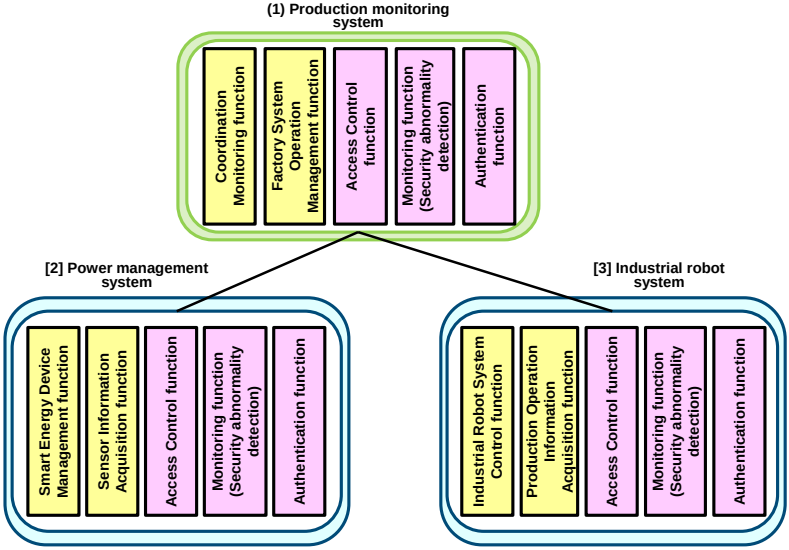


Table A-21. Measures against threats on abnormality monitoring

(2) Monitoring function (Detection of conflicts)

As a measure to detect conflicts between instructions sent from the Power Management System to the A/C to control power usage and instructions sent from the Industrial Robot System to the A/C to control the temperature of the production environment, the Monitoring function (detection of conflicts) is included in the Production Monitoring System.

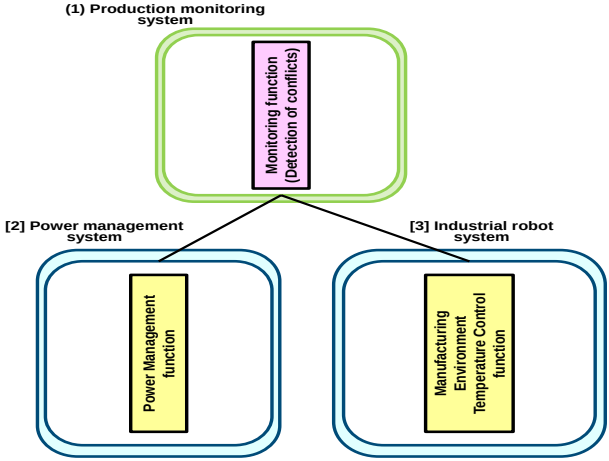


Figure A-22. Detection of conflicts

(3) Time Synchronization function

To ensure the reliability of timestamps of monitored events in each system, the Time Synchronization function is included in the Production Monitoring System, Power Management System, and Industrial Robot System.

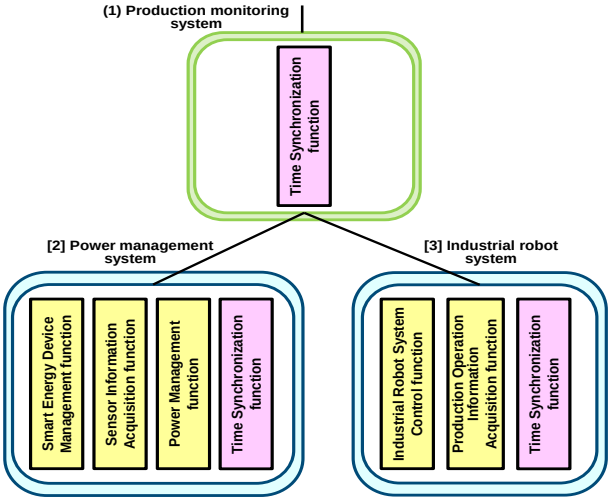


Figure A-23. Time synchronization

Appendix B. Analysis and Organization of Information Regarding High Reliability of IoT

(1) Summary of threats and measures

Table B-1 shows the summary of categories of threats, hazards, and technical measures identified based on the *IoT Safety/Security Development Guidelines* and use cases, when conducting the analysis and information organization for high reliability of IoT, which is described in Chapter 2.

Physical measures, human measures, administrative measures, and technical measures can be implemented as measures against potential threats and hazards. As IoT high reliability functions are technical measures, we focused on the technical measures and organized the gathered information. The technical measures pertain to mainly the design, (designing of) maintenance, and (designing of) operation phases, but we also included those measures that the risk analysis deemed as necessary in the analysis phase.

Table B-1. Summary of threats and measures

	Guideline No.	Guideline	Type of threat/hazard	Main technical measure (function)
Policy	Guideline 1	Formulate a basic policy on safety/security/reliability.	(Not applicable)	(Not applicable)
	Guideline 2	Review the team/employees involved in the effort on safety/security/reliability of IoT.	(Not applicable)	(Not applicable)
	Guideline 3	Prepare for internal fraud and mistakes.	(Not applicable)	(Not applicable)
Analysis	Guideline 4	Identify the objects to be protected.	(Not applicable)	(Not applicable)
	Guideline 5	Identify the risks that may arise due to higher connectivity.	Unauthorized access	Authentication function, Access Control function, Monitoring function (unauthorized access)
			Virus infection	Antivirus function
			Incorrect settings	Initial Setting function
	Guideline 6	Identify the risks that may spread due to higher connectivity.	Conflict between controls	Monitoring function (Detection of conflicts)
	Guideline 7	Identify the physical risks.	(Not applicable)	(Not applicable)

Design	Guideline 8	Create a design that can be complied both individually and as a whole.	Unauthorized use	Authentication function (user authentication, biometric authentication, device authentication)
			Tampering of data	Encryption function (Message) Authentication function
			Tampering of clock settings	Time Synchronization function
			Incorrect access from an unexpected device	Authentication function, Access Control function, Configuration Information Management function
			Virus infection	Antivirus function
	Guideline 9	Create a design that will not impact other connected entities negatively.	Spreading of abnormality.	Monitoring function (fault/failure monitoring and notification) Isolation function Suspend function Diagnostic function
			Service interruption	Degenerate function Redundant Configuration function Recovery function
	Guideline 10	Ensure consistency in the design to achieve safety/security/reliability.	(Not applicable)	(Not applicable)
	Guideline 11	Create a design to ensure safety/security/reliability even when connected to nonspecific devices and systems.	Connection with a device with low reliability.	Access Control function (trust assurance level check)
	Guideline 12	Verify and evaluate the design to achieve safety/security/reliability.	(Not applicable)	(Not applicable)
Maintenance	Guideline 13	Include a function to self-identify its own status and record it.	Failure Unauthorized access	Predictive function Monitoring function (fault/failure monitoring and notification) Log Collection function
	Guideline 14	Include a function to maintain safety/security/reliability over a long period.	Vulnerability	Remote Update function
Operation	Guideline 15	Identify the IoT-related risks even after the product is shipped and release relevant information.	(Not applicable)	(Not applicable)
	Guideline 16	Communicate to relevant businesses on compliance matters after the product is shipped.	Improper initial settings	Initial Setting function
			End of support period	Lifetime Management function
	Guideline 17	Let the public know the risks that may arise due to better connectivity.	Information leakage when reused or discarded.	Erase function

(2) Related standards and guides

The following are standards and guides related to IoT that we referenced when selecting the IoT high reliability functions described in 2.2.

Table B-2. Related standards and guides referenced when selecting IoT high reliability functions

Standard/Guide	Organization	Description
Industrial Internet of Things Volume G4:Security Framework [10]	IIC	Framework that summarizes the security measures and processes that are related to industrial IoT.
Security Guidance for Early Adopters of the Internet of Things (IoT) [11]	CSA	Security controls for organizations planning to introduce IoT.
IoT Security Guide for Consumers [12]	Japan Network Security Association	Security-related matters that should be considered when making IoT devices available as a vendor. This guide uses the two axes below that intersect orthogonally to organize the threats and measures. ・ Start of use (Introduction) — Normal operation — Replacement (Disposal) ・ Abandoned (Stray) — Normal operation — Abnormality
Security Design Guide for IoT Development [13]	Security Center, IPA	This guide describes the security threats and measures that can be expected when using IoT devices and those that can be expected in an environment that uses IoT devices.
IoT Security Guidelines [14]	GSMA	Guideline on secure IoT products and services and guideline for network operators.
Security Guidelines for Product Categories [7]	CCDS	Security guidelines for products in four categories: Automotive On-board devices, IoT gateway, ATMs, and POS.

Appendix C References

[1] IPA, "つながる世界の開発指針," [Online]. Available: https://www.ipa.go.jp/sec/publish/tn16-002.html.

[2] 経済産業省　産業構造審議会　商務流通情報分科会　情報経済小委員会　分散戦略 WG, "中間とりまとめ," [Online]. Available: http://www.meti.go.jp/report/whitepaper/data/pdf/20161129001_01.pdf.

[3] 高田　信彦、南　俊博, 情報セキュリティ教科書, 東京電機大学出版局, 2008.

[4] 一般社団法人重要生活機器連携セキュリティ協議会, "重要生活機器の脅威の事例集　Ver.1.2," [Online]. Available: https://www.ccds.or.jp/public/document/other/CCDS_CaseStudies_v1_2.pdf.

[5] 一般財団法人日本自動車研究所, "平成 26 年度　戦略的イノベーション創造プログラム　V2X（Vehicle to X）システムに係わるセキュリティ技術の海外動向等の調査," [Online]. Available: http://www.meti.go.jp/meti_lib/report/2015fy/000326.pdf.

[6] 独立行政法人情報処理推進機構, "つながる世界のセーフティ＆セキュリティ設計入門," [Online]. Available: https://www.ipa.go.jp/files/000055007.pdf.

[7] 一般社団法人重要生活機器連携セキュリティ協議会, "製品分野別セキュリティガイドライン," [Online]. Available: https://www.ccds.or.jp/public_document/index.html.

[8] 一般社団法人日本電機工業会　HEMS 専門委員会, "外部システムとの連携における HEMS の定義," [Online]. Available: http://www.meti.go.jp/committee/kenkyukai/energy_environment/energy_resource/pdf/004_03_03.pdf.

[9] 一般社団法人エコーネットコンソーシアム, "ECHONET Lite 規格書," [Online]. Available: https://echonet.jp/spec_g/#standard-01.

[10] Industrial Internet Consortium, "Industrial Internet of Things Volume G4: Security Framework," [Online]. Available: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf.

[11] 一般社団法人日本クラウドセキュリティアライアンス, "IoT 早期導入者のためのセキュリティガイダンス(日本語バージョン)," [Online]. Available: https://www.cloudsecurityalliance.jp/newsite/wp-content/uploads/2016/02/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things_J_160224.pdf.

[12] 特定非営利活動法人日本ネットワークセキュリティ協会, "コンシューマ向け IoT セキュリティガイド," [Online]. Available: http://www.jnsa.org/result/iot/.

[13] IPA, "IoT 開発におけるセキュリティ設計の手引き," [Online]. Available: https://www.ipa.go.jp/files/000052459.pdf.

[14] GSM Association, "IoT Security Guidelines," [Online]. Available: http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/.

The Guidance is created by the Working Group on IoT High Reliability, Software Reliability Enhancement Center (SEC), Technology Headquarters, Information-technology Promotion Agency (IPA).

Editors/authors (titles omitted)

Chief editor/author	Shuji Morisaki, Nagoya University
Member	Kosuke Ito, Connected Consumer Device Security Council (CCDS)
	Hiroyuki Kazuma, Japan Electronics and Information Technology Industries Association (JEITA)
	Akira Tsuge, YRP R&D Promotion Committee / WSN-ATEC General Incorporated Association
	Kazutaka Tsuji, The Japan Electrical Manufacturers' Association
	Yoshio Nakagaki, Denso Corporation
	Takashi Murakami, ECHONET CONSORTIUM
	Kenji Yoshifu, Communications and Information Network Association of Japan (CIAJ) / NEC Corporation
IPA/SEC	Masayoshi Nakao
	Shinji Miyahara
	Tomoko Kaneko
	Mitsuyoshi Kozaki
	Hidefumi Maruyama

Guidance for Practice Regarding “IoT Safety/Security Development Guidelines”
[IoT High Reliability Functions]

December 26, 2017 First edition

Editorial supervisor	Software Reliability Enhancement Center (SEC), Technology Headquarters, Information-technology Promotion Agency (IPA)
Publisher	Takaaki Matsumoto
Publishing office	Information-technology Promotion Agency (IPA) Bunkyo Green Court Center Office 16F 2-28-8 Hon-komagome, Bunkyo-ku, Tokyo 113-6591, Japan URL http://www.ipa.go.jp/sec/