IoT Safety/Security Design Tutorial

- Important Points to be understood by Software Developers toward the Smart-society -

The Software Reliability Enhancement Center, Technology Headquarters,
Information-technology Promotion Agency

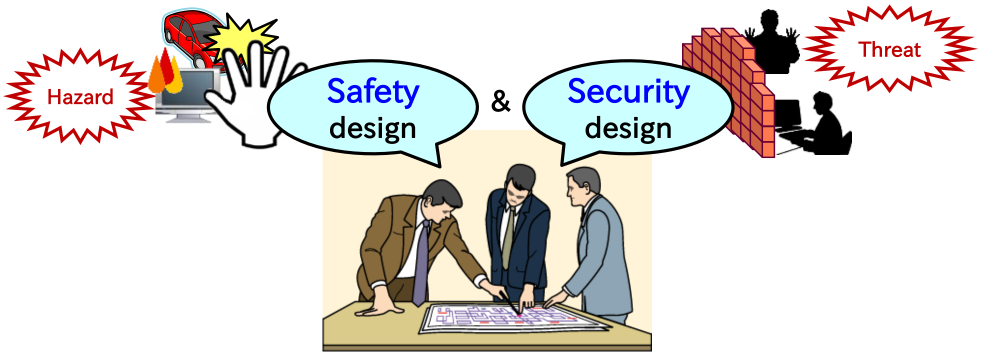
Introduction

i) Overview

This document is created by a Working Group (WG) established under the Software Reliability Enhancement Center, Technology Headquarters, Information-technology Promotion Agency (IPA/SEC). This tutorial document explains safety and security design methods for achieving Safety/Security of devices and systems, and visualization methods that enables logical explanations of design quality to third parties in software reuse and distribution, etc., in an easy-to-understand manner. The scope of explanation includes risk evaluation of devices and systems required in pre-design phases.

This document uses devices that are essential to our daily lives, including automobiles, smartphones, health care devices, and smart home electrical appliances, etc. (hereinafter referred to as “consumer devices”), as examples to help readers to have an image of concrete devices and systems. When developing these consumer devices, not only safety design (ensuring safety in the design phase) but also, similar to PCs and other information devices, security design (considering vulnerability reduction and measures against threats in the design phase) is required because in recent years they are connected to networks. The above-mentioned consumer devices are therefore selected as “examples of products for which Safety/Security should be achieved” in this document.

At present, safety and security design are assumed to be usually carried out in independent processes, but for the reason given above, they need to be promoted with relevance.



Design quality evaluation through “visualization”

ii) Intended readers

Intended readers of this document and the contents directed for each reader are as shown in the following table. Since safety and security designs are important processes for protecting users' bodies and properties against hazards and threats, this document should be read by everyone who is related to products/systems concerned, from the management level to operation/support engineers.

Intended readers of this document

Structure of this document Intended readers	Chapters 1 and 3 Safety and security	Chapter 2 Accident cases	Design/development/visualization methods		
			Chapter 4 Safety design	Chapter 5 Security design	Chapter 6 Visualization
Management/planning	○	○			
Design/development	○	○	○	○	○
Evaluation/verification	○	○	○	○	○
Operation/support	○	○			○

iii) Ideas of this document

IPA/SEC published the previous version of this document, a tutorial document for improving the safety of systems around us, in 2006 [1]. In recent years, however, "security design" to prevent tapping, software falsification, etc., is becoming important for consumer devices. In addition, security incidents involving consumer devices can also affect "Safety". Therefore, the descriptions of both "safety design" and "security design", as well as the description of visualization of their design quality, are provided in this document.

iv) List of abbreviations

The following table shows abbreviations used in this document and their full names.

Abbreviation	Full name
ASIL	Automotive Safety Integrity Level
CAPEC	Common Attack Pattern Enumeration and Classification
CC	Common Criteria for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
CSIRT	Computer Security Incident Response Team
CVSS	Common Vulnerability Scoring System
EAL	Evaluation Assurance Level
ECC	Error Check and Correction
EDSA	Embedded Device Security Assurance
EVITA	E-safety vehicle intrusion protected applications
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability
ISIRT	Information Security Incident Response Team
IEC	International Electrotechnical Commission
IPA	Information-technology Promotion Agency, Japan
IPA/SEC	Information-technology Promotion Agency, Japan Software Reliability Enhancement Center
JIS	Japanese Industrial Standards
IoT	Internet of Things
ISO	International Organization for Standardization
MBD	Model-Based Development
MBSE	Model-Based Systems Engineering
MoD	UK Ministry of Defence
OMG	Object Management Group
PKI	Public Key Infrastructure
PL	Performance Level
PP	Protection Profile
SIL	Safety Integrity Level
SQuaRE	Systems and software Quality Requirements and Evaluation
ST	Security Target
STAMP	Systems-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis

Table of contents

Chapter 1

Safety and security for Smart-systems

Recent systems work with various devices and clouds through network connections. In these “Smart systems”, security threats can spread over networks and affect software-controlled safety functions of other systems. Appropriate risk treatment, safety and security design, and sharing design information through visualization are therefore important.

1.1 Systems and risks in the Smart-society

(1) Image of the Smart-society

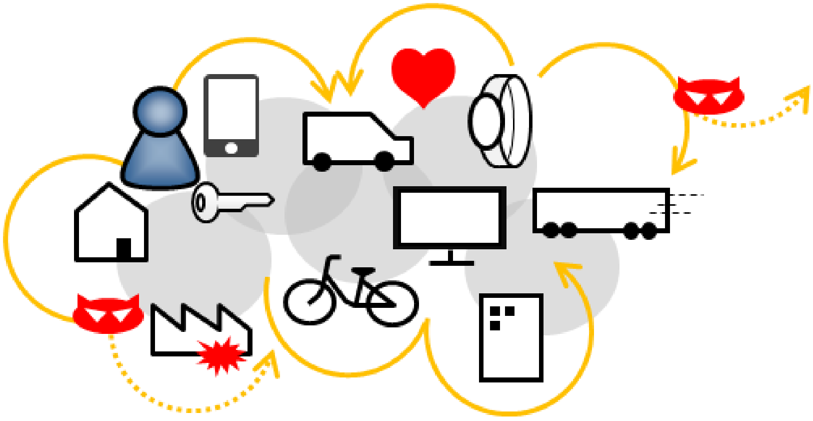


Figure 1-1 Image of the Smart-society

With the advancement in information and communication technologies, consumer devices that worked individually in the past are now connected to each other through networks to jointly provide services to users and to automatically collect/analyze data and send it to other consumer devices. More devices and systems in different sectors are expected to work together in the future.

(2) Systems in the Smart-society

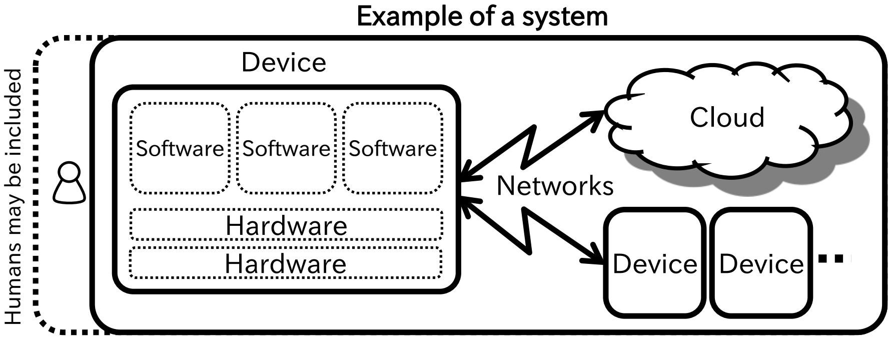


Figure 1-2 Image of a system in the Smart-society

In this document, a “system” refers to a configuration in which devices are connected with clouds and other devices through networks and work together in a “systematic” manner. Device failures or malfunctions can affect other devices through networks. In addition, connection to external systems like clouds increases the risk of attacks like viruses. In the Smart-society, Safety/Security of not only individual devices but also the entire system must be considered.

1.2 Risk treatment through safety and security

(1) Safety and security from the point of view of risks

In businesses, there are various business risks, including competition, disasters, etc. For devices and systems in the Smart-society, however, dealing with safety and security risks such as accidents and attacks is also necessary. This document focuses on these risks, and explains the necessity of analyzing and reducing them.

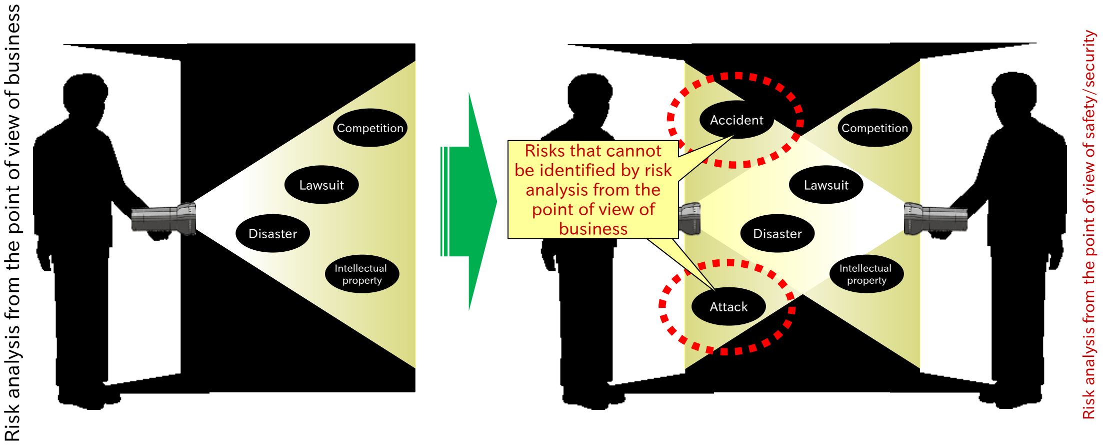

Risk analysis from the point of view of business
Competition
Lawsuit
Disaster
Intellectual property
Risks that cannot be identified by risk analysis from the point of view of business
Accident
Competition
Lawsuit
Disaster
Intellectual property
Attack
Risk analysis from the point of view of safety/security

Figure 1-3 Image of risks covered in this document

First, safety and security risks are explained. For devices and systems used in businesses, there may be factors such as software defects, vulnerabilities, etc., that can potentially cause harm to users' bodies and properties by malfunctions or third party attacks (factors affecting safety are called "hazards" and factors affecting security "threats"). In case of actual harm, there would be significant business impacts, including compensation for damages, recall of defective devices, responding to the System for Report and Publication of Product Accident Information [4] under the Consumer Product Safety Act, etc.

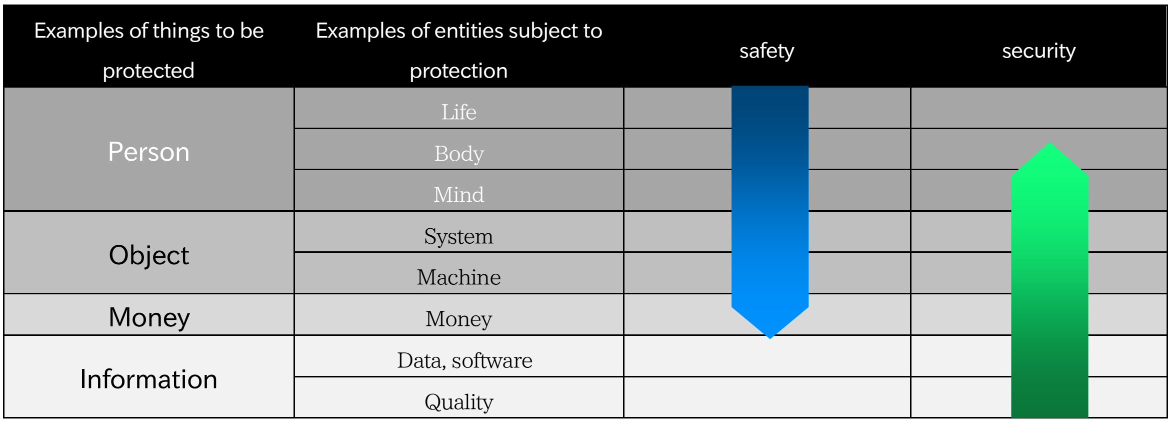
There is a method for evaluating safety and security risks from the probability of occurrence of hazards and threats and the severity of damage caused by them. Even when the damage caused is severe, the risk would be small if the probability is close to zero. In contrast, the risk would be large even for slight damage if the damage can spread through networks. Since many functions that improve safety (hereinafter referred to as "safety functions") are controlled by software, the risk would be enormous if security threats affect software on other devices through networks and cause safety functions to malfunction on a wide scale.

In the Smart-society, damage from hazards and threats can spread on a wide scale and pose significant risks to companies' businesses. Active treatment is therefore needed.

(2) Safety and security from the point of view of things to be protected

Examples of “damage” subject to safety include injuries from automobile collisions, houses burned down by devices igniting, etc. In contrast, “damage” subject to security include, for instance, unauthorized use and interruption of devices and systems, software and data falsification, personal information leakage, fraudulent electronic payments, etc. As such “damage” is wide-ranging, and things to be protected must first be identified in safety and security design.

In addition, since security threats can affect safety functions, things to be protected by security design are expanding to cover those protected by safety as shown in Figure 1-4.



Examples of things to be protected	Examples of entities subject to protection	safety	security
Person	Life		
	Body		
	Mind		
Object	System		
	Machine		
Money	Money		
Information	Data, software		
	Quality		

Figure 1-4 Expanding scope of things to be protected by safety and security

After determining things to be protected, evaluating the risks against them and reducing the risks to a tolerable level by safety and security design will enable the provision of safe and secure services.

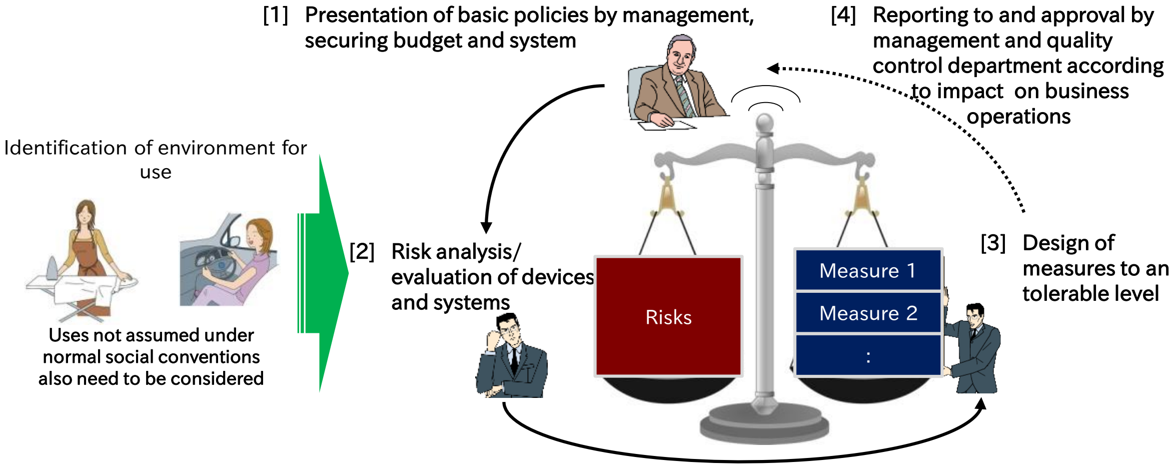

[1] Presentation of basic policies by management, securing budget and system
[4] Reporting to and approval by management and quality control department according to impact on business operations
Identification of environment for use
Uses not assumed under normal social conventions also need to be considered
[2] Risk analysis/ evaluation of devices and systems
Risks
Measure 1
Measure 2
:
[3] Design of measures to an tolerable level

Figure 1-5 Safety and security measures based on basic policies

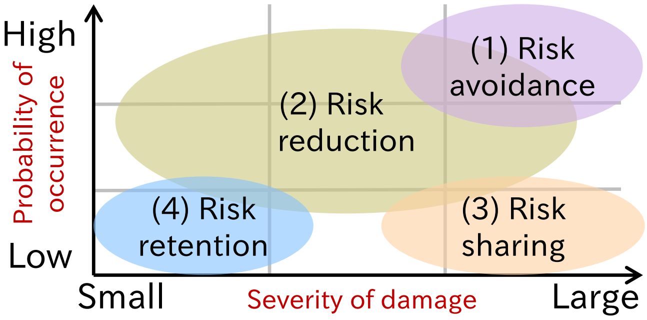
In information security in business systems, risk treatment is organized in four ways as shown in Figure 1-6. Security design of devices and systems requires the discussion of methods for dealing with risks with consideration also given to impacts on safety functions.

(1) Risk avoidance Eliminating the possibility of risk occurrence by deleting functions at risk or replacing them with completely different methods.

(2) Risk reduction Reducing the probability of occurrence and severity of damage by taking measures against risks.

(3) Risk sharing Transferring risks to others by buying insurance, replacing the components at risk with products/systems of other vendors, etc.

(4) Risk retention Accepting risks as being in the tolerable range without taking any particular measures to reduce them if the risks are small enough.



Source: Prepared based on a figure from “情報セキュリティマネジメントと PDCA サイクル” [5]

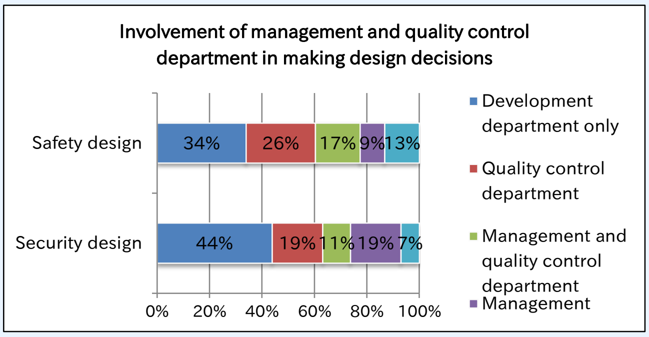
Figure 1-6 Guidelines of risk treatment methods based on the probability of occurrence and severity of damage

Column 1 Who will decide important matters concerning safety and security design?

- From "Questionnaire survey for promoting visualization of safety and security design" -

Conducted in 2015

In order to identify the actual situation of the implementation of safety and security design, a questionnaire survey was conducted in the four sectors that are taking initiatives in safety and security efforts, namely automotive, smartphone, health care, and smart home electrical appliances sectors. The results revealed that the necessity of safety and security design has been recognized with the vast majority of respondents answering that safety and security design is necessary (both safety and security designs are necessary: 76%, only security design is necessary: 19%, only safety design is necessary: 4%). Although the necessity of safety and security design has been recognized, more than half of the respondents answered that they did not have basic policies on safety and security design that could actually be used as decision criteria (safety: 65%, security: 54%). Additionally, to the question "Are the management and quality control department managers involved in making safety and security design decisions?", 34% and 44% answered that safety and security decisions, respectively, were made on-site (by development departments) and the managers were not involved in making these decisions.



The results suggest that many organizations do still not yet have basic principles for making decisions on important matters concerning safety and security (including requirements/specifications) on-site and little involvement of the management in making decisions on designs that can lead to serious incidents or accidents, leaving such decisions to be made on-site.

A survey is also conducted on visualization using an assurance case, etc., which can also be used as a powerful tool for sharing information with stakeholders, including the management, quality control department managers, etc. The results showed that common tools (GSN, CAE, and D-Case, etc.; see p.74) have not yet been fully introduced (introduction results: safety: 15%, security: 3%). This suggests the situation where appropriate explanations cannot be made even where shareholders' decisions are needed.

Questionnaire survey URL: http://www.ipa.go.jp/sec/reports/20150910.html

1.3 Necessity of visualization of safety and security design

“Visualization of safety and security design” in this document refers to logically explaining safety measures, security treatment, etc., which tend to be rather complex, by using evidence for third parties. The purposes of visualization include support for design/development, verification by third-party testing organizations, acquisition of certifications of industrial and international standards, etc.

(1) Design/development support

In the respective phases of design and development, “visualization” can be utilized for sharing the design content. Figure 1-7 shows the concrete effects of visualization.

Example of effects	Outline
1 Understanding the design content when designing and reusing software.	Utilizing visualization for understanding the design content when reusing software for new product development and version upgrading.
2 Sharing design information with stakeholders	Utilizing visualization for sharing design information with relevant personnel within a company or providers of collaboration services. Visualization can also be utilized for making adjustments between safety and security designs.
3 Traceability, accountability	Utilizing visualization for verifying the design content in case problems arise and explaining the relationships between the problems and the design.

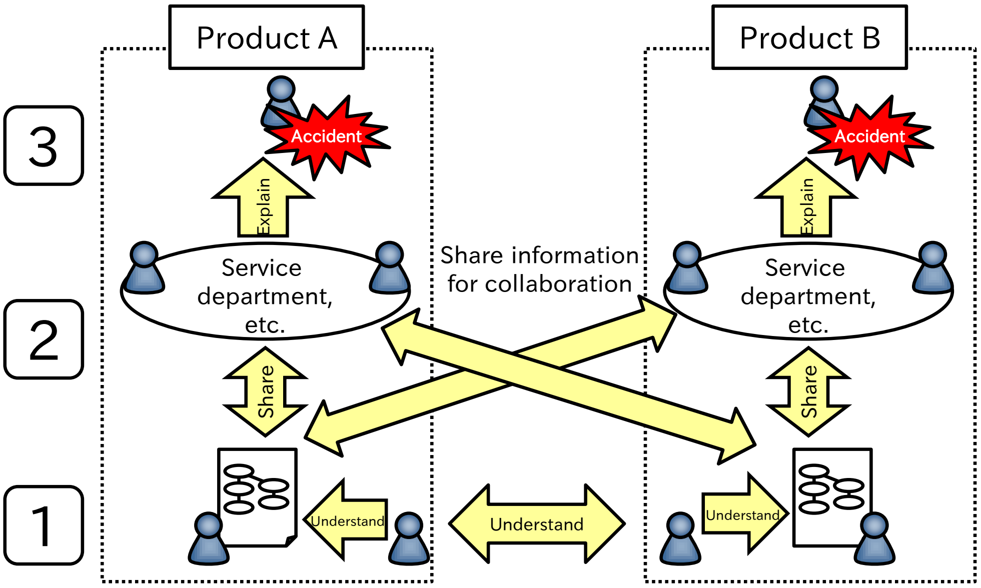


Figure 1-7 Expected effects of visualization of safety and security design

(2) Acquisition of industrial and international standards certifications

Certifications can be utilized for explaining that the safety and security designs confirm to industrial and international standards. Depending on the standards, “Assurance Case”, a visualization method, may be required (see 6.2, p.73).

1.4 Quality assurance in the Smart-society

When devices and systems of different sectors are connected to each other, the effects of accidents and attacks that occurred against some device may propagate to other devices through networks. In Smart-systems, advisability of information provision, reliability of information and control signals received, service coverage, etc., must be determined based on the safety and security levels of the connected devices and systems.

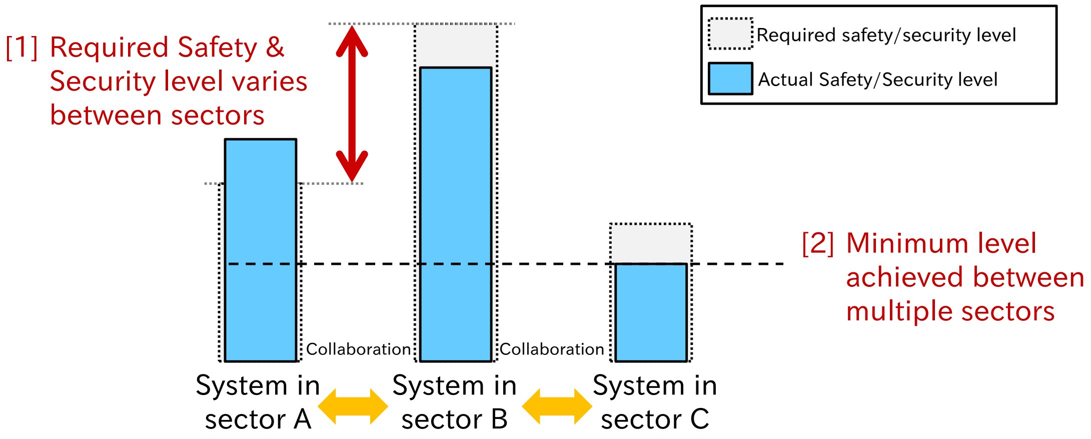

[1] Required Safety & Security level varies between sectors
Required safety/security level
Actual Safety/Security level
[2] Minimum level achieved between multiple sectors
Collaboration
Collaboration
System in sector A
System in sector B
System in sector C

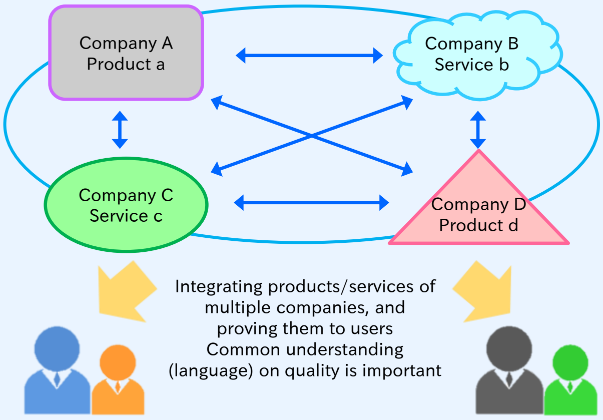
Figure 1-8 Approaches to quality in the Smart-society

Moreover, different sectors, including automotive, smartphone, health care device, and smart home electrical appliances sectors, have their own histories and backgrounds, and thus their approaches to safety and security also vary.

As described above, visualizing safety and security designs of each device/system and sharing them among stakeholders of different sectors will enable understanding the approaches of other sectors, evaluating quality of device/system designs, and determining service coverage according to the safety and security levels. Visualization of design quality is therefore essential to achieving Safety/Security in the Smart-society.

Column 2 Quality model in the Smart-society - “SQuaRE” as a common language -

"Smart-system"



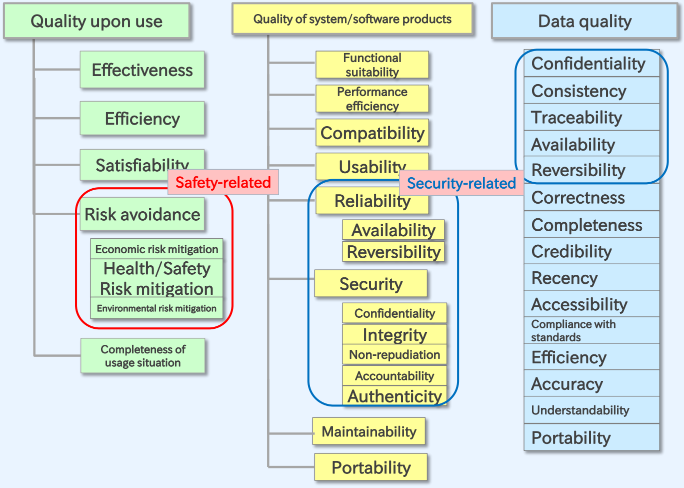
Integrating products/services of multiple companies, and proving them to users
Common understanding (language) on quality is important

As the roles of products that utilize IT in society are increasing, users’ expectations are not limited to their functions but also diversified to include safety and security, comfort, enjoyment, and contribution to business as well as a higher level of satisfaction. In addition, cloud services that utilize smartphones serve as “Smart-systems” in which various business operators who have not previously had any contact are connected to each other. However, because the definition of and approaches to quality expected by stakeholders, including various types of users and business operators involved in the products/services, etc., may be different, having a common understanding among different stakeholders is difficult at present.

A quality model provided in the international standard “SQuaRE: ISO/IEC 25000 series” can be effectively used in such cases. SQuaRE serves as a common language among stakeholders who have not previously had any contact and enables them to clarify various needs in a common framework. Safety and security subject to this guidebook are also included as part of the quality model of SQuaRE.

IPA published a guidebook for product/service providers, which describes the basic knowledge and utilization of SQuaRE. Readers are advised to make effective use of SQuaRE in developing “Smart-systems”.

Quality model of SQuaRE (ISO/IEC 25000 series)



■ Guidebook

Book: つながる世界のソフトウェア品質ガイド (published in 2015)

http://www.ipa.go.jp/sec/publish/20150529.html

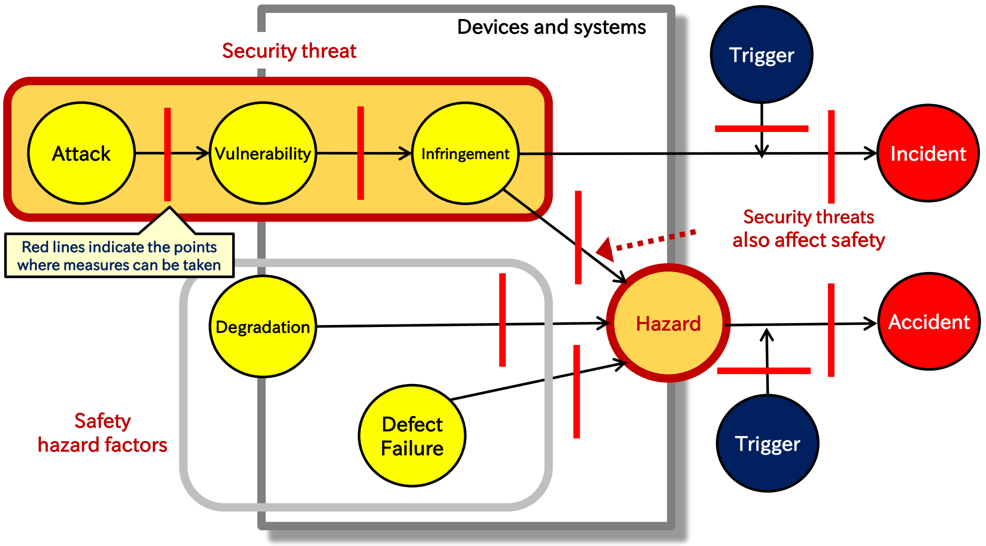
Chapter 2

Accident and incident cases

Modern software undertakes an important role of continuously supporting daily life and society in every situation. Although the utmost efforts have been made in the development to prevent safety accidents and security incidents due to software, reviews are necessary to respond to technological innovations and changes in society. As for reference, accident and incident cases are presented here.

2.1 Mechanisms of occurrence of accidents and incidents

Understanding the mechanisms of occurrence is important for preventing accidents and incidents. Figure 2-1 shows examples of the processes of occurrence of accidents and incidents. Multiple causes shown in yellow lead to accidents/incidents in red through hazards/threats in orange. Red lines in between them indicate the places where countermeasures can be taken. [6] [7]



Source: Prepared based on "The Yellow Book", UK RSSB, and "SECURITY AND SAFETY MODELLING FOR EMBEDDED SYSTEMS", SESAMO Project

Figure 2-1 Processes of occurrence of safety and security damages

This chapter presents accident and incident cases, and discusses at which points in the figure above they could have been stopped. The relevant terms are defined in international standards on safety and security, but many of them may be unfamiliar to readers. Table 2-1 shows how these terms are used in this document.

Table 2-1 Use of safety and security terms in this document

Concept	Terms used in this document	
	Safety	Security
1)Undesirable event	Accident	Incident
2)Direct source of danger that causes the event of 1)	Hazard	Threat
3)Weakness, problem, or source of danger of devices and systems in which 2) is caused	Failure, defect, degradation	Vulnerability, intrusion

2.2 Accident cases

Case 1 Following train unable to enter the platform - Overlooked defects due to incomplete identification of operation patterns -

Event

A railroad company had an error in controlling trains using the same platform of a station, resulting in the following train being unable to enter the platform. More concretely, despite the preceding train being turned back and departing from the platform, control signals for the preceding train continued to be sent out and blocked control signals for the following train from being sent out, thus disabling the following train from entering the platform.

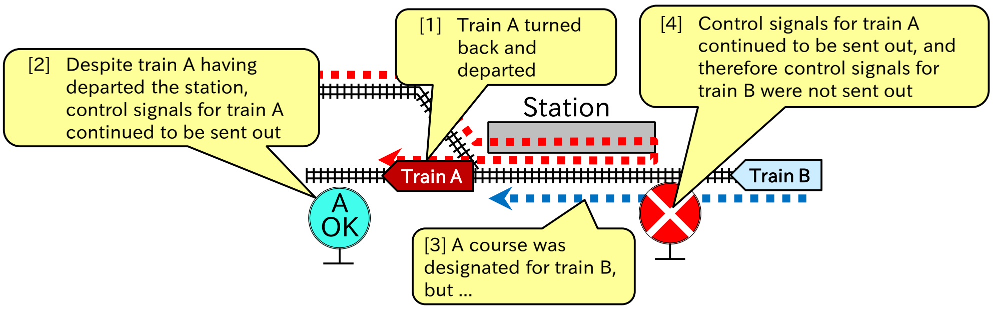

[1] Train A turned back and departed
[2] Despite train A having departed the station, control signals for train A continued to be sent out
[4] Control signals for train A continued to be sent out, and therefore control signals for train B were not sent out
Station
Train A
Train B
A OK
[3] A course was designated for train B, but ...

Figure 2-2 Failure occurrence situation at station [8]

Cause

Tests using actual trains had been conducted prior to going live, but identification of test scenarios was incomplete, and the above-mentioned case was left out and not tested. In addition, there was no verification environment for testing system behavior in a comprehensive manner.

Tips for measures

As will be described in Chapter 4, achieving safety requires identification of hazards and conducting risk evaluation for every possible case. This accident did not lead to any harm to human life or facilities, but complete identification of patterns and development of a verification environment through the use of simulation are necessary to enable verification of all operation cases without omission.

⇒ For the identification of hazards, see 4.2.1, p.36

Case 2 Extended braking distance - Malfunction of safety functions -

Event

In August 2014, an automobile company released the following recall information.

> Improper programing of the EV-ECU which controls the brake vacuum pump may cause the ECU to make the false judgment as if the contact point in the relay is being stuck. As a result, the brake warning lamp may illuminate with the warning sound causing the brake vacuum pump function to be stopped. If use continues under this condition, the stopping distance could increase.

Source: Excerpt from “リコール・改善対策の届出”, Ministry of Land, Infrastructure, Transport and Tourism, Japan

The brake booster uses a vacuum to multiply the driver’s braking force transmitted through a brake pedal, which is then transmitted to the brake unit. The brake unit still operates even if the brake vacuum pump function is stopped, but requires larger force. Therefore, the braking distance may be extended.

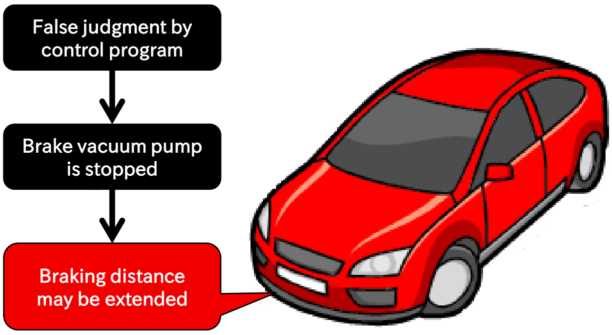

False judgment by control program
Brake vacuum pump is stopped
Braking distance may be extended

Figure 2-3 Danger caused by false judgment of control program

Cause

It was assumed that, due to a defect of the ECU control program, a false judgment that a failure had occurred was made, causing the brake vacuum pump function to stop to prevent a more severe accident from occurring.

Tips for measures

The design quality of safety functions, which are included to reduce risks such as accidents, even when a failure or malfunction occurs, is expected to be improved to avoid the functions themselves from malfunctioning.

⇒ For the improvement of design quality, see 4.2.3, p.45

Case 3 Safety functions of gas meters stopped operating - Operation bases for safety functions was stopped -

Event

In 2003, the Japan Gas Association and the Ministry of Economy, Trade and Industry, Japan made an announcement that a defect was found in the controller software of some models of microcomputer gas meters, which might cause safety functions, including gas flow monitoring/shut-off functions, earthquake sensitive shut-off functions, etc., and communication functions to stop operating, and thus approximately 27,000 units of these models would be replaced. There was no problem, however, in the measurement of the amount of gas used.

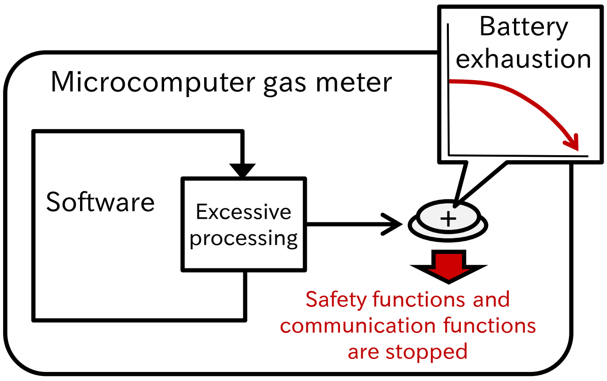


Figure 2-4 Safety functions of gas meters stopped operating

Cause

The valid period of verification of gas meters is between 7 to 10 years, and internal batteries of microcomputer gas meters are designed to generally last for that period. Due to a software defect, however, internal batteries rapidly run out, causing low battery voltage in approximately a year and a half and various functions to stop operating correctly.

Tips for measures

This case provides a good example that even if the quality of safety functions themselves is high, safety cannot be ensured if core functions of devices and systems (internal batteries in this case) become unavailable. Many modern gas meters have functions to ensure safety by cutting off the gas supply when internal batteries run out, but the hazard (battery exhaustion) should have been identified in risk analysis of the safety design and dealt with.

⇒ For the assumption of hazards, see 4.2.1(3), p.38

Case 4 Cardiac pacemakers stopped operating - Products that must never stop, stopped operating due to a failure -

Event

In February 2007, a medical device distribution company made an announcement that it would correct system software for cardiac pacemakers because they would malfunction under certain conditions.

Cardiac pacemakers are supporters to help hearts beat at a normal rhythm by detecting (sensing) heartbeats that are discontinuous or exceeding a certain interval and delivering electrical stimulus to hearts.

In this particular event, an announcement was made that in situations where electrical stimulus should be delivered to correct heartbeats, the function was suspended (a defect) under certain conditions, thus disabling hearts to beat at a normal rhythm and possibly causing symptoms that patients had before implanting pacemakers, including shortness of breath, lassitude, headaches, fainting, etc.

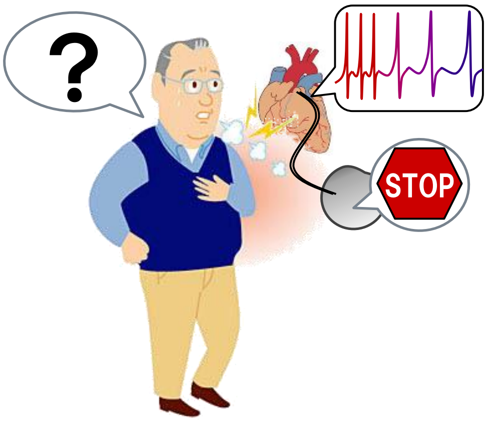


Figure 2-5 Cardiac pacemakers stopped operating

Cause

Due to a defect in the system software, suppression of pacing occurred, triggered by some automatic processing.

Tips for measures

Software defects can exist even in devices and systems that can affect people's lives. Devices and systems requiring safety treatment include not only those such as automobiles that can protect people's lives by safely stopping in case of failure but also those that are not allowed to stop even in the case of failure because they are essential to people's health and lives. For the latter devices and systems, secondary and even tertiary measures may be required in addition to normal safety measures.

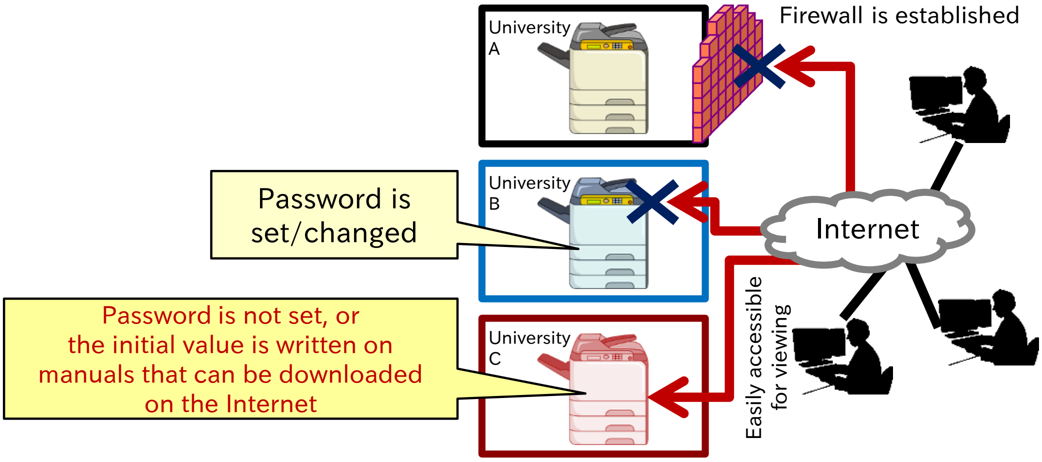
⇒ For safety treatment, see Chapter 4, p. 34

2.3 Incident cases

Case 1 Data in multi-function printers happened to be externally accessible - Important security treatment was left to users -

Event

In 2013, a newspaper reported that multi-function printers installed in universities, happened to be externally accessible via the Internet. There would have been no problem if firewalls were installed or passwords were properly set/changed, but at some universities copied data stored on multi-function printers, including resident cards, driver's licenses, medical questionnaires for health examinations, etc., were openly accessible.


University A
Firewall is established
University B
Password is set/changed
Internet
University C
Password is not set, or the initial value is written on manuals that can be downloaded on the Internet
Easily accessible for viewing

Source: Prepared based on an article on the website of Yomiuri Shimbun

Figure 2-6 Data in multi-function printers happened to be externally accessible

Cause

The fact that the manufacturers did not set administrator passwords and/or made manuals on which the initial passwords (such as "123456") were written openly available on the Internet is considered to be problematic. The problem also lies in the fact that they did not assume multi-function printers installed in universities were unintentionally connected to the Internet without firewalls, and thus failed to give advice upon installation.

Tips for measures

Assuming that users may not have sufficient security knowledge and the usage environment may not be sufficiently secure, the manufacturers should have ensured password setting/change, limited access in cases where passwords were not properly set, and provided users with appropriate advice.

⇒ For security design methods, see 5.2.3, p.59

Case 2 Cardiac pacemakers being able to be stopped wirelessly - Not only safety but also security needs to be considered -

Event

In 2012, a U.S. researcher published an experiment, showing that transmission equipment can make cardiac pacemakers deliver a fatal electric current to hearts or falsify software in the pacemakers from a distance of less than 10m. Similar experimental research was also conducted in 2008; at the time the U.S. Government Accountability Office (GAO) urged the U.S. Food and Drug Administration (FDA) to discuss this matter, and the FDA issued a warning to medical device manufacturers.

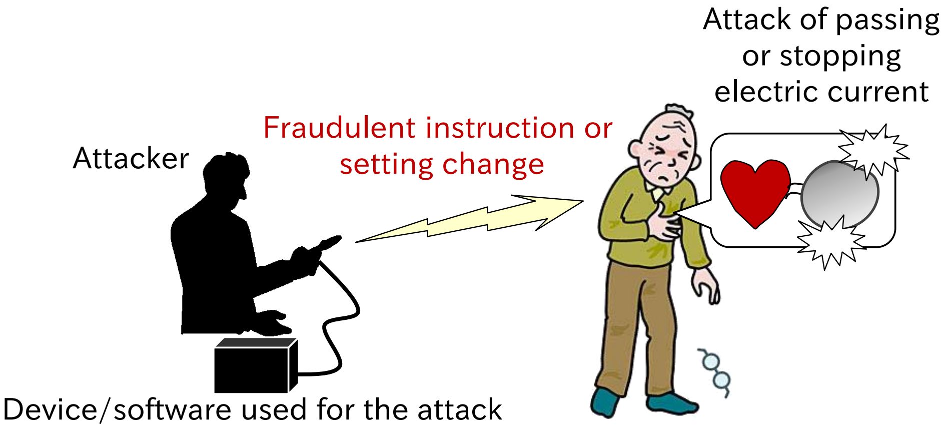

Attack of passing or stopping electric current
Fraudulent instruction or setting change
Attacker
Device/software used for the attack

Figure 2-7 Vulnerability of pacemakers

Cause

The quality and safety of pharmacological products and medical devices are ensured by a number of laws and regulations, but standards and legal systems have not yet been sufficiently developed for their security. The manufacturers also seemed to not have considered intentional attacks.

Tips for measures

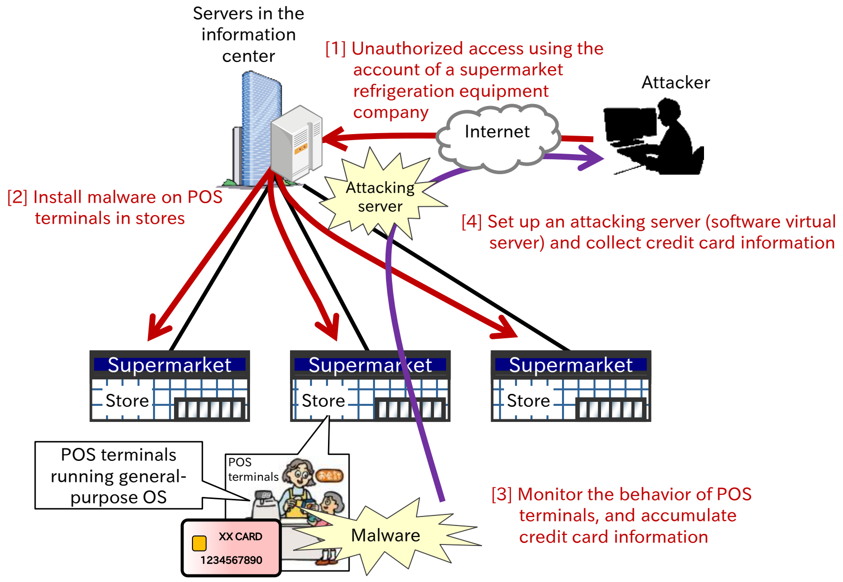
Wireless attacks in particular are easier to conduct because attackers do not need to be near the target of the attack. For devices and systems that affect people's lives in particular, threats that are not normally assumed also need to be identified from the attackers' point of view and dealt with.

⇒ For the identification of threats, see 5.2.1, p.53

Case 3 Leakage of massive customer information due to infection of POS terminals - Malware running on general-purpose OS on devices -

Event

In 2013, it was found that POS terminals of a large retail chain in the U.S. were infected by malware (malicious software), and credit card information of 40 million customers and personal information of 70 million customers were leaked. The method assumed to have been used was as follows: (1) unauthorized access was made to the information center of the retail chain, and (2) malware was distributed from control servers and embedded on POS terminals of each store to collect credit card information, etc. [9]


Servers in the information center
[1] Unauthorized access using the account of a supermarket refrigeration equipment company
Attacker
Internet
Attacking server
[2] Install malware on POS terminals in stores
[4] Set up an attacking server (software virtual server) and collect credit card information
Supermarket
Store
Supermarket
Store
Supermarket
Store
POS terminals running general-purpose OS
POS terminals
XX CARD
1234567890
Malware
[3] Monitor the behavior of POS terminals, and accumulate credit card information

Source: Prepared based on “生活機器の脅威事例集”, Connected Consumer Device Security Council

Figure 2-8 Leakage of personal information from POS terminals

Cause

Intrusion into servers in the information center was said to have been made by fraudulently obtaining IDs and passwords for remote access provided to a supermarket refrigeration equipment company using “fishing mail”. In addition, the latest anti-malware tools were not used on POS terminals in stores, thus enabling attackers to embed malware on them. Malware attacking POS terminals appeared around 2008, and this types of malware rapidly increased in 2014 [10].

Tips for measures

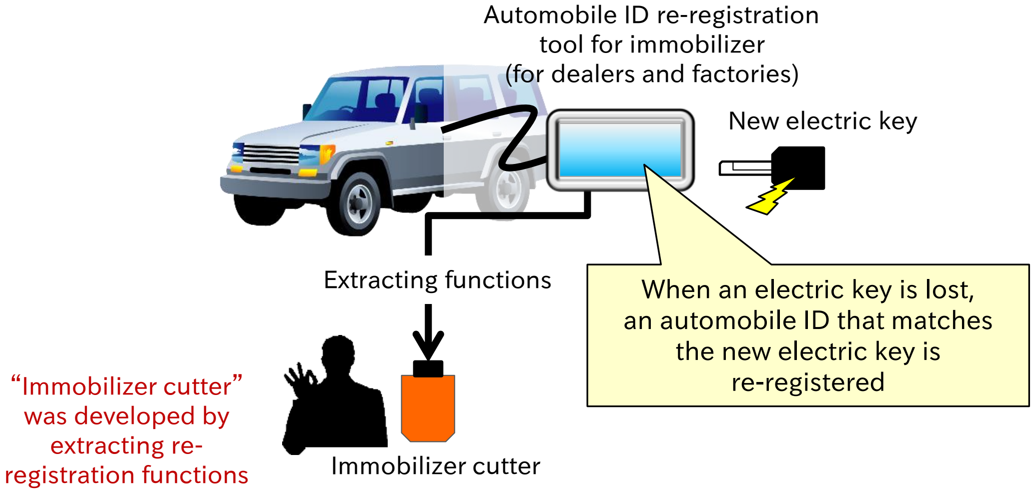
Enhanced access restrictions on servers in the information center and authentication of software to be distributed to POS terminals are needed. In addition, during the period when attacks are quite active in relevant industries, checking the existence of attacks to own systems is important.

⇒ For the collection of threat information, see 5.2.1(5), p.56

Case 4 Automobile thefts by disabling immobilizers - Top-level security privilege was sold on the Internet -

Event

An immobilizer that matches electronic keys with automobile IDs is said to be far more difficult to counterfeit than physical keys. In recent years, however, automobile thefts using a tool to disable immobilizers ("immobilizer cutter") are increasing. An immobilizer cutter is created by extracting the ID re-registration function, which is used when an electronic key is lost, from automobile maintenance tools. It enables unlocking by connecting to the maintenance terminal of automobiles and writing the ID that matches the electronic key in hand [9]. In November 2012, a group of people who had been stealing automobiles using immobilizer cutters were arrested. In Aichi Prefecture, an ordinance to penalize the possession of immobilizer cutters without justifiable reasons was enforced in July 2013.


Automobile ID re-registration tool for immobilizer (for dealers and factories)
New electric key
Extracting functions
When an electric key is lost, an automobile ID that matches the new electric key is re-registered
"Immobilizer cutter" was developed by extracting re-registration functions
Immobilizer cutter

Source: Prepared based on "生活機器の脅威事例集", Connected Consumer Device Security Council

Figure 2-9 Immobilizer cutter used to disable immobilizer

Cause

The cause of this case was the abuse of the re-registration function, a security function of top-level privilege, of automobile maintenance tools used by automobile dealers.

Tips for measures

Measures are necessary not to allow fraudulent use of such privileged operating authorities even if they are sold as a part of a tool. In this particular case, authentication between devices can be effective.

⇒ For security design methods, see 5.2.3, p. 59

2.4 List of other accident and incident cases

(1) Accident cases

Table 2-2 List of accident cases

Period of media coverage	Device involved	Description
2005	Stock ordering system	Transactions of erroneous orders of 42 times the number of stocks issued were closed and could not be canceled due to a software defect.
2006	Self-balancing electric bicycle	Due to a software defect, tires may rotate backwards, placing drivers at the risk of being thrown off.
2008	Duplex system	At the time of a failure of the stand-by system, reset notifications continued being sent, causing the active system to conclude that it was in operation mode and the stand-by system was not able to detect failures of the active system, thereby making the system switch over to fail.
2008	Monorail	Due to high-frequency noise in the power-supply unit, an inverter failed to recognize operations, resulting in abnormal acceleration that caused the train to overrun. Because it was a single-track railway, there was also a possibility of a crash.
2014	Large truck	A defect in the control program of the gearbox disabled the detection of the gear select position, posing a risk of wrong gear change.

(2) Incident cases

Table 2-3 List of incident cases

Period of media coverage	Device involved	Description
2013	Fetal monitor	At a medical center in the U.S., fetal monitoring devices were infected by malware and responses of these devices were delayed.
2014	ATM	An attack method was found that used smartphones to connect to the internal unit of an ATM via USB to cause virus infection, enabling cash withdraw from the ATM simply by cell-phone text-messaging.
2015	Infusion pump	A vulnerability was found in microcomputer controlled pumps that automatically infuse medicinal solutions into patients, which could allow changing the upper and lower limit of medicinal solutions through networks.

Chapter 3
Development processes for safety and security

This chapter explains the necessity of considering safety and security in the development process and presents concrete processes. In addition, the issues concerning the inclusion of safety and security design and examples of how to deal with them are also described. Moreover, an approach to improve efficiency by understanding the difference of safety and security and implementing them in a collaborative manner is presented.

3.1 Safety and security treatment in the development process

(1) Necessity of safety and security treatment

Consider how the accidents and incidents such as those given as examples in Chapter 2 could have been prevented. For the accident cases, the following issues are observed:

- Test scenarios were incomplete, and thus defects were not found.
- Despite being safety-related functions, a defect caused problems in their operations.

For the incident cases, the following issues are observed

- Assumptions about user environment and operations were overly optimistic.
- Assumptions of threats were not sufficient.

These cases could have been prevented by collecting and analyzing the past knowledge and cases, assuming hazards and threats that could cause accidents/incidents, and taking safety and security treatment measures.

In the future "Smart-society", however, hazards and threats that cannot be assumed from past knowledge and cases will also be of concern. For example, failures and attacks can affect other devices and systems through networks and cause currently unpredictable situations. Therefore, incorporating safety and security treatment into the upper stage of the development process, and preparing for future hazards and threats as early as at the requirements specification phase is necessary.

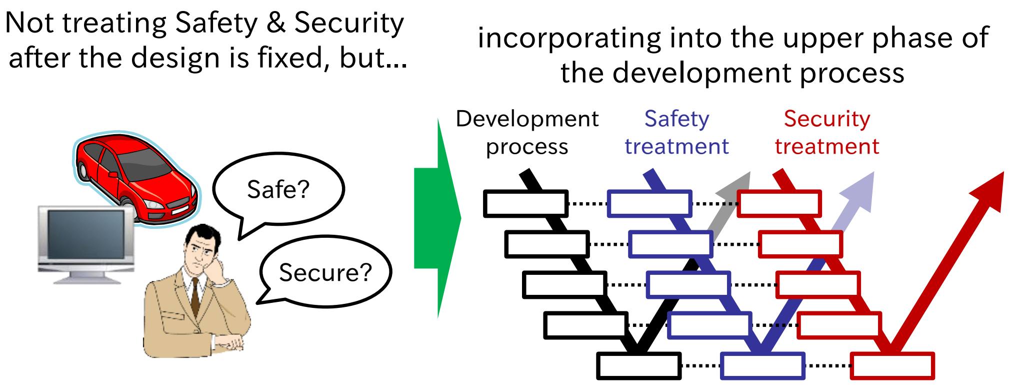

Not treating Safety & Security after the design is fixed, but...
Safe?
Secure?
incorporating into the upper phase of the development process
Development process
Safety treatment
Security treatment

Figure 3-1 Incorporating safety and security treatment into the upper phase of the development process

(2) Involvement of the management in safety and security design

Safety and security treatment is required for the entire life cycle of devices and systems, from planning, design and development to distribution, support and disposition. Furthermore, once accidents or indents occur, they can pose an irreparable impact on business, including compensation for damages, a loss of credibility of the company, etc. Therefore, involvement of not only managers of development departments but also the management and quality control department managers in safety and security treatment is required.

More concretely, the management needs to formulate the basic policies for achieving safety and security for the company and ensure their thorough implementation at the development site. Securing budget and establishing systems for achieving safety and security are also essential. Furthermore, in device and system design, implementing "requirement/analysis" , "design/development" and "test/evaluation" cycles with respect to safety and security at the respective phases of requirement level, system level and hardware/software level of design are necessary. Concerning the matters that can have a significant impact on business operation, reporting to and obtaining approval from the management and quality control department managers using visualized documents are also necessary (see 6.1, p.69 for "visualization").

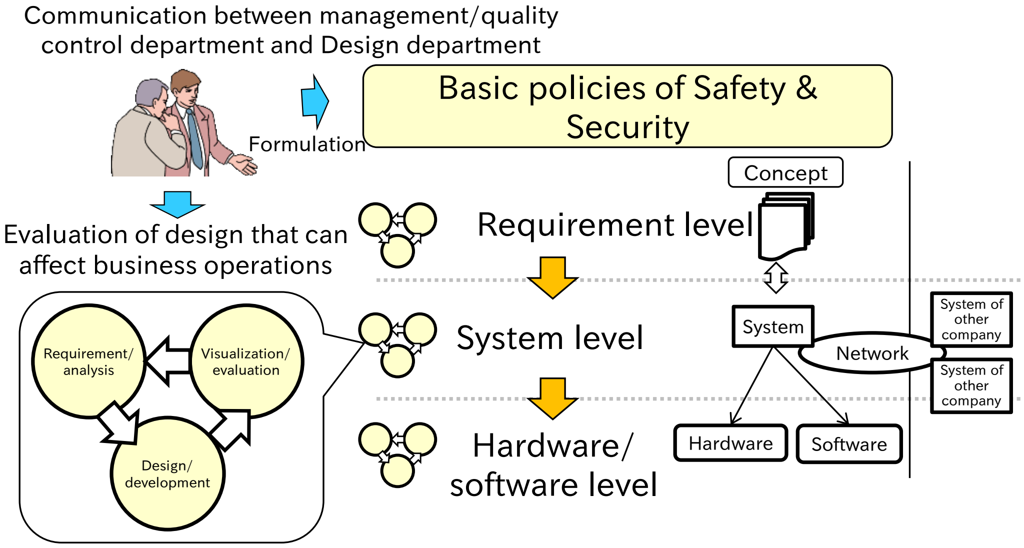

Communication between management/quality control department and Design department
Formulation
Basic policies of Safety & Security
Concept
Evaluation of design that can affect business operations
Requirement level
System level
Hardware/ software level
Requirement/ analysis
Visualization/ evaluation
Design/ development
System
Network
System of other company
System of other company
Hardware
Software

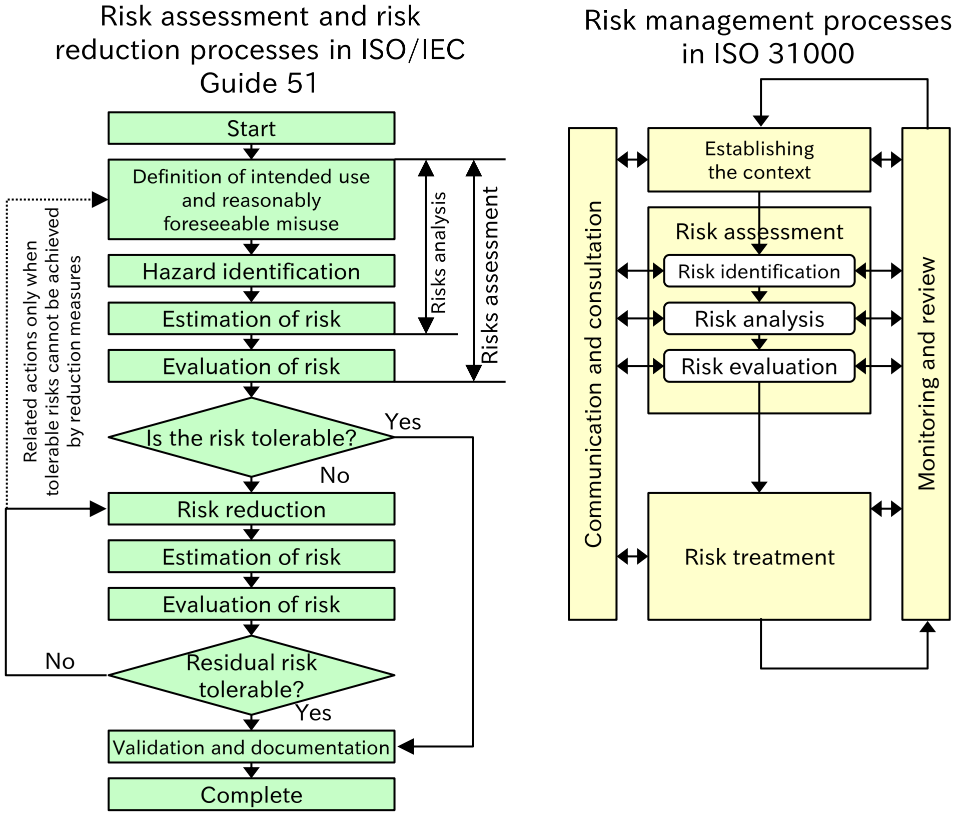
Figure 3-2 Involvement of the management in safety and security design

This enables dissemination of the ideas of Safety/Security at the development site and rapid responses by the management in case any accident or incident occurs.

3.2 Safety and security treatment processes

(1) Entire risk treatment processes

In the international standards ISO/IEC Guide 51, which defines the basic concept of safety, and ISO 31000, which is a risk management international standard and referred to by various security-related standards, risk treatment processes are described as shown in Figure 3-3.



Source: Prepared based on ISO/IEC GUIDE 51:2014 and ISO 31000:2009

Figure 3-3 Risk treatment processes in ISO/IEC Guide 51 and ISO 31000

Although the wording of safety and security risk treatment processes vary, the basic flow of repeating the processes of risk identification, risk analysis, risk evaluation, and risk treatment is the same. As for the identification of the causes of risks, hazards are identified for safety and threats for security.

(2) Risk reduction process

In the above-mentioned ISO/IEC Guide 51, the following “three-step method” is provided as a risk reduction process in the design phase.

Table 3-1 Risk reduction measure “three-step method” in ISO/IEC Guide 51

Three-step method	Outline
Step 1: Inherently safe design	Eliminating or reducing risks to the extent possible (removing, disabling, or isolating hazards)
Step 2: Guarding and protective devices	Adopting necessary protective methods for risks that cannot be eliminated
Step 3: Information for use	Notifying users of the risks that remained after taking the reduction measures in Step 2, clarifying whether special training or body protective equipment, etc., is required or not

Source: Prepared based on “リスクアセスメント・ハンドブック実務編”, Ministry of Economy, Trade and Industry, Japan [11]

Inherently safe design in Step 1 refers to measures to remove components and functions that can themselves be a hazard, to reduce the probability of occurrence by using components with high durability, etc. Step 2 refers to measures that use necessary protective methods, and those that use safety functions in particular are called “functional safety”. Step 3 refers to measures to provide users with risk information. Similarly, for security, risk avoidance by removing information and functions that can be the cause of threats, risk reduction by adding and/or strengthening security functions, etc., shall be promoted.

As described above, since similar processes exist in safety and security risk reduction, implementing them in a collaborative manner is expected to result in efficient implementation.

(3) Importance of making safety and security functions highly reliable

In the risk reduction process described above, when safety and security functions are used for risk treatment in Step 2 after implementing inherently safe design and risk avoidance in Step 1, risks cannot be reduced if these functions themselves fail or malfunction. Therefore, a higher quality design is required for safety and security functions.

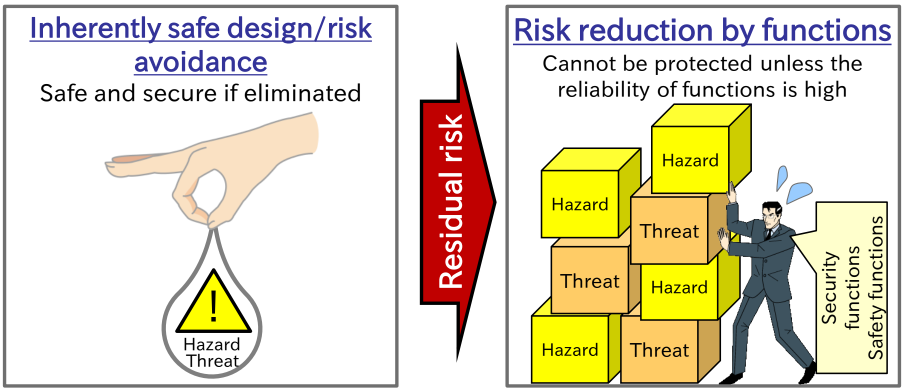

Inherently safe design/risk avoidance
Safe and secure if eliminated
Hazard
Threat
Residual risk
Risk reduction by functions
Cannot be protected unless the reliability of functions is high
Hazard
Hazard
Threat
Threat
Hazard
Hazard
Threat
Security functions
Safety functions

Figure 3-4 Importance of safety and security functions

3.3 Issues in the development process concerning safety and security and how to deal with them

Figure 3-5 illustrates the relationship between processes of the V-Model [12] and that of safety and security design. For embedded systems (computer systems embedded in devices) that compose devices and systems, design to incorporate safety and security functions for risk reduction is carried out in accordance with the processes such as those shown in the figure.

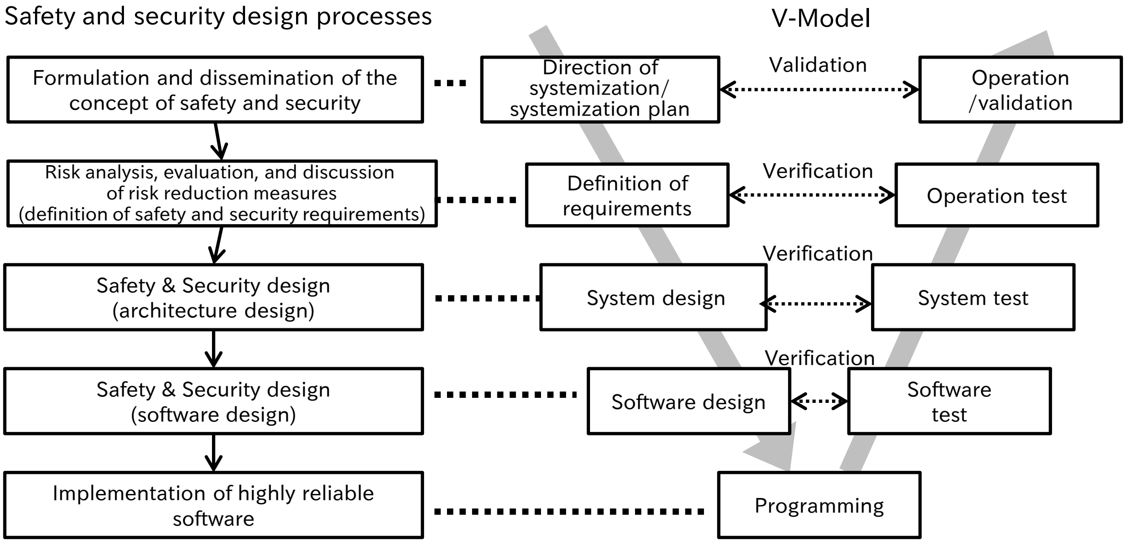

Safety and security design processes
V-Model
Formulation and dissemination of the concept of safety and security
Direction of systemization/ systemization plan
Validation
Operation /validation
Risk analysis, evaluation, and discussion of risk reduction measures (definition of safety and security requirements)
Definition of requirements
Verification
Operation test
Safety & Security design (architecture design)
System design
Verification
System test
Safety & Security design (software design)
Software design
Verification
Software test
Implementation of highly reliable software
Programming

Figure 3-5 Processes of V-Model and safety and security design

In many cases, however, the speed of CPU, memory, and communication of embedded systems of consumer devices is low, and newly adding safety and security functions may cause delay in processing. In addition, making data placement on memory more complex to prevent external attacks against security functions may affect the processing of other functions.

Therefore, implementing safety and security functions on devices and systems requires sufficient system resources, and adjustment between requirements definition and system design (through repeated discussions). For this, using methods such as Twin Peaks model [13] shown in Figure 3-6, to make refinement by repeating the cycle of "requirement definition" → "safety/security analysis" → "architecture design" is considered effective.

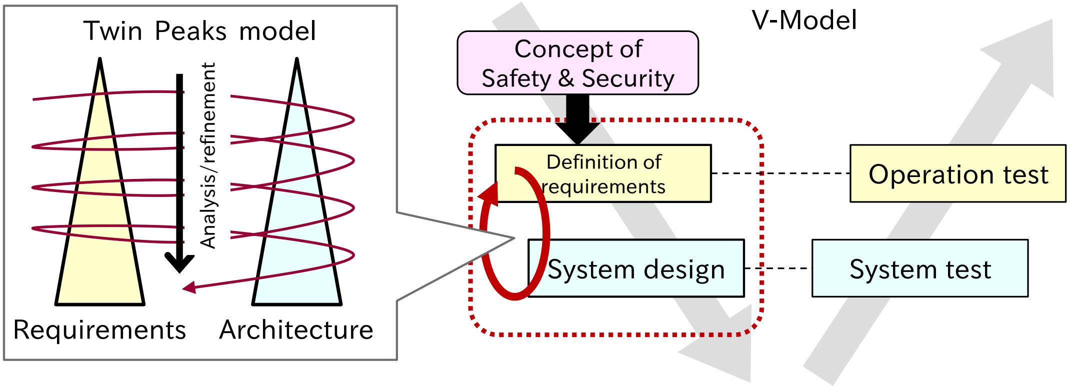


Figure 3-6 Analysis/refinement of requirements and architecture using Twin Peaks model

3.4 Comparing characteristics of safety and security

Because of the similarity of the safety and security treatment processes, an approach of discussing them together for efficiency is described in this chapter. However, the characteristics of safety and security differ in many ways, and the terms used are also different. As for reference, their differences are shown in Table 3-2.

Table 3-2 Difference between safety and security

Difference	Safety	Security
Difference in entities to protect	People's lives, properties (houses, etc.), etc.	Confidentiality, integrity, availability of information, etc.
Difference in causes	Reasonably foreseeable misuse, malfunction of devices	Intended attacks
Difference in damage detection	Easily detected since damage appears as accidents	Most incidents are difficult to detect; for instance, tapping, intrusion, etc.
Frequency of occurrence	Can be addressed as the probability of occurrence	Hard to be addressed in terms of the probability because attacks are made intentionally by humans
Timing of taking measures	Dealt with by risk analysis/treatment at the design phase	Since new attack methods are developed as time passes, continued analysis/treatment is necessary

As described above, significant differences in protected entities, causes, etc., exist between safety and security, and required technologies and knowledge also vary. For this reason, engineers who are responsible for safety treatment and those for security treatment are different in many cases at present. In the Smart-society, however, safety and security affects each other because security threats can propagate through networks and affect safety of devices and systems. Therefore, in order to achieve Safety/Security of devices and systems, engineers of both domains must understand the differences and cooperate in their treatment.

Chapter 4

Safety design for software engineers

Accidents due to device/system failures and improper operations by users can harm people's lives/properties and significantly affect company's businesses. Therefore, hazards need to be eliminated as early as possible. This chapter mainly explains the identification of hazards in the safety treatment process, risk evaluation, and safety design.

4.1 Development process of safety treatment

Safety of a system refers to the degree of expectation that the device/system will not cause any harm or damage. It is defined in ISO/IEC 15026 as follows:

> Safety: The expectation that a system does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered.
> ISO/IEC/IEEE 24765:2010 “Systems and software engineering — Vocabulary”

When accidents actually occur, business loss, including compensation for damages, a loss of credibility of the company, etc., will be significant, and people’ s lives in particular are irreversible. Therefore, appropriate safety treatment is required at the design phase.

In the safety treatment process, potential dangers (hazards) in devices and systems are identified first, and then risks are evaluated from the probability of occurrence and severity of damage. Based on the results, safety design proceeds according to the risks evaluated.

This chapter mainly explains the methods used in each process by following the flow of Figure 4-1.

Safety-related international standards (evaluation/certification systems) are also explained here.

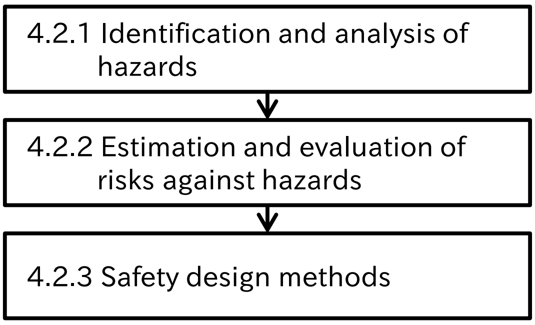

4.2.1 Identification and analysis of hazards
4.2.2 Estimation and evaluation of risks against hazards
4.2.3 Safety design methods

Figure 4-1 Development process of safety treatment

4.2 Safety design

4.2.1 Identification and analysis of hazards

A hazard means a potential factor that leads devices and systems to cause harm or damage by nonoperational means or malfunctioning. When new devices and systems are developed, accident cases regarding such products and other industry's products need to be collected and analyzed to identify hazards. As examples of methods to be used, outlines of FTA, FMEA, HAZOP, and STAMP/STPA are described below (each method is independent, and can be arbitrary selected and applied).

(1) FTA (Fault Tree Analysis)

FTA is a method used for analyzing the causes of events, such as accidents, in a top-down manner to identify hazards, and the notation is provided in IEC 61025:2006. An example is shown in Figure 4-2. An event such as an accident of some sort is set as the target, and "intermediate events" that cause the event ("top event") are expanded into a tree structure. In the following example notation, "AND gates" and "OR gates" are used for branching with the conditions of all occurrence and of any one occurrence, respectively. "Basic events" are events that cannot be expanded any further. In the example of Figure 4-2, the basic event [1] is a hazard to the intermediate event [1]. "Unexpanded events" are events that can be expanded but their expansion is omitted.

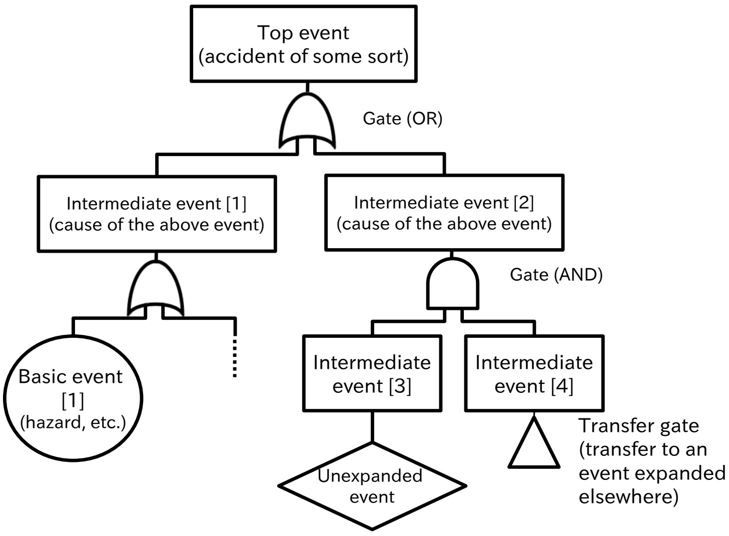


Figure 4-2 Example of FTA notation

FTA is a simple and easy-to-understand method, but for cases where many devices and systems work with each other, the tree structure can become very large and difficult to deal with.

(2) FMEA (Failure Mode and Effects Analysis)

FMEA is a method for extracting factors of device/system failures. This method is used to find devices and components having significant effects by analyzing what effects a failure has on the system when it occurs in devices or components comprising the system. More concretely, a worksheet is created by setting appropriate evaluation items that match target devices and systems and evaluation methods of the frequency of occurrence and severity of failure modes using the standard worksheet of the second edition of the international standard on FMEA (IEC 60812) as a reference.

Table 4-1 Example of FMEA for air conditioner design

Components, features	Failure mode	Cause	Effect	Severity	Treatment by design	Verification, Effectiveness
Hot water valve	Valve not closed	Valve abrasion	Unable to stop heating	A	Valve leakage reduction structure	Verification of accelerated durability
	Electrode damage	Insulation failure	Fire	A	Maintenance Introduction of protective cover	No problem occurrence in case of damage
Drain pump	Not rotating	Overheat (bearing)	Unable to discharge water	A	Improved motor cooling	Verification (for at least 20 years)
		Overheat (winding)	Unable to operate	A	Adoption of ball bearing, protection circuit	

Source: Prepared based on “消費生活用製品向けリスクアセスメントのハンドブック”, Ministry of Economy, Trade and Industry, Japan [14]

“Failure modes” (status and phenomenon of device or component failures) of devices and systems are then extracted and analyzed using the worksheet.

In contrast to FTA, which analyzes hazards that can be a factor of events such as accidents from the causes in a top-down manner, FMEA assumes effects such as accidents from the failure modes in a bottom-up manner. FMEA therefore has an advantage that failures can be assumed and prevented before the occurrence of accidents. There are issues, however, that assuming the failure modes and the causes in consideration of human errors such as misuse and environmental conditions before accidents actually occur is difficult. FMEA is also not suitable for discussing multiple failures.

(3) HAZOP (Hazard and Operability)

HAZOP (IEC 61882:2001) focuses on “deviations (abnormalities)” between the processes assumed in design and the actual processes to eliminate the “deviations” or to prevent proceeding to dangerous states or accidents due to the “deviations”. “Guide words” such as those in Table 4-2 are used in HAZOP. They are combined with appropriate parameters (variables) according to systems and devices to clarify the “deviations” as shown in Table 4-3.

Table 4-2 Basic guide words of HAZOP

HAZOP guide words	Meaning
No or not	Complete negation of design intent
More	Quantitative increase
Less	Quantitative decrease
As well as	Qualitative modification/increase
Part of	Qualitative modification/decrease
Reverse	Logical opposite of the design intent
Other than	Complete substitution

Source: Prepared based on IEC 61882

In contrast to FTA, which uses accidents as a starting point, HAZOP has an advantage that unforeseen events can be identified by using “deviations” between the design and actual conditions as a starting point. However, events that do not lead to accidents are also included, thus increasing the number of items to be examined. Arrangements are therefore necessary.

Table 4-3 Example of arrangement of “deviations (abnormalities)” in HAZOP

No.	Parameter	Guide word	Content of deviation	Cause of deviation	Effect on system	Safety measure
1	Rotation speed	Less	Rotation speed: Low	・ Foreign matter jammed in rotating mechanism	・ Heat generation in electronic devices due to overcurrent ・ Excessive vibration of devices	・ Electric current limiter ・ Power shutdown by variation sensors
2	Temperature	More	Temperature of cooling water: High	・ Incorrect closure of valves for controlling the flow rate to heat exchanger due to a software error	・ Improper operation of electronic control system due to a rise in temperature ・ Degradation of devices	・ Temperature monitor ・ Flow rate monitor

Source: Prepared based on “川原卓也：潜在危険分析とリスク分析、(株)日本機能安全、機能安全エキスパート・セミナー”

(4) STAMP/STPA

STAMP (Systems-Theoretic Accident Model and Processes) is an accident model based on system theory, and STPA (System-Theoretic Process Analysis) is a hazard analysis method based on STAMP. FTA and HAZOP mainly cover hazard analysis of individual devices. In the Smart-society, however, systems work together in a complex manner, and therefore STAMP and STPA focus on the control structure between systems and analyze "interactions between components". Outlines of the procedures are described below.

Step 0. Preparation

Accidents and hazards to be avoided are assumed, and then the control structure of the system is expressed in a diagram.

Step 1. Analysis of hazard scenarios by identifying unsafe controls

Based on the following four guide words, hazards of concern for causing accidents in controls between devices are identified.

1. "Not Provided"

   Control actions for safety are not established.

2. "Incorrectly Provided"

   Unsafe control actions that can still lead to hazards are established.

3. "Provided Too Early, Too Late, or Out of Sequence"

   Control actions for Safety are established, but the timing is too late, too early, or not in the predefined order.

4. "Stopped Too Soon"

   Control actions for Safety are established, but are stopped too soon or applied too long.

Step 2. Analysis of potential contributing factors by creating control loops

A control loop diagram consisting of controlling entities and controlled processes for each hazard is created to identify inappropriate controls and possible inconsistencies that can be the causes. Controlling entities take control of controlled processes. As a result of the control, controlled processes may return feedback such as responses to the controlling entities. Controlling entities hold the status of controlled processes as "models" and determine whether a control is needed or not.

Step 3. Measures against potential contributing factors

Whether safety restrictions (safety measures and safety control) are established or not for the identified inappropriate controls and inconsistencies is verified to prevent them from occurring.

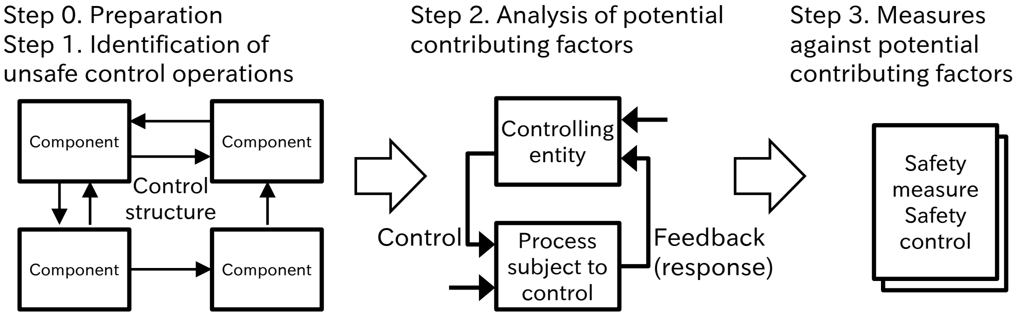

Step 0. Preparation
Step 1. Identification of unsafe control operations
Component
Component
Control structure
Component
Component
Step 2. Analysis of potential contributing factors
Controlling entity
Control
Process subject to control
Feedback (response)
Step 3. Measures against potential contributing factors
Safety measure
Safety control

Figure 4-3 Image of STAMP/STPA

STAMP and STPA are used in hazard analysis in a number of sectors, including space, aeronautics, automotive, and energy sectors [15] [16] [17].

(5) Example of hazards

For the purpose of showing what hazards are identified by the methods described in this section, examples of concrete hazards in automotive and smart home electrical appliances sectors are listed here.

Table 4-4 Example of hazards in automotive sector

No.	Type of hazard	Example of hazard
1	Actuator failure	Brake failure, steering gear failure, etc.
2	Sensor failure	Abnormal wheel speed value, abnormal door open/close value, etc.
3	Malfunctioning	Malfunctioning due to electromagnetic wave, voltage fluctuation, etc.
4	Pinching	Automatic door, automatic window, etc.
5	Entanglement in rotating parts	Wheels, fans, belts, etc.
6	Silent approach	The movement is hardly noticeable, etc.
7	Fire caused by fuel	Gasoline, gas, large capacity battery, etc.
8	Electric shock	During EV battery charge, exposure of rechargeable battery due to accidents, etc.
9	Explosion of chemical substance	Unexpected explosion of air-bag
10	Crash into people/objects	People/objects in blind spot, skidding, lane change, crossing collision, etc.
11	Wrong operation	Unintended acceleration into walls, simultaneous application of brake and accelerator, etc.
12	Reduced attention	Drowsiness, inattentive driving, etc.
13	Loss of consciousness	Being in critical condition or unable to call for help due to lesion or accident, etc.

Table 4-5 Example of hazards in smart home electrical appliances sector

No.	Type of hazard	Example of hazard
1	Entanglement, pinching	Washing machine drum, automatic door, etc.
2	Heat generation for an extended period of time	Low temperature burns due to rechargeable battery, electric carpet, etc.
3	High temperature/overheat	Overflow of hot water from a pot, device overheating, etc.
4	Component failure	Fire caused by motor/power conditioner/rechargeable battery, malfunctioning elevator, etc.
5	Electric shock	Wet hands, short circuit, grounding fault, etc.
6	Overcurrent	Battery overcharge, wire/plug burning, etc.
7	Battery exhaustion	Portable medical device stoppage, drone crash, etc.
8	Interference of radio waves	Malfunctioning/interruption of a remote controller for air conditioners, drones, etc.
9	Submersion	Electronic device breakage, human death, etc.
10	Dust	Short electric circuit, overheating, etc.
11	Accidental ingestion	Infant and button-shaped battery, tiny device, etc.
12	Falling	Falling of an electrical product due to tumbling over, vibration, etc.
13	Power restoration	Fire caused by electric power recovery after earthquake, etc.

4.2.2 Estimation and evaluation of risks against hazards

Once hazards are identified, the risks are estimated by analyzing situations where the hazards lead to damage and clarifying the probability of occurrence and severity of damage. For instance, the probability of occurrence varies between failures that occur as a result of degradation of components and failures that invariably occur with certain combinations of user operations and environmental conditions. In addition, the severity of damage varies between failures that disable operations and malfunctioning that affect people’s lives. The risks are therefore estimated by combining the probability of occurrence and severity of damage. The estimated risks are then evaluated to determine whether they are at a tolerable level or not.

Table 4-6 shows examples of the methods used. The methods marked with “*” are those presented in 4.2.1 as the methods for identifying and analyzing hazards, but they can also be used for estimating risks at the same time.

Table 4-6 Example of risk estimation and evaluation methods

Method	Outline of method
Risk matrix	The degree of risk is classified by the frequency of occurrence and severity of harm in a 2-axis table format (see 4.2.2(1), p.42)
Risk graph	The risk level is classified by determining the existence of multiple factors such as the frequency, severity, ease of prevention, etc., in order (see 4.2.2(2), p.43)
FTA*	The causes of occurrence are clarified in a systematic manner by using undesirable events such as accidents as the starting point (see 4.2.1(1), p.36)
FMEA*	Effects on systems are discussed in a systematic manner by using component failures as a starting point (see 4.2.1(2), p.37)
HAZOP*	Hazards to systems are assumed by combining the guide words and parameters (variables) and supposing “deviations” from the design assumptions in a systematic manner (see 4.2.1(3), p.38)
STAMP/STPA*	Interaction hazards in complex systems are identified by applying the guide words to each inter-system control (see 4.2.1(4), p.39)

(Note) Methods marked with “*” are those also used for hazard identification (see 4.2.1, p.36)

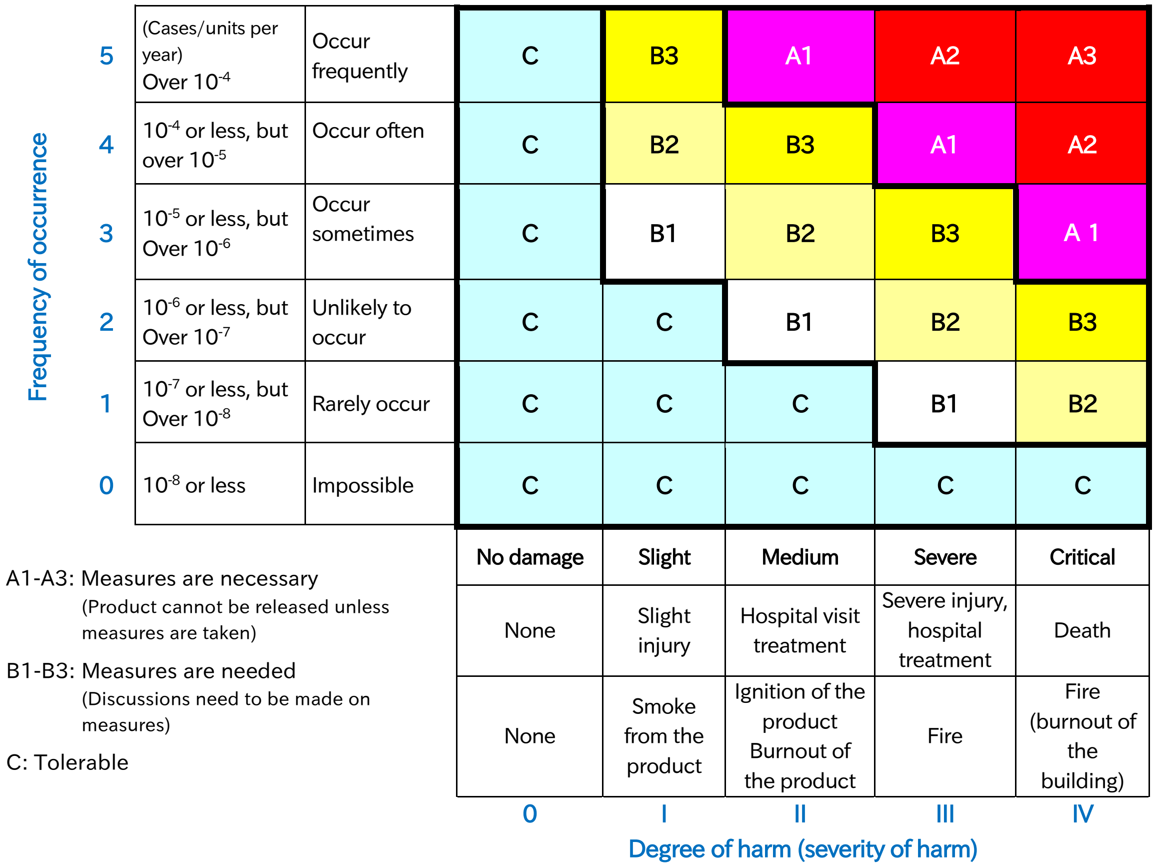
Source: Prepared based on “米国における STAMP（システム理論に基づく事故モデル）研究に関する取り組みの現状” [15], “機能安全規格の技術解説”, JEMIMA [18]

The outlines of risk matrix and risk graph are described below as examples.

(1) Risk matrix

A matrix using the frequency of occurrence and severity of harm as vertical and horizontal axes, respectively is created, and the class numbers indicating the significance of risks are entered in the corresponding cells. Vertical and horizontal axes of risk matrix are classified according to the characteristics of products or selected from those publicly available. As for the procedures, the frequency of occurrence and degree of harm are estimated for defined hazards. The classes are then determined using a risk matrix.

Figure 4-4 shows a type of risk matrix called R-Map adopted by the Product Safety Technology Center, National Institute of Technology and Evaluation (NITE), Japan [19]. For the hazards mapped to classes A1 to A3 (intolerable level), measures are taken to reduce the frequency of occurrence and degree of harm to a tolerable level.



Frequency of occurrence

5	(Cases/units per year) Over 10^{-4}	Occur frequently	C	B3	A1	A2	A3
4	10^{-4} or less, but over 10^{-5}	Occur often	C	B2	B3	A1	A2
3	10^{-5} or less, but Over 10^{-6}	Occur sometimes	C	B1	B2	B3	A 1
2	10^{-6} or less, but Over 10^{-7}	Unlikely to occur	C	C	B1	B2	B3
1	10^{-7} or less, but Over 10^{-8}	Rarely occur	C	C	C	B1	B2
0	10^{-8} or less	Impossible	C	C	C	C	C
			No damage	Slight	Medium	Severe	Critical
			None	Slight injury	Hospital visit treatment	Severe injury, hospital treatment	Death
			None	Smoke from the product	Ignition of the product Burnout of the product	Fire	Fire (burnout of the building)
			0	I	II	III	IV

Degree of harm (severity of harm)

A1-A3: Measures are necessary
(Product cannot be released unless measures are taken)

B1-B3: Measures are needed
(Discussions need to be made on measures)

C: Tolerable

Source: Prepared based on “製品安全,リスクアセスメントのための R-Map 入門(第 1 版)”, Union of Japanese Scientists and Engineers [19]

Figure 4-4 Example of R-Map

NITE made public the results of estimation and evaluation of accident cases of consumer products using R-Map on their website [20].

(2) Risk graph

An International standard “ISO 13849-1:2006” (Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design) defines the “PL (Performance Level)” based on the probability of occurrence of a dangerous failure per hour. The components implementing safety functions of machines are called “Safety-related components of the control systems”. In recent years, many semiconductor components are used in devices comprising safety-related components, and the form of their control has shifted from hard-wired control to software control. The classification level used to define the ability of safety-related components of the control systems to execute safety functions under foreseeable conditions are called PL. The PL of the safety-related control systems is required to be equal or higher than the “Performance Level required (PLr)”. Figure 4-5 shows the risk graph used to determine the PLr.

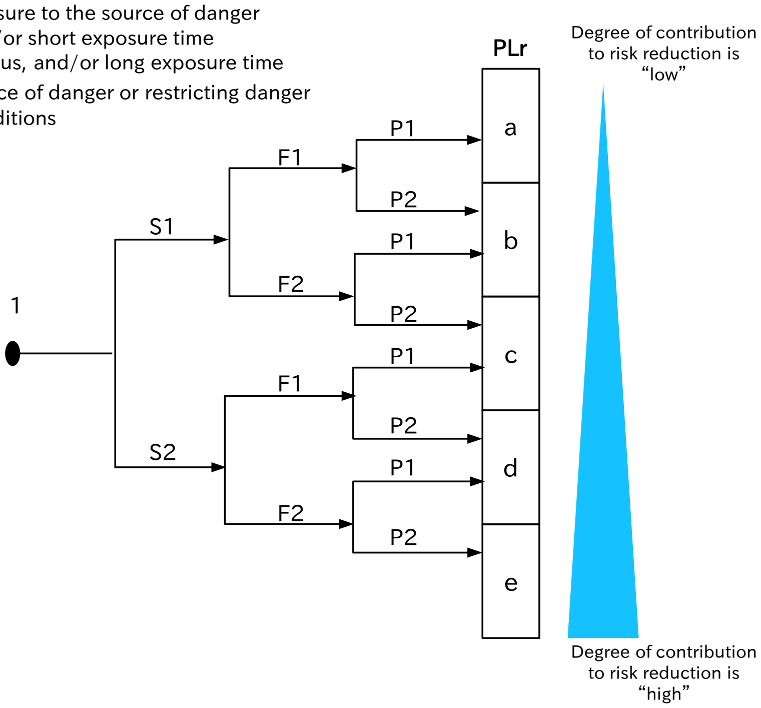
Description of symbols

1: Starting point for evaluating the degree of contribution of safety functions on risk reduction

S: Severity of injury
S1: Slight injury (normally recoverable injury)
S2: Severe injury (normally not recoverable or death)

F: Frequency and/or time of exposure to the source of danger
F1: Rare to low frequency, and/or short exposure time
F2: High-frequency to continuous, and/or long exposure time

P: Probability of avoiding the source of danger or restricting danger
P1: Possible under certain conditions
P2: Almost impossible


PLr
Degree of contribution to risk reduction is "low"
1
S1
S2
F1
F2
F1
F2
P1
P2
P1
P2
P1
P2
P1
P2
a
b
c
d
e
Degree of contribution to risk reduction is "high"

Source: Prepared based on ISO 13849-1:2006

Figure 4-5 Risk graph

With a risk graph, risk evaluation is conducted by making decisions on three risk factors (risk parameters [S], [F], and [P]) between two options. Three risk factors are "severity of injury (S)", "frequency and/or duration of exposure to hazard (F)", and "probability of avoiding or limiting harm (P)".

The PL is the ability of safety-related components of the control systems to avoid hazards, and is ranked from "a" to "e" according to the probability of occurrence of a dangerous failure (probability of occurrence of a failure that makes the system unsafe) per hour.

Table 4-7 Performance level

Performance level (PL)	Average probability of occurrence of a dangerous failure per hour
a	10^{-5} or higher, but lower than 10^{-4} (0.001%-0.01%)
b	3 x 10^{-6} or higher, but lower than 10^{-5} (0.0003%-0.001%)
c	10^{-6} or higher, but lower than 3 x 10^{-6} (0.0001%-0.0003%)
d	10^{-7} or higher, but lower than 10^{-6} (0.00001%-0.0001%)
e	10^{-8} or higher, but lower than 10^{-7} (0.000001%-0.00001%)

Source: Prepared based on ISO 13849-1:2006

The probability of occurrence of a dangerous failure is determined by the factors such as "category (structure of safety-related component)", "mean time of a dangerous failure", "diagnostic coverage", and “common cause failure” (see “ISO 13849-1:2006” for the determination method. If the PL is at an intolerable level, measures such as adding/enhancing safety functions are taken, and then the PL is derived again. See Table 6-1 of Chapter 6, p.72 for the scales of safety and security, including the PL.

4.2.3 Safety design methods

(1) Approaches to safety measures

If the identified risks are at an intolerable level, risk elimination and reduction are undertaken by inherently safe design as described in 3.2. If intolerable risks still remain, they are dealt with by safeguard measures and protective devices (such as safety functions, etc.). Table 4-8 shows examples of approaches to risk reduction.

Table 4-8 Examples of approaches to risk reduction

Idea	Description	Example of inherent safety	Example of functional safety
Foolproof	Mechanisms for avoiding accidents even in cases where knowledge and experience are lacking	・ Digital cameras into which batteries can only be inserted in the right direction	・ Functions to detect the rotation of the washing machine drum and disable the door from opening until it stops
Affordance	Mechanisms that make users naturally choose the use methods assumed	・ Using shapes (achieved by structure) ・ Using colors (achieved by structure) ・ Using locations (achieved by structure)	・ Using shapes (achieved by function) ・ Using colors (achieved by structure) ・ Using locations (achieved by structure)
Fail safe	Mechanisms for minimizing damage due to environmental conditions and component failures	・ Automobile door locks that can be mechanically unlocked even if batteries run out	・ Functions to detect earthquake shaking and stop the heater
Fault Tolerance	Mechanisms for preventing operations from stopping even if a problem occurs in one of the system components	・ Tires that enable automobiles to run safely for a short distance even if they blow out	・ Functions to autonomously maintain operations in case of communication failure of network control devices
Multi-layered protection	Availability of another mechanism if protection cannot be achieved by one mechanism	・ Reducing risks by combining inherent safety	・ Reducing risks by another safety function even if some safety functions fail

Source: Prepared based on “組込みシステムの安全性向上の勧め”, IPA [1]

(2) Effective design methods for safety

Many safety functions are implemented by computer systems that are embedded in devices to enable flexible operations based on the information from sensors and external networks. However, safety functions themselves may stop operating due to software defects or hardware failures. The methods for improving design quality are therefore used for embedded systems implementing safety functions.

The scale of software in embedded systems is growing each year, and the lines of source code are said to be around several millions to ten million [21]. Table 4-9 shows the examples of methods that can be used to make the design/verification of such large-scale embedded software easier and improve design quality.

Table 4-9 Examples of methods to improve design quality

Design method	Description	Effectiveness
Model-based development (MBD)	A method for discussing specifications and making design by simulating the behaviors of devices and systems using "models" in which operations such as controls are expressed as mathematical expressions	Design can be carried out while verifying the behaviors, and the development cycle can also be made faster
Model-based systems engineering (MBSE)	A technique for optimizing the entire system development with the aim of "leading the development of the systems for products and services, etc. to success", and processes for achieving it are defined	Large-scale, complex systems can also be easily expressed as a set of models
Formal methods	A method that expresses design targets using specification description language based on mathematical logic to enable the elimination of ambiguities and support for design verification using tools	Logical rigidity is increased by the elimination of ambiguities

For "model-based design" and "formal methods", tools for automatically generating codes from the design information are available. They are expected to contribute to the improvement of development quality and costs.

Table 4-10 shows examples of mechanisms to improve safety of devices and systems.

Table 4-10 Examples of mechanisms to improve safety of devices and systems

Mechanism	Contents
Domain segmentation	Limit the extent of the impact of damage by dividing microcomputer (core), virtual machine, memory area, and network, etc., into segments based on function and degree of safety. Examples include inhibit design [22] to minimize the extent of the impact of failures and software defects, etc.
Self-diagnosis	Regularly monitor for abnormalities in products/systems, and recover or stop them accordingly. Examples include "watchdog", FDIR (Fault Detection, Isolation and Recovery) [23], etc.
Human centered design (ISO 9241-210)	Build easy-to-use interfaces with few operation errors by applying the knowledge and skills of human engineering and usability.
Duplication (multiplication)	Duplicate (or multiplex) software/hardware to enable them to switch operations in case of abnormalities (duplex method), or to concurrently operate to detect abnormalities by comparing their behaviors, etc. (dual method).

In embedded systems, the above-mentioned methods and mechanisms can be flexibly used in combination to utilize their individual characteristics.

(3) Risk reduction by providing information for use

After designing inherent safety and functional safety against risks, reduction of residual risks by providing information to users is discussed. Table 4-11 shows items listed in the risk reduction procedures in ISO/IEC Guide51:2014.

Table 4-11 Risk reduction measures taken in design (excerpt from ISO/IEC Guide 51:2014)

Information for use
- on the product or its packaging - warning signs, signals - warning devices - in the instructions for use, including information or training (where necessary)

The effectiveness of risk reduction by the above-mentioned warning functions and provision of information in manuals is evaluated/verified to clarify final residual risks at the time of design. Warning signs/labels, warning signals, and warning devices are also included in safety functions, and therefore, high-quality design is required.

4.3 Evaluation/certification of safety design

IEC 61508, an international standard established in 1998, divides life cycles with regard to “functional safety of electrical/electronic/programmable electronic safety-related systems” into 16 phases, from conceptual phase that includes design/development to maintenance/disposition phases, and defines the requirements for each phase. This standard provides, in addition to the requirements for hardware/software, the concepts of risk and safety degree, and methods for determining “the safety integrity level (SIL)”. To date, functional safety-related standards are established in the respective sectors as shown in Table 4-12.

Table 4-12 Status of establishment of major functional safety-related standards

Year of establishment	Sector	Standard No.
1998	All	IEC 61508-1,3,4,5
2000	All	IEC 61508-2,6,7
2001	Nuclear power plants	IEC 61513
2002	Railway applications (RAMS: reliability, availability, maintainability and safety)	IEC 62278
	Railway applications	IEC 62279
2003	Process industry sector	IEC 61511-1
2004	Process industry sector	IEC 61511-2,3
	Household electrical appliances (Software evaluation)	IEC 60335-1 (Annex R)
2005	Machinery	IEC 62061
2006	Medical device software	IEC 62304
2007	Adjustable speed electrical power drive systems	IEC 61800-5-2
2011	Road vehicles	ISO 26262
2014	Robots and robotic devices	ISO 13482

Functional safety certifications by certification bodies include “product certification”, which certifies the compliance of devices or systems with the above standards, and “process certification”, which certifies the compliance of the development processes of companies, etc., with functional safety standards. The product certifications obtained can be used as evidence to explain to customers that the devices and systems meet a certain safety integrity level. In addition, by obtaining process certifications, evaluation of the software development process can partially be omitted when obtaining product certifications for new devices and systems.

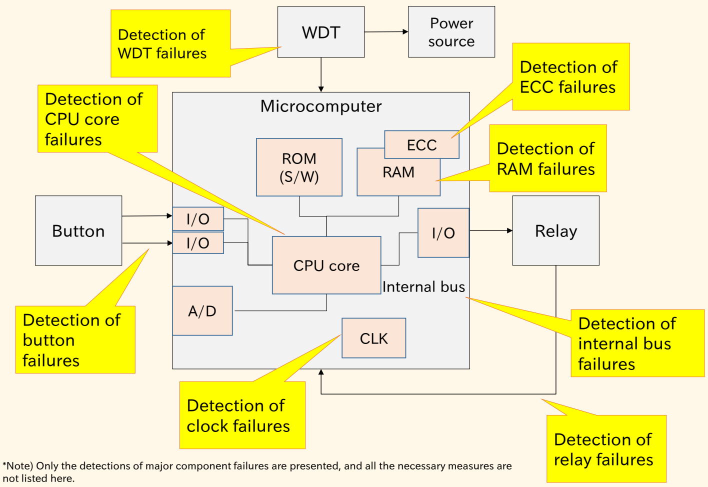
Column 3 When can functional safety design be considered completed!?

Akihisa Morikawa
WITZ Co., Ltd.

Functional safety standards such as IEC 61508 and ISO 26262 require design that can prevent "dangers due to failures" of various components, but explaining "to what extent they should be dealt with to be considered sufficiently safe" is very difficult.

Failures can be divided into permanent failures and temporary failures, and handling "temporary failures" is more difficult in general. For RAM (Random-access memory), for example, a case where a bit of some variable is garbled due to noise or cosmic radiation needs to be considered. If such a momentary failure can cause significant danger, it must always be monitored. RAM with ECC (Error-correcting code) is widely adopted as a simple measure for this. However, it is not sufficient because failures of an internal bus that connects RAM and a microcomputer cannot be detected. In contrast, a method of duplicating variables and comparing them by software can be used to detect internal bus failures.

Would "ECC" + "the measure for internal bus failures" be sufficient then? Actually, it is not. That is because ECC is not guaranteed to always function correctly. As an example of handling such situation, from the author's past experience, ECC equipped with a "failure detection circuit for ECC itself" can be used for monitoring at all times.


Detection of WDT failures
WDT
Power source
Detection of ECC failures
Detection of CPU core failures
Microcomputer
ECC
ROM (S/W)
RAM
Detection of RAM failures
Button
I/O
I/O
I/O
Relay
CPU core
Internal bus
A/D
CLK
Detection of button failures
Detection of internal bus failures
Detection of clock failures
Detection of relay failures

*Note) Only the detections of major component failures are presented, and all the necessary measures are not listed here.

What about, then, the monitoring of the failure detection circuit for ECC itself? These questions can continue endlessly... How far these questions should be considered depends on the safety integrity level (SIL, ASIL, PL, etc.; see 6.1(5), p.71) specified by the standards. Railway standards require as far as triple failures to be considered in some cases.

In software design, by contrast, implementation of "check mechanisms for detecting bugs" is required. Such mechanisms include data range checking, execution order monitoring, and a method of implementing software with two types of algorithms and comparing their results, etc.

Finally, this column focuses on functional safety design, but it cannot alone guarantee the "reliability of the components for ensuring safety". We must not forget that safety can only be achieved by high quality management for development.

Chapter 5

Security design for software engineers

The security treatment costs in the operation phase are said to be 100 times higher than that in the design phase, and therefore, security treatment needs be taken at the earliest stage possible. This chapter mainly describes the identification of threats, risk evaluation, and security design, which precede the security treatment process.

5.1 Development process of security treatment

Threats against devices and systems assumed include information leakage, invasion of privacy by tapping, unauthorized access, malfunctioning or unexpected termination due to data and software falsification, etc. Depending on the threats, functions for achieving safety can also be affected. This raises concerns of significant damage, including the occurrence of accidents, loss of customers' trust, costs for device replacement/system repair, etc. Steady security treatment is therefore required.

In the security treatment process, things to be protected and goals are set first. Examples include: not to allow leakage of important information; not to allow software falsification; and not to allow the system to stop. Threats against them are then identified, and risks are evaluated from the probability of occurrence and severity of damage. Based on the results, security design is proceeded according to the scale of risks. This chapter mainly explains the methods used in the processes, from the identification of threats to security design, by following the flow of Figure 5-1. Security related international standards (evaluation/certification systems) are also explained here.

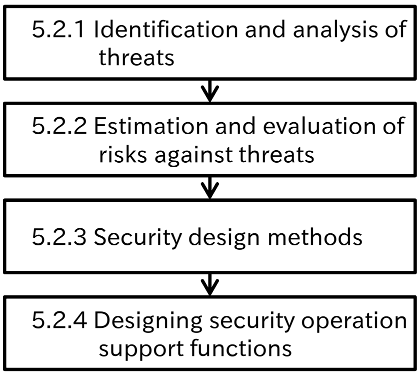

5.2.1 Identification and analysis of threats
5.2.2 Estimation and evaluation of risks against threats
5.2.3 Security design methods
5.2.4 Designing security operation support functions

Figure 5-1 Development process of security treatment

As shown in Figure 5-2, if vulnerabilities are found in the market operation phase, device replacement, system repair, etc., will become necessary. This requires significant costs and efforts when compared to the design/development/test phases. Security treatment therefore needs to be taken at the earliest stage possible [24].

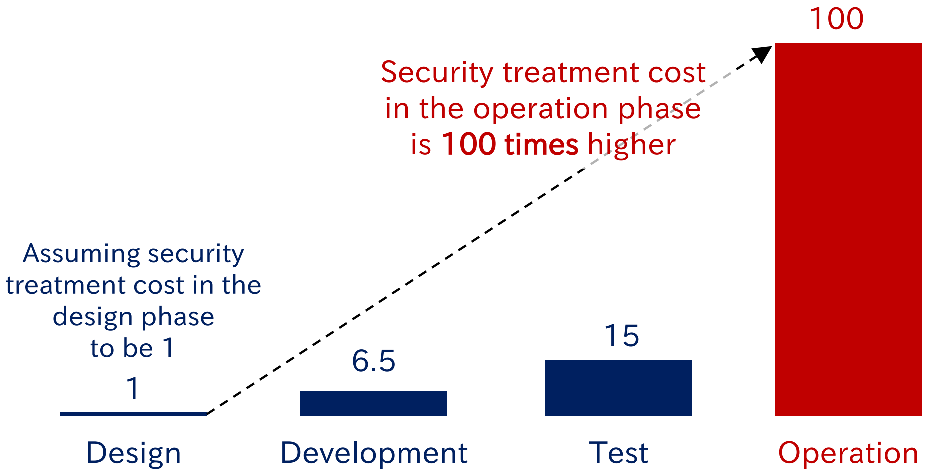


Figure 5-2 Security treatment costs by development process

Security design-related standards include IEC 62443 for the sectors of large-scale control systems such as factories and plants, and general-purpose Common Criteria (CC; ISO/IEC 15408). Evaluation and certification schemes are also implemented, but they are still in the discussion phase in the sectors covered by this document, including automotive and home electrical appliances sectors. This document therefore presents security design methods, including the use of safety design methods that are standardized in a wide range of sectors.

5.2 Security design

5.2.1 Identification and analysis of threats

“Threats” to security are equivalent to “hazards” to safety, and refer to potential factors that lead to an “intolerable state” such as an accident or incident. Examples of threats include unprivileged users using devices and systems by stealing other users’ passwords, attacks that terminate services by exploiting system vulnerabilities, etc.

The attackers attack devices and systems in a manner unexpected by the designers and users of devices and systems. This makes the identification of threats difficult. Identifying threats requires clarification of software and system structures, entry points for attacks (networks, users, other devices and systems, etc.), and information and services to be protected (referred to as “properties”). Based on the above, what threats will occur and what events will be caused are assumed and listed.

Effective methods for identifying and analyzing threats are presented below. (1) and (2) assume direct threats against devices and systems, and then identify the severity of damage caused by them. (3) assumes threats that cause serious damage, and then breaks down the means of attacks. For important devices and systems, the completeness of identifying threats can be improved by not just adopting only one method but also combining multiple methods.

(4) identifies threats from the point of view of attackers, and selects methods based on the characteristics of devices and /systems and environment for use. (5) is for collecting information of threats, and is commonly required.

(1) STRIDE threat model

Threats exist in a wide variety and new attack methods are being developed every day. Exhaustively covering them is therefore difficult. STRIDE threat model described here covers major threats. The name “STRIDE” is taken from the initials of major threats, and it provides a clue for identifying threats by verifying whether these major threats exist against devices and systems concerned or not.

Table 5-1 STRIDE threat model

Item	Outline
Spoofing	Pretending to be other users to deceive computers
Tampering with data	Falsifying data without privileges to harm data integrity
Repudiation	Users denying performing an action while other parties having no way to prove otherwise
Information disclosure	Disclosing information to individuals who are not supposed to have access to it
Denial of Service	Denying valid users from accessing servers and services
Elevation of privilege	Unprivileged users gaining privileged access

Source: Prepared based on “セキュリティ上の脅威の評価” [25] and “Security Planning Through Threat Analysis” [26], Microsoft

(2) Common Attack Pattern Enumeration and Classification

In “CAPEC (Common Attack Pattern Enumeration and Classification)” [27], not only attacks against devices and systems but also the attack mechanisms that include tactics used to lead human operations into error and get out information are provided in a hierarchical way. The identification of threats can be made easier by discussing them through applying in sequence from the top category the mechanisms of attack and the domains of attack shown in Table 5-2.

Table 5-2 Top category of Common Attack Pattern Enumeration and Classification (CAPEC)

Mechanisms of attack	Targets for attack
Gather information, deplete resources, injection, deceptive interactions, manipulate timing and state, abuse of functionality, probabilistic techniques, exploitation of authentication, exploitation of authorization, manipulate data structures, manipulate resources, analyze target, gain physical access, execute illegal code, alter system components, manipulate system users	Social engineering (person) Supply Chain Communications Software Physical security Hardware

Source: Prepared based on CAPEC website [27]

(3) Threat analysis using attack tree

“Attack tree analysis” is used to analyze threats by setting the objectives of attackers and expanding the procedures of attacks for achieving the goals in a tree structure. Figure 5-3 shows the image of an attack tree.

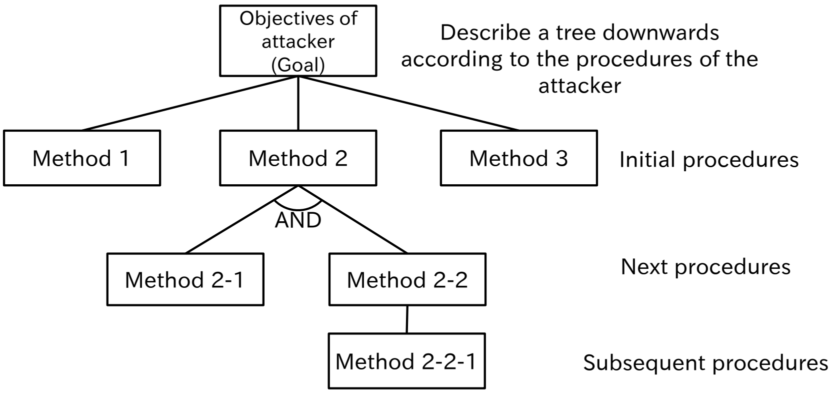
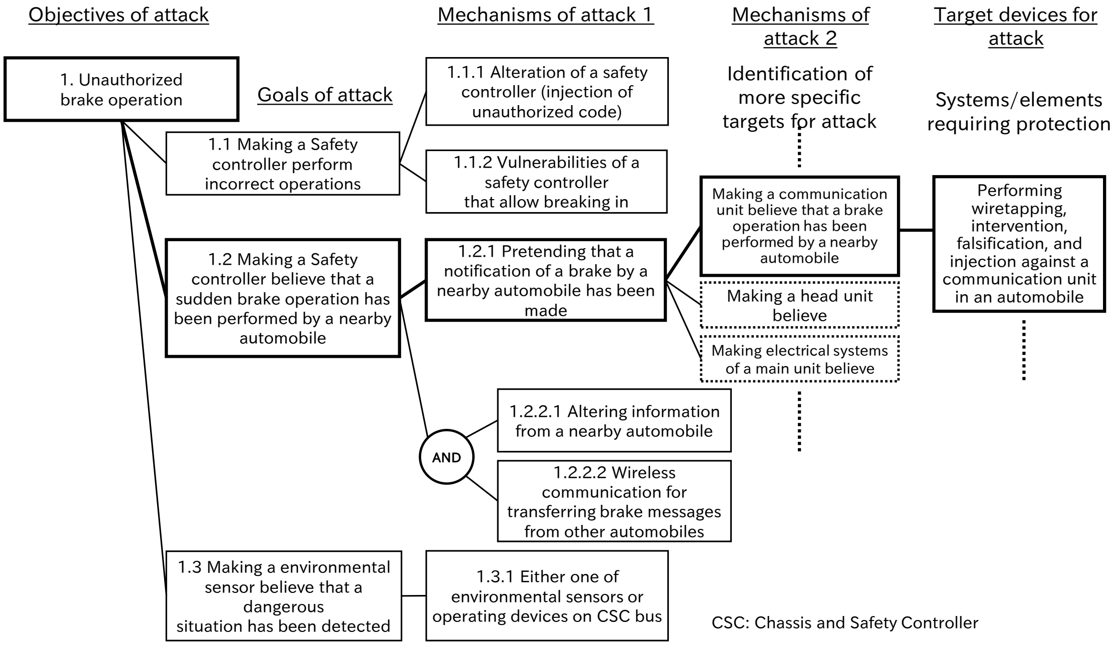


Figure 5-3 Image of an attack tree

In attack tree analysis, the objectives of the attack assumed from the attacker’s motives are expanded downwards in a tree structure by refining the steps for achieving the objectives and listing all assumed means.

Figure 5-4 shows an example of an attack tree created by an automotive security-related EU project “EVITA” [28]. For the top event “1” in the upper left of the figure, the threats and attack methods are expanded in a tree structure. It differs from the attack tree in Figure 5-3 in that, similar to FTA described in Chapter 4, terminal leaves refer to devices subject to the first attack.


Objectives of attack
Mechanisms of attack 1
Mechanisms of attack 2
Target devices for attack
1. Unauthorized brake operation
Goals of attack
1.1.1 Alteration of a safety controller (injection of unauthorized code)
Identification of more specific targets for attack
Systems/elements requiring protection
1.1 Making a Safety controller perform incorrect operations
1.1.2 Vulnerabilities of a safety controller that allow breaking in
Making a communication unit believe that a brake operation has been performed by a nearby automobile
Performing wiretapping, intervention, falsification, and injection against a communication unit in an automobile
1.2 Making a Safety controller believe that a sudden brake operation has been performed by a nearby automobile
1.2.1 Pretending that a notification of a brake by a nearby automobile has been made
Making a head unit believe
Making electrical systems of a main unit believe
1.2.2.1 Altering information from a nearby automobile
AND
1.2.2.2 Wireless communication for transferring brake messages from other automobiles
1.3 Making a environmental sensor believe that a dangerous situation has been detected
1.3.1 Either one of environmental sensors or operating devices on CSC bus
CSC: Chassis and Safety Controller

Source: Prepared based on “自動車の情報セキュリティへの取組みガイド”, IPA [29]

Figure 5-4 Example of an attack tree of automotive security in EVITA (FTA type)

(4) Identification of threats using Misuse Case

Attackers attack devices and systems in a manner unexpected by the designers. Threats are therefore identified by creating a “Misuse Case diagram”, which adds “attackers” to a “Use Case diagram” (diagram created by assuming the scenes for use from the point of view of users), and assuming the attacker’s objectives of attacking the target devices and systems and benefits to be gained [30]. This method makes assuming the attacker’s motives easier by setting the attribute of the attacker to an individual or organization and assuming the consequences such as money or social impacts.

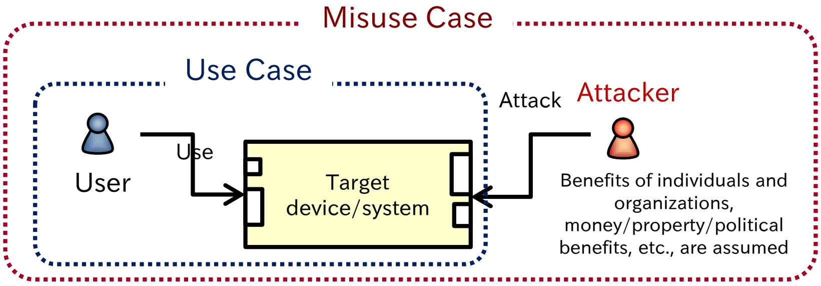

Misuse Case
Use Case
User
Use
Target device/system
Attack
Attacker
Benefits of individuals and organizations, money/property/political benefits, etc., are assumed

Figure 5-5 Analysis including the point of view of attackers

(Misuse Case diagram)

(5) Collecting and sharing information on the latest threats

In order to respond to diversified cyber-attacks, Information Sharing and Analysis Centers (ISAC) are established in the respective sectors both domestic and overseas [31] [32] to collect and share information on the latest threats. Information on the latest threats can also be collected from ICS-CERT (The Industrial Control Systems Cyber Emergency Response Team), a threat response organization by the U.S. Department of Homeland Security (DHS), statistical documents and reports (10 Major Security Threats, etc.) published by IPA, Japan, and research papers of international conferences such as “Black Hat”. Information on threats to consumer devices is expected to be also provided both domestically and overseas in the future. Utilization of such information is considered to make the identification of the latest threats to devices and systems easier.

(6) Example of threats

For the purpose of showing what threats are identified by the methods described in this section, examples of concrete threats in automotive and smart home electrical appliances sectors are listed here.

Table 5-3 Example of threats in automotive sector

No.	Type of threats	Example of threats
1	Settings without much consideration	Setting passwords to car navigation systems that can easily be guessed, etc.
2	Virus infection	Virus infection to car navigation systems via USB and abnormal behavior caused, etc.
3	Unauthorized use	Interference of using automobiles by abuse of remote vehicle management systems, etc.
4	Unauthorized setting	Unauthorized change of vehicle settings using maintenance tools, etc.
5	Information leakage	Leakage of personal information on car navigation systems, etc.
6	Tapping	Tapping of communications between in-vehicle devices and service centers, etc.
7	Service stoppage	Smart key locks disabled by radio interference, etc.
8	False message	Provision of false traffic information by taking over the control of traffic systems, etc.
9	Loss of logs	Deletion of data on drive recorders, etc.
10	Unauthorized relay	Smart keys unlocked through unauthorized relay of wireless communications, etc.
11	Repudiation	Denial of vehicle setting change and other operations by users, etc.
12	Elevation of privilege	Extraction of data from an event data recorder (recording equipment of operation and vehicle behavior histories) by unauthorized persons, etc.

Table 5-4 Example of threats in smart home electrical appliances sector

No.	Type of threats	Example of threats
1	Settings without much consideration	Setting passwords to air conditioners that can easily be guessed, etc.
2	Virus infection	Virus infection of home routers, unauthorized relay of communications, etc.
3	Unauthorized use	Peeking through unauthorized access to home cameras, etc.
4	Unauthorized setting	Remote unauthorized change of recording settings, etc.
5	Information leakage	Identification of life patterns through leakage of electric power data from smart meters, etc.
6	Tapping	Fraudulently obtaining health data by tapping wireless communications of health care devices, etc.
7	Service stoppage	Battery exhaustion and termination of gas meters by repeated illegal meter operations, etc.
8	False message	Display of false messages by falsifying home information services data, etc.
9	Loss of logs	Loss of traces by deletion of logs after unauthorized access to home electrical appliances is made, etc.
10	Unauthorized relay	Unauthorized operation of home electrical appliances by unauthorized relay of wireless communications of wearable devices that turn air conditioners on when the devices come close to home
11	Repudiation	Denial of pay-per-use services of home electrical appliances, etc.
12	Elevation of privilege	Removal of parental settings by children, performing operations prohibited by parents, etc.

5.2.2 Estimation and evaluation of risks against threats

Once threats are identified, the probability of occurrence and severity of damage are clarified by analyzing situations where the threats lead to damages. For instance, the attacks made by entering into a parking space or home and connecting wires to devices are more likely to be witnessed when compared to the attacks made over the Internet, and are therefore considered to be more difficult to perform (less likely to occur). In addition, the severity of damage varies between the attacks that cause malfunction to safety functions of devices and systems and the attacks that wiretap measurement data such as temperature and humidity.

The risks are then estimated from the probability of occurrence (determined from the actual frequency of occurrence, level of difficulty, benefits of attackers, etc.) and severity of damage to determine whether they are at a tolerable level or not. The concrete risk evaluation procedures are described below.

(1) Risk evaluation using hazard analysis methods

The safety methods such as FTA, FMEA, and HAZOP described in Chapter 4 can be used for risk evaluation. In FTA, for instance, the causes of “events” such as failures and accidents, are analyzed using a tree structure. The probability of occurrence of threats can be calculated by replacing “events” with “threats” and applying the “probability of occurrence (annual frequency of occurrence)” to the events in processes of a tree [33]. The risks can then be estimated from the value calculated and severity of damage.

(2) Risk evaluation of vulnerabilities using CVSS

CVSS (Common Vulnerability Scoring System) is a method that quantifies the “severity of damage” from the “depth of damage” and “ease of attack” of “vulnerabilities” that can cause threats to information systems under the same criteria [34]. The risks can be estimated from the probability of occurrence and quantified severity. CVSS has an advantage of simplicity that a single indicator can be derived by using a specified calculation formula. The calculation formula for CVSS is weighted based on accumulated information on the current vulnerabilities. In CVSS v2 (version 2), the CVSS base values less than 4 are classified into the severity of “caution”, values 4 or greater but less than 7 into the severity of “warning”, and values 7 or greater into the severity of “dangerous”. CVSS was established as an international standard by ITU X.1521, and is adopted as an indicator for vulnerabilities by more than 30 websites that provide information on vulnerabilities worldwide [35].

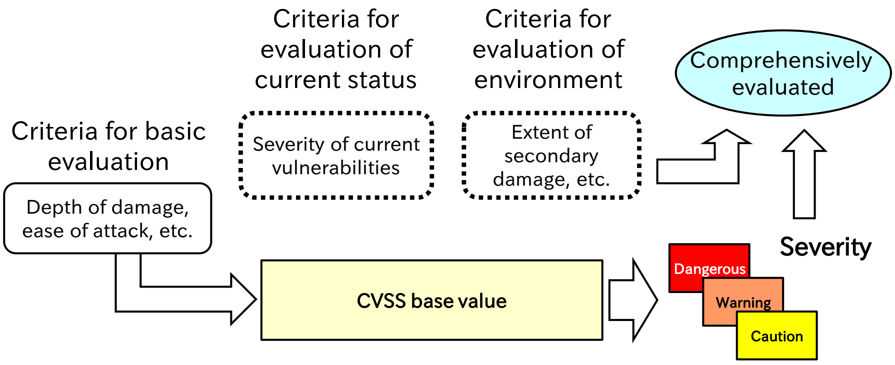

Criteria for evaluation of current status
Criteria for evaluation of environment
Comprehensively evaluated
Criteria for basic evaluation
Severity of current vulnerabilities
Extent of secondary damage, etc.
Depth of damage, ease of attack, etc.
Severity
CVSS base value
Dangerous
Warning
Caution

Figure 5-6 Image of evaluation of vulnerability severity in CVSS

(3) Other risk evaluation methods on threats

Other than those described above, methods such as MASG (Advanced Misuse Case Analysis Model with Assets and Security Goals) [36], goal-oriented requirements analysis methods (KAOS method, etc.) [37], i* (i-star) framework [30] [38], Secure Tropos [30] [38] are under research.

In March 2015, Society of Automotive Engineers of Japan, Inc. published a guidebook for information security for vehicles. . It provides analysis methods developed by applying CVSS described in this section, and serves as a useful reference as risk analysis procedures in other sectors.

5.2.3 Security design methods

(1) Approaches to security measures

As shown in Figure 1-6 in Chapter 1 (p.10), the following measures are taken based on the results of risk evaluation.

・If the risk is very large, take “risk avoidance”, including termination of the development

・If the risk is sufficiently small, take “risk retention” by not taking any particular measures

・If the damage is serious but the probability of occurrence is low, take “risk sharing”, including insurances, outsourcing, etc.

In cases other than the above, “risk reduction” is taken by security design. However, convenience and security are in a trade-off relationship. For instance, strengthening user authentication functions of devices and systems has issues such as increasing users’ efforts. Certain considerations are therefore required.

Considering the possibility that security threats may affect safety functions, the management needs to be involved and formulate basic policies that will be the basis for making the above-mentioned decisions. In addition, a mechanism for adjusting the requirement specifications of safety and security measures is also necessary to avoid these measures from being duplicated or inconsistent.

The ideas of foolproof, fault tolerance, and multi-layered protection, etc., described in Table 4-8 in Chapter 4 (p.45) are also effective for security measures. More concretely, on the assumption that users are not capable of securely managing consumer devices, measures are taken based on the ideas of not allowing attacks to succeed by minimizing information stored in devices and user privileges, maintaining functionality of devices/systems even at the minimum in the case of a massive unauthorized access, and implementing multiple security functions.

(2) Effective design methods for security

The methods for improving design quality and mechanisms for improving safety of devices and systems shown in Table 4-9 and Table 4-10 in Chapter 4 (p.46) are also effective for security design. More concretely, designing with ambiguities eliminated by formal methods, minimizing the damage even in the case of virus infection of devices by domain segmentation, and enhancing availability (being able to be used when required) of devices and systems by multiplication can be achieved.

In addition, software defects that do not lead to accidents with normal use may provide clues to intentional attackers. The point of view of preventing attacks is therefore necessary in security design.

Table 5-5 shows examples of effective design methods for security design.

Table 5-5 Examples of effective design methods for security design

Method	Outline
Software quality improvement design	Integrate secure programming, secure coding, static analysis of codes, vulnerability evaluation, etc., into the development process in order to reduce vulnerabilities. [39]
Utilization of security framework	Discuss the adoption of development tools and parts with integrated security measure methods and functions for efficient implementation of security functions
Programming language	Discuss the use of programming languages with which vulnerabilities are less likely to be created such as those that enforce strict type checking, elimination of adverse effects, and use of declarative and simple technologies
Formal methods	If particularly high security is required, discuss the use of formal methods that enable logical verification of whether the design content meets the requirements or not

(3) Scale of Security level

Examples of scale of security level include the evaluation assurance level of Common Criteria called EAL (Table 5-6). For example, a high evaluation assurance level of “EAL4+”, which is “EAL4” with vulnerability test added, is required for smart cards (IC cards) embedded in passports [40]. In contrast, “EAL3”, which assumes the environment of use by unspecified users, is required for multi-function printers used in offices, home, and convenience stores [41]. Setting the scale of security level makes agreements on security levels between procurers and suppliers of the products easier.

Table 5-6 Evaluation assurance level (EAL) of security functions in Common Criteria

EAL	Content of assurance requirements	Assumed security assurance level
EAL1	Functional test	Assurance level of products for which safe use and operation are assured with the assumption that the products operate in closed environments
EAL2	Structural test	Assurance level of products of which the users and developers are limited and for which there is no significant threat to safe operation
EAL3	Methodical test and check	Assurance level of products that are used by unspecified users and for which measures against unauthorized use are required
EAL4	Methodical design, test and review	Assurance level of products that are produced by introducing security-oriented development and production lines to ensure high security in commercial devices/systems
EAL5	Semi-formal design and test	Assurance level of products that are developed and produced with support from security experts to ensure the maximum security in commercial products/systems in certain sectors
EAL6	Semi-formally verified design and test	Assurance level of special products that are developed by applying security engineering technologies in their development environments for protecting high-value assets against significant risks
EAL7	Formally verified design and test	Assurance level of products that are developed for protecting environments at extremely high risk and assets that justify high development costs

Source: Prepared based on the pamphlet of ISO/IEC 15408 (April 2014 version), IPA

(4) Elemental technologies for security treatment

Attackers make full use of various information, technologies, and tools to make attacks. Security treatment therefore needs to be performed by combining various security elemental technologies. More concretely, security needs to be ensured by combining technologies for protecting against attacks such as tamper resistance and encryption, technologies for verifying authenticity such as authentication and electronic signature, technologies for detecting attacks such as logging/monitoring and intrusion detection, etc. Table 5-7 shows examples of these elemental technologies.

Table 5-7 Examples of security elemental technologies

Technology name	Outline	Example of threats to be dealt with
Tamper resistance	In order to disallow analysis of software, encryption key data, etc., stored in devices, improve resistance to attacks by adding mechanisms such as automatically erase memory when broken open, special circuits that prevent analysis by electromagnetic emanations and measuring power consumption, etc.	Prevent software stored in devices from being retrieved and used to produce copied products
Encryption	Prevent information leakage, even when data is retrieved in an unauthorized manner or wiretapped, by encrypting data stored in devices and data transmitted between devices	Prevent invasion of privacy through tapping personal data measured by consumer devices during transmission
Authentication	Prevent unauthorized use and replacement of devices/components through spoofing by verifying authenticity of legitimate users, servers, and devices, etc.	Prevent devices from being used by non-owners without permission
Access Control	Allow authenticated users to use devices and systems only within their privileges	Prevent children from using paid services without parents' permission by limiting operations using parental functions
Electronic signature	Ensure authenticity and integrity (not being falsified) of files by placing an electronic signature on important data such as software update files, etc.	Prevent virus infection through fake software update files being sent out
Intrusion detection	Detect unauthorized intrusion into devices and systems and falsification of memory or software in operation in real time	Immediately detect and block unauthorized access to devices through networks
Logging/ monitoring	Accumulate/analyze access records to devices and systems and produce statistics on the number of attacks, etc., to identify the source of attack in case of intrusion	Analyze logs of unauthorized access, identify the source of attack and the causes that allowed the attack to succeed, and respond

For security treatment of embedded systems, the guidebook for information security for embedded systems (IPA) [42], the guidebook for information security for vehicles (IPA) [29], etc., can be good references.

5.2.4 Designing security operation support functions

(1) Necessity of updating security functions

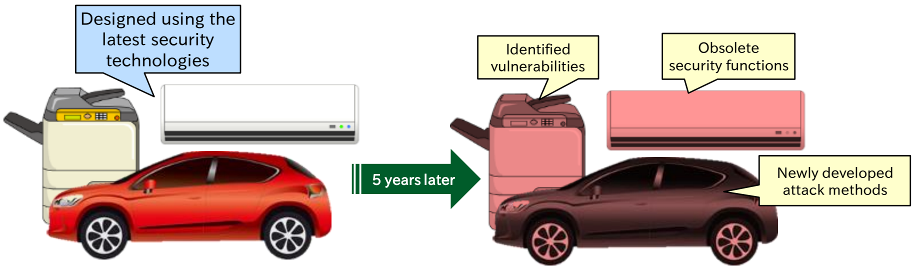

Designed using the latest security technologies
5 years later
Identified vulnerabilities
Obsolete security functions
Newly developed attack methods

Figure 5-7 Obsolescence of security design

In many cases, devices and systems that are related to daily life are used for 5 to 10 years. Even if security design is carried out using the latest technologies at the time of development, products are expected to quickly become obsolete over time after the release due to new vulnerabilities found, new methods developed by attackers, obsolescence of embedded security technologies associated with the advancement of technology, etc. In addition, attackers start attacking all at once when a new vulnerability is found. In security design to be performed in the future, security design that can quickly respond to vulnerabilities due to aging is important.

(2) Designing security updating functions

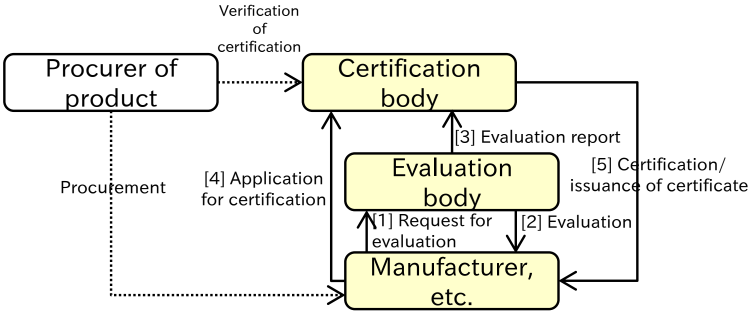
When responding to vulnerabilities due to aging, replacing devices or updating security functions at service centers require a lot of cost and effort. The method similar to that used for PCs of distributing software and security update data through networks and making devices and systems automatically update security functions is considered effective. For some devices such as car navigation systems, software functions and map data are updated by inserting USB memories, SD cards, through wireless networks, etc. The same mechanism is also considered usable in updating software to update security. In these cases, however, attacks that abuse software updating operations, including virus infection when devices are connected to networks, download of fake update data from spoof servers, falsification/transmission of update data, etc., need to be dealt with. In addition, mechanisms for detecting abnormal behavior of software and backdating updates are also necessary for cases where attacks to make unauthorized updates could not be prevented.

5.3 Evaluation/certification of security design

Mechanisms for objectively evaluating appropriate implementation of security treatment include certification systems for the management of information security control systems of companies/organizations and certification systems for the design and implementation of devices and systems. The latter includes Common Criteria certification for security functions of products and devices, CMVP (Cryptographic Module Validation Program) certification for encryption modules, and EDSA (Embedded Device Security Assurance) certification for control devices, and assures the design and implementation of standards-based security functions.

(1) Common Criteria-based third-party certification system

Common Criteria is an international standard for evaluating the appropriate design of information technology-related devices and systems and the correct implementation of the design from the point of view of information security [43]. Evaluation bodies evaluate the compliance with protection profile (PP) in which security requirements for each sector are compiled by the procurers and security target (ST) in which security requirements of devices and systems are compiled by the developers, and certification bodies certify compliance. The procurers can check certified devices on the certification bodies' websites (available if manufacturers prefer to disclose such information).


Verification of certification
Procurer of product
Certification body
[3] Evaluation report
Procurement
[4] Application for certification
Evaluation body
[5] Certification/ issuance of certificate
[1] Request for evaluation
[2] Evaluation
Manufacturer, etc.

Source: Prepared based on "IT セキュリティ評価及び認証制度", IPA [43]

Figure 5-8 Common Criteria certification scheme

The certificates of devices and systems under this scheme are valid in accordance with an international agreement by the member countries (CCRA: Common Criteria Recognition Arrangement [44]). Many products certified in the multi-function printer sector are disclosed on certification bodies' websites. A new agreement was announced in 2014, and in order to promote the utilization of this scheme in government procurement in each member country, cPP (Collaborative Protection Profile) [45] has been formulated for each product type in succession, including encryption storage such as USB memories, mobile devices, etc. [46]

(2) Vulnerability evaluation

In the software development of security-related functions, not only the verification of the correct implementation of security design but also the evaluation of vulnerabilities by methods such as those shown in Figure 5-9 is important.

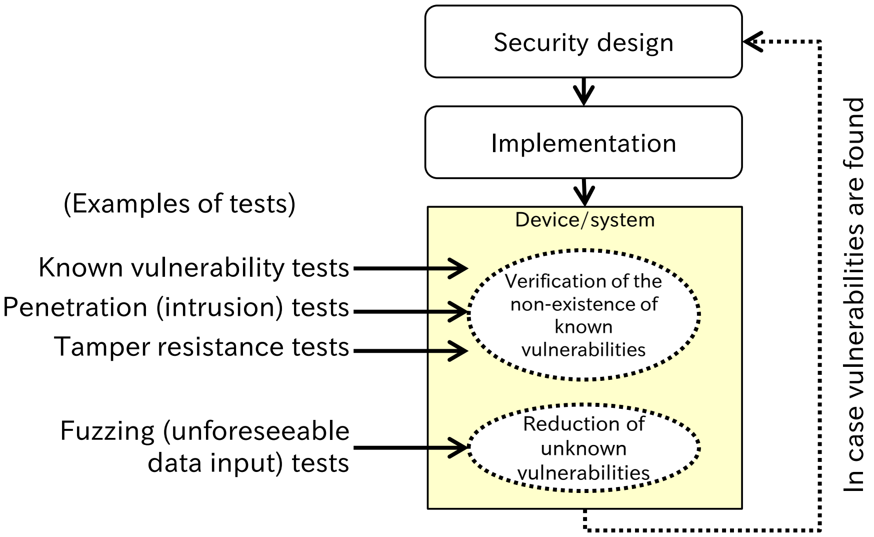

Security design
Implementation
(Examples of tests)
Device/system
Known vulnerability tests
Penetration (intrusion) tests
Tamper resistance tests
Verification of the non-existence of known vulnerabilities
Fuzzing (unforeseeable data input) tests
Reduction of unknown vulnerabilities
In case vulnerabilities are found

Figure 5-9 Image of vulnerability evaluation

In the evaluation phase, whether certain vulnerabilities are eliminated or not is verified. More concretely, verification is made to ensure that basic and important known vulnerabilities [47], including "SQL injection", "vulnerabilities in login functions", etc., do not exist. According to the intended use of the products, penetration tests, which imitate certain intrusion attack methods, and tamper resistance tests are also conducted.

In addition, "fuzzing test" is available as a black-box-like test that repeatedly inputs data that is likely to cause defects in products. This test is performed by using a tool that automatically generates an amount of test data [48]. Some certification standards such as EDSA require communication robustness tests [49], and fuzzing tests are performed for that purpose.

For important systems, security treatment is required even after the product release, including conducting risk evaluations whenever a new threat or attack method is found and making public the methods for avoiding risks, updating products, etc., as appropriate.

Column 4 Common Criteria and formal methods

For safety, obtaining certifications based on an international standard IEC 61508 for functional safety of electronic devices is becoming common practice. SIL is defined from 1 to 4 based on the probability of occurrence of a failure per hour (the higher the value, the higher the reliability), and for SIL2 and higher levels, adopting formal methods is recommended. As evaluation assurance levels for verifying the implementation of security functions based on ISO/IEC 15408, EAL1 to EAL7 are defined for security. These levels are also known as Common Criteria. For EAL5 or higher levels, the use of formal methods is provided as an assurance requirement. Formal methods are mathematics-based technologies used for the specification description, development, and verification of software and hardware systems in software engineering. Security requirements can be described as propositions (invariant conditions), and formal methods can effectively be used to prove the propositions. A number of methods, descriptions, and tools of formal methods are developed as the range of application expands, and are used according to the objectives.

For those who are planning to introduce formal methods, IPA published the following documents for beginners and those who are already familiar with them.

- “形式手法活用ガイドならびに参考資料” for solving the issues of introducing formal methods
- “厳密な仕様記述を志すための形式手法入門”, an educational material of formal methods for practitioners
- “厳密な仕様記述における形式手法成功事例調査報告書”

In addition, the following documents are listed in “先進的な設計・検証技術の適用事例報告書”, a collection of cases for improving software reliability.

Title	Source of case	Description language
形式手法を用いたセキュリティ検証	Arc System Solutions, Inc.	Event-B
宇宙システムにおける上流工程仕様の妥当性確認技術	Japan Aerospace eXploration Agency (JAXA)	SpecTRM, SPIN
モデル検査の適用による上流工程での設計の誤り	Toshiba Corporation	Promela, SPIN
モデル検査とテストによる車載オペレーティングシステムの検証	Japan Advanced Institute of Science and Technology	Promela, SPIN
通信制御ソフトウェア開発における状態遷移設計の品質向上への取り組み	Fujitsu Limited	Promela, SPIN
仕様記述言語 VDM++ を用いたシステムの仕様の記述	FeliCa Networks, Inc.	VDM++
形式仕様記述手法を用いた高信頼性を達成するテスト手法とその実践	FeliCa Networks, Inc.	VDM++

Column 5 Vital points of incident treatment

Masayuki Okuhara
Fujitsu Limited.

Cases and accidents that affect business operation, pose a threat to information security, etc., are generally called “security incidents”. For instance, the occurrence of external attacks to information systems, computer virus infections, discovery of security holes in information systems and products, etc., can be security incidents. When a security incident occurs, the situation needs to be appropriately and quickly controlled in order to minimize the damage caused by it.

The first thing we have to do when an incident occurs is to prevent the damage from spreading. We must collect necessary information and take an appropriate action within a limited time. Depending on the situation, we may have to make decisions that impose significant costs, including stopping operation, product recalls, etc. In order to be able to make such decisions quickly, establishing emergency response policies in advance is extremely important.

We must then recover from the incident situation. The threats and problems that caused the incident must be fundamentally removed. Therefore, we need to spend a certain amount of time investigating the causes. After the threat of the incident is removed, we must make detailed analysis of the incident and report to relevant parties. The results are then accumulated as knowledge to be utilized for preventing future incidents.

Such security incident treatment is mainly carried out by security incident response teams, CSIRT (Computer Security Incident Response Team) or ISIRT (Information Security Incident Response Team). Establishing these teams on a regular basis helps appropriately and quickly carrying out incident treatment.

Examples of guidelines for incident treatment and reference information on the establishment of security incident response teams are as follows:

ISO/IEC 27035:2011	Information technology -- Security techniques -- Information security incident management
ISO/IEC 29147:2014	Information technology -- Security techniques -- Vulnerability disclosure
ISO/IEC 30111:2013	Information technology -- Security techniques -- Vulnerability handling processes
Japan Computer Emergency Response Team Coordination Center	https://www.jpcert.or.jp/

Chapter 6

Explaining logical design quality

The method of explaining why the design used for target devices and systems can achieve the objectives logically and in a manner easily understandable by third parties based on the facts (evidences) is called "visualization of design quality". Visualization is also effective in safety and security design.

A visualization method "Assurance Case" is required in certification of some industrial and international standards, and is beginning to be utilized as a method for sharing complex design information at the design/development sites.

6.1 Visualization of software design quality

When the content of software design is reviewed within the company or by outsourced companies, or software resources are reused for the new development, design documents must be available. These documents need to be described in a manner understandable by third parties and explained logically based on the facts (evidence) that the objectives can be achieved by the design. This makes explaining/sharing "design quality" to/with third parties and understanding past designs easier.

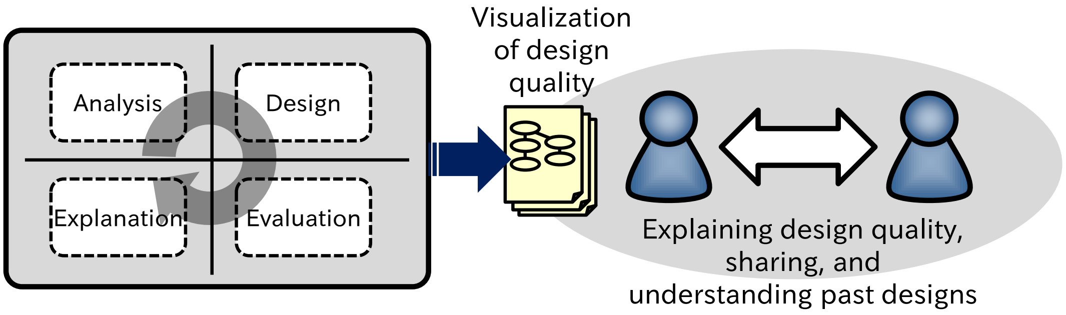

Analysis
Design
Explanation
Evaluation
Visualization of design quality
Explaining design quality, sharing, and understanding past designs

Figure 6-1 Visualization of software design quality

The expected effects of the "visualization of design quality" of software are as follows.

(1) Verification of design content when reusing software

When using software of existing products or general-purpose libraries in new development of products or version upgrade, utilization of "visualized" documents is effective for verifying the design content. In safety and security design in particular, verifying the assumptions, processes, and rationale of safety and security design of existing software and sorting out the parts to be reused can make the design more efficient.

(2) Agreement of design quality with stakeholders

In performing safety and security design of devices and systems, whether the objectives can be achieved by the design or not and whether the review process in design is appropriate or not need to be explained to stakeholders (relevant development department, quality control department, ordering and outsourced companies, etc.) as appropriate. This requires a mechanism to share design information.

In safety and security design in particular, explaining the treatment of significant risks to the management to obtain their understanding and consent is necessary. For this reason, "visualized" documents that enable explaining the design logically and in a manner understandable by third parties based on the facts (evidence) are effective.

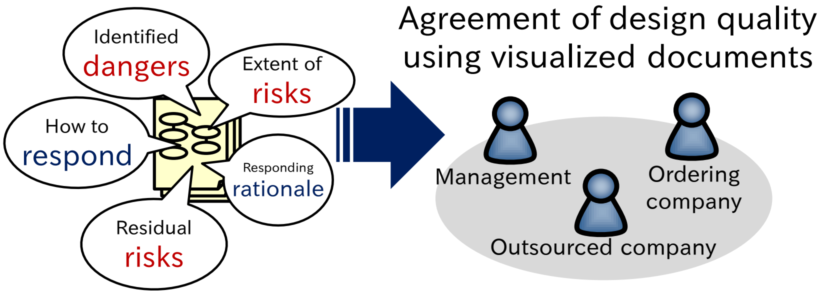


Figure 6-2 Agreement of design quality with the management, ordering companies, outsourced companies, etc.

(3) Traceability and accountability

If a problem occurs in devices or systems, the causes need to be immediately identified by tracking design history and review processes, based on documents and other materials (traceability). In addition, obligations to clarify the existence of design defects and explain it to users and relevant parties also arise (accountability). For this, documents of the "visualization of design quality" can be effective. Preparing such documents using design documents as reference after the accidents occur would be too late for emergency response and would not be suffice as evidence for design quality. Implementing visualization when designing devices and systems is therefore important.

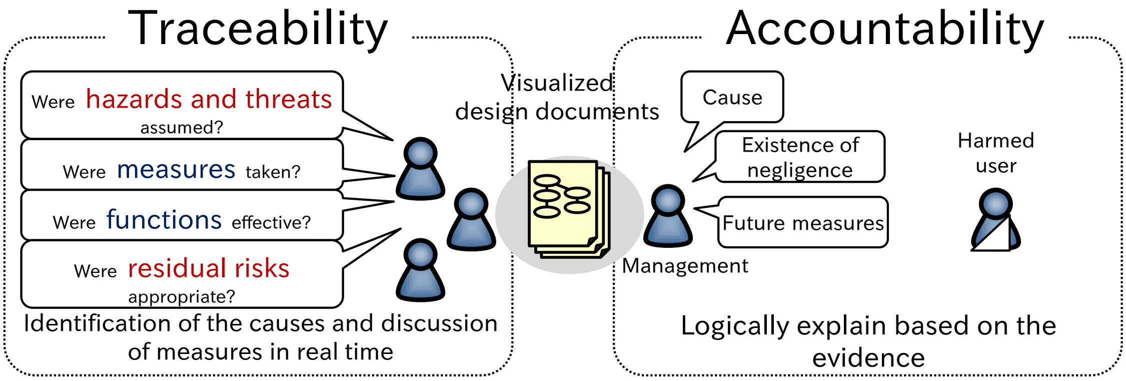

Traceability
Were hazards and threats assumed?
Were measures taken?
Were functions effective?
Were residual risks appropriate?
Identification of the causes and discussion of measures in real time
Visualized design documents
Accountability
Cause
Existence of negligence
Future measures
Management
Harmed user
Logically explain based on the evidence

Figure 6-3 Explaining and sharing design quality at the time of problem occurrence

(4) Acquisition of industrial and international standards certifications

There are schemes for certifying products in certain sectors based on industrial and international standards. In these schemes, evaluation bodies evaluate whether products confirm to standards or not and certification bodies certify/register products that meet the requirements of standards. Governments and companies that are users of products can make reliable product procurement without evaluating the products themselves by using the existence of certification as reference and/or including it in the procurement conditions. “Visualization of design quality” is effective when explaining to certification bodies that products are designed in compliance with standards.

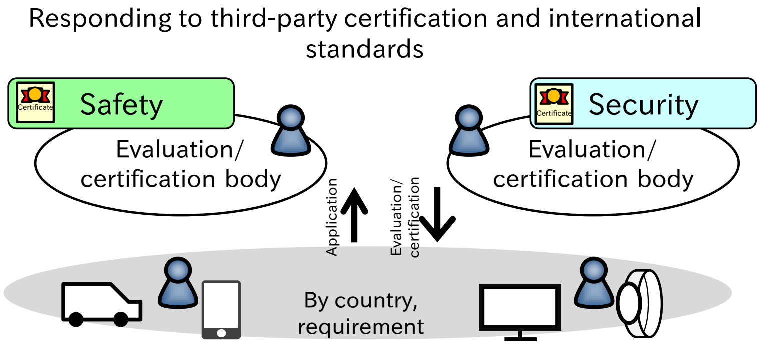

Responding to third-party certification and international standards
Certificate
Safety
Evaluation/ certification body
Certificate
Security
Evaluation/ certification body
Application
Evaluation/ certification
By country, requirement

Figure 6-4 Responding to third-party certification and international standards

International standards on safety exist in automotive and health care sectors, and inclusion of security is being discussed at present. In some international standards, certification schemes that make certifications obtained in Japan to be effective in other countries exist. However, there are still many standards that require evaluation/certification for each country/region. Making visualization of design in a manner that is internationally acceptable is therefore effective.

(5) Various scales of safety and security in international standards

Table 6-1 shows the scales that indicate safety and security treatment levels used in international standards. This reveals that different scales are used in each industry, and even if the name of the scales are the same, those that are defined differently are used. At present, there has been a trend of unifying safety scales in some standards, including IEC 62061 (SIL) and ISO 13849-1 (PL), etc. In anticipation of the coming “Smart-society”, discussions are expected to proceed to enable the application of safety of security scales also between devices in different sectors.

Table 6-1 Examples of scales used in international standards

Standard/series of standard	Examples to which the scale applies	Scale	Remark
Safety			
ISO 10218-1	Robots and robotic devices (industrial robots)	PL/SIL	Refers to PL (ISO 13849-1) and SIL (IEC 62061) for the scale
ISO 13482	Robots and robotic devices (personal care robots)	PL/SIL	Refers to PL (ISO 13849-1) and SIL (IEC 62061) for the scale
ISO 13849-1	Machinery (parts of control systems)	PL	Interrelationship with SIL of IEC 62061 is defined
ISO 25119	Tractors and machinery for agriculture and forestry	AgPL	5 levels indicating the performance of safety-related components under foreseeable conditions
ISO 26262	Road vehicles	ASIL	ASIL is a scale specific to ISO 26262
IEC 61496	Machinery (Electro-sensitive protective equipment)	Type	SIL/PL is applied by type
IEC 61508	Electrical/electronic/programmable electronic safety-related systems (general)	SIL	IEC 61508 is positioned as a functional safety-related basic standard
IEC 61511	Safety instrumented systems for process industry	SIL	Same as SIL of IEC 61508
IEC 62061	Safety-related electronic control systems for machineries	SIL	Similar to SIL of IEC 61508, but the definition is different in a precise sense
IEC 62304	Life cycle process of medical device software	Class	Scale based on the significance of hazards caused by software systems
Security			
ISO/IEC15408	Security techniques on IT products and information systems	EAL	Scale applied according to the number and type of evaluation items of products and design documents. In the process of discussing revisions at present
IEC 62443	Industrial communication networks	SL	Covers all aspects of operational administration, systems, and equipment of control systems (partly completed and partly under development)

PL: Performance Level, SIL: Safety Integrity Level, AgPL: Agricultural Performance Level, ASIL: Automotive Safety Integrity Level, EAL: Evaluation Assurance Level, SL: Security Level (in the order of appearance in the table)

Examples of methods for visualization of design quality described in this section include a method called “Assurance Case” . It is described in the next section with concrete notations.

6.2 Assurance Case

(1) Outline of Assurance Case

In 1988, a fire broke out in a North Sea oil field “Piper Alpha”, resulting in 167 deaths [50]. Operational rules were established in this oil field, but mechanisms to ensure safety were not sufficient and information exchange did not work out very well on-site. These are considered to be the causes of this catastrophic outcome. Reflecting on this accident, not only the rules and procedures on the safety of devices and systems are established but also “Safety Case” for logically explaining in an understandable manner based on evidence that safety can be ensured by them was introduced in the UK HSE (Health and Safety Executive) [51]. Similar approaches are also introduced in security and other sectors. They are called “Security Case” in the case of ensuring security and “Dependability Case” in the case of ensuring dependability, and are collectively called “Assurance Case”. Today, Assurance Case is required in a number of standards and guidelines as shown in Table 6-2.

Table 6-2 Examples of standards and guidelines that require Assurance Case

Sector	Examples of standards and guidelines that require Assurance Case	Outline
Aeronautics	Safety Case Development Manual (EUROCONTROL: The European Organization for the Safety of Air Navigation) [52]	Guidelines for creating Safety Case on safety management of air traffic control
Railway	The Yellow Book (UK Rail Safety and Standards Board Ltd.) [7]	Assurance of safety of railway signaling systems in the UK
Military	Defence Standard 00-56 (MoD: UK Ministry of Defence) [53]	Standards of the UK Ministry of Defence on safety management systems for defence systems
Automotive	ISO 26262 (ISO: International Organization for Standardization) [54]	Standards on functional safety of automobiles
Medical Devices	Infusion Pumps Total Product Life Cycle / Guidance for Industry and FDA Staff (FDA: U.S. Food and Drug Administration / Infusion Pump Improvement Initiative) [55]	Guidelines on infusion pumps of medical devices

(2) Notations of Assurance Case

The basic descriptions of "Assurance Case" are provided for in ISO/IEC 15026-2, and notations are described in natural language used by humans on a daily basis. In addition, the use of graphical notations of "Assurance Case" as shown in Table 6-3 is also becoming popular. By using these notations, the content and rationale of the claims as well as their relationship can be expressed in an understandable manner with diagrams and arrows.

Table 6-3 List of graphical notations of Assurance Case

Notation / Characteristic	CAE	GSN	D-Case
Formal name	Claims, Arguments and Evidence	Goal Structuring Notation	Dependability Case
Year of appearance	1998	2011	2012
Constituent element	3 types (claim, argument, evidence)	6 types (see Table 6-4 on the next page)	Extended GSN (monitor, parameter, action, external, accountability)
Developed by	Adelard (UK), University of London	York University (UK)	DEOS Project (Japan)

CAE is a notation designed for simplicity and efficiency, which uses 3 elements of Claims, Arguments, and Evidence [56]. GSN is a notation used for Assurance Case that serves as an evidence document in standards such as ISO 26262 [57]. D-Case is a notation based on GSN and extended for making descriptions to ensure dependability. The Working Group on D-Case of the Association of Dependability Engineering for Open Systems (DEOS Association) made publicly available D-Case editor, which can also be used to describe GSN [58]. In addition, SACM (Structured Assurance Case Metamodel) has been standardized as a meta-model of Assurance Case notations by OMG [59], and Assurance Case expressed in CAE and GSN, etc., can be converted via attribute notations in SACM format.

As an example of notations, Table 6-4 shows constituent elements of GSN.

Table 6-4 Constituent elements of GSN

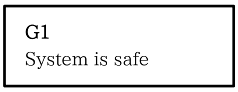
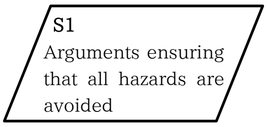
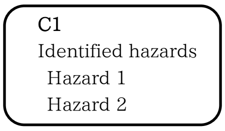
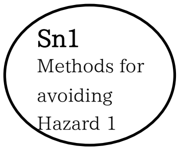
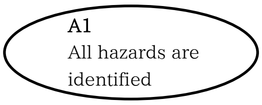
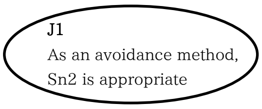
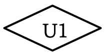
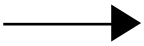
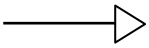
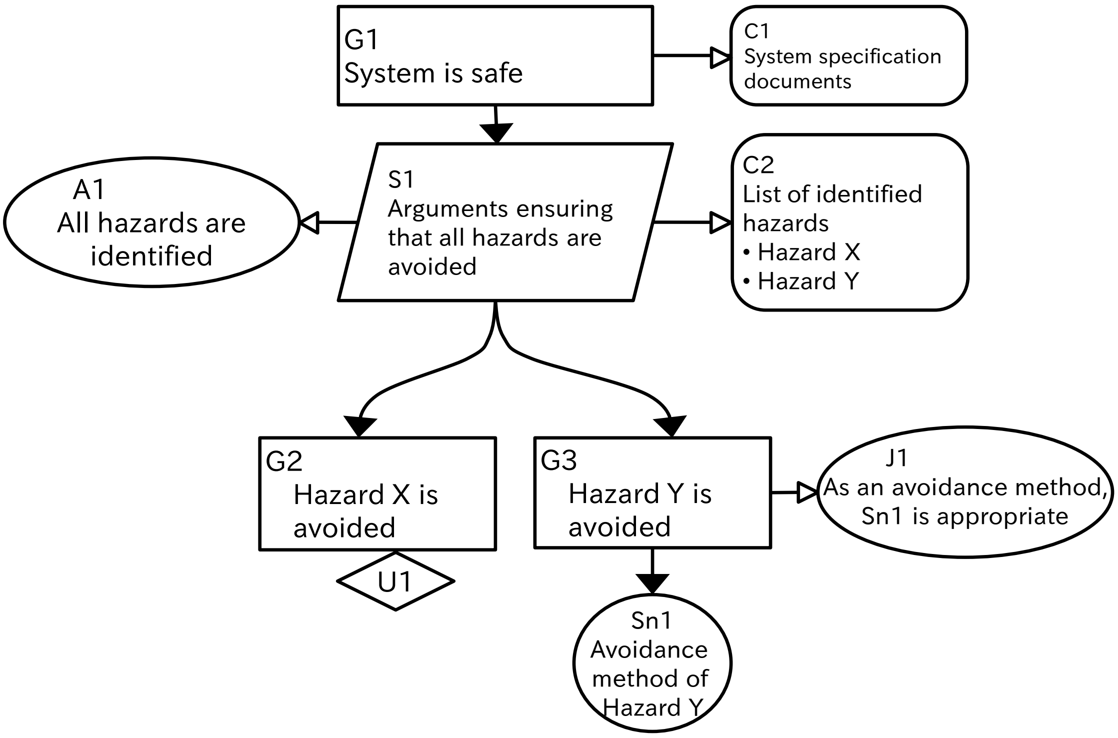
Constituent element	Description	Example of notation
Goal (Goal)	Matters to be assured (claim of arguments), goals are further broken down into more detailed goals (sub-goals)	
Strategy (Strategy)	Inferences existing between the goal and sub-goals that support the goal, ideas for breaking down into sub-goals	
Context (Context)	Underlying facts, information, and statements, etc., can also be expressed	
Solution (Solution)	Matters eventually ensuring that the goal can be achieved, concrete evidence	
Assumption	Assumptions on which certain claims or strategies are based	
Justification (Justification)	Reasons for applying certain claims or strategies, or the validity	
Undeveloped	Indicates elements not expanded in the flow of arguments. Can be attached to goals and strategies.	
Support link (Supported by)	Expressed with black arrows, and can be used from goals to goals, from goals to strategies, from goals to solutions, and from strategies to goals	
Context link (In Context by)	Expressed with white arrows, and can be used from goals to contexts, from goals to assumptions, from goals to justifications, from strategies to contexts, from strategies to assumptions, and from strategies to justifications	

Figure 6-5 shows an example of GSN notifications. As shown in the figure, shapes of boxes are fixed for each element. The boxes contain descriptions in natural language and are linked by lines, enabling notations of design arguments and proofs in a manner understandable by third parties.


G1
System is safe
C1
System specification documents
A1
All hazards are identified
S1
Arguments ensuring that all hazards are avoided
C2
List of identified hazards
• Hazard X
• Hazard Y
G2
Hazard X is avoided
U1
G3
Hazard Y is avoided
J1
As an avoidance method, Sn1 is appropriate
Sn1
Avoidance method of Hazard Y

Source: Prepared based on “セーフティとセキュリティ規格の同時認証方法論について”, National Institute of Advanced Industrial Science and Technology [57] and “GSN COMMUNITY STANDARD VERSION 1”, Origin Consulting, LLC (GSN Working Group) [60]

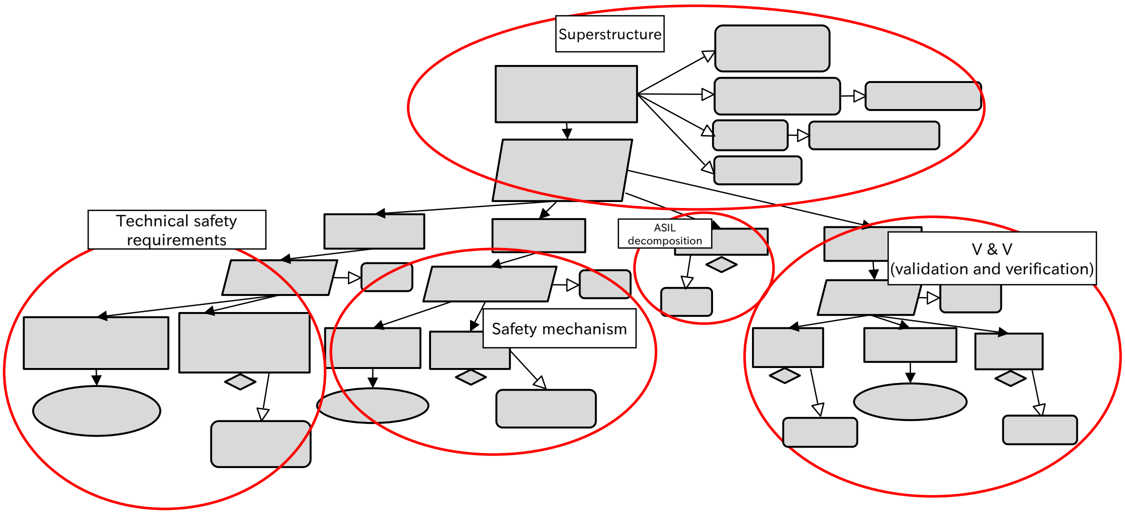
Figure 6-5 Example of GSN notifications

6.3 Concrete examples of Assurance Case

(1) Concrete examples on safety

In automotive sector, ISO 26262 is established as a functional safety standard. In this standard, “functional safety” is defined as “absence of unreasonable risk due to hazards caused by malfunctioning behavior of Electrical/Electronic (E/E) systems”, and covers electrical/electronic systems for automobiles. IPA experimentally created Safety Case for automobiles that complies with ISO 26262 using the above-mentioned GSN in FY 2012 [61].

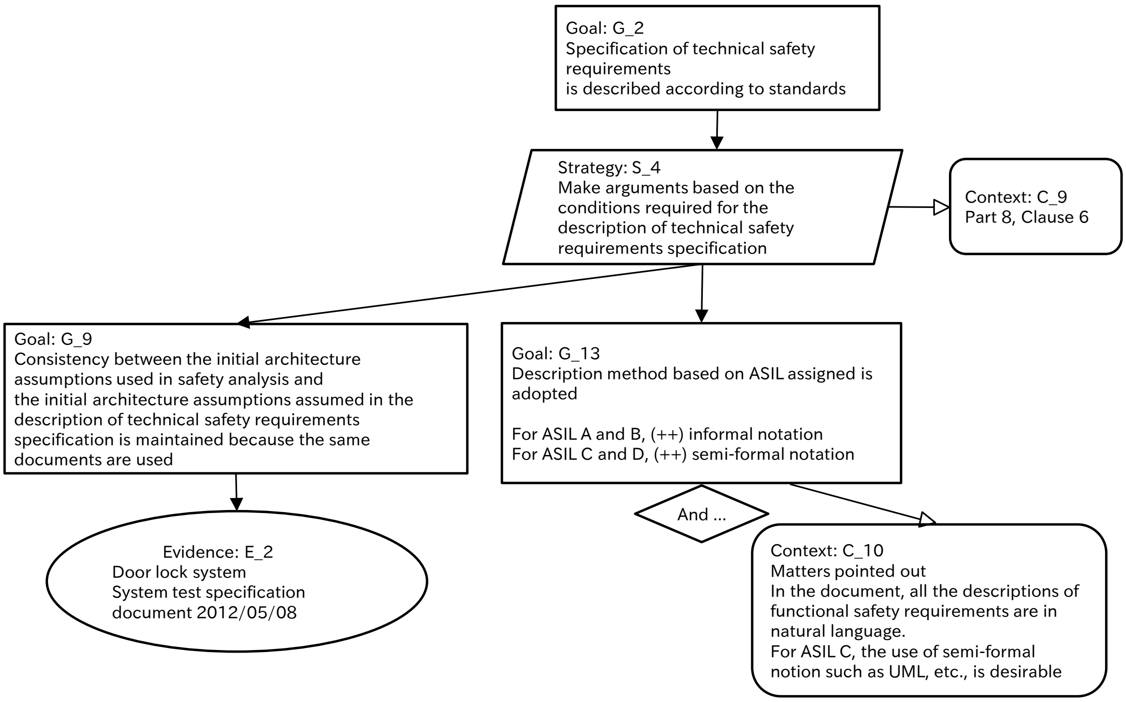
ISO 26262 is divided into 10 parts, and Part 4 provides for system-level product development. Figure 6-6 shows GSN notations of Clause 6 “Specification of the technical safety requirements” of this standard, consisting of “superstructure” for determining argument structure, the portion describing “technical safety requirements” specification, “safety mechanism”, “ASIL decomposition”, and “V & V (validation and verification)” of functional safety requirements.


Superstructure
Technical safety requirements
ASIL decomposition
V & V (validation and verification)
Safety mechanism

Source: Prepared based on “既製システムを ISO 26262 に適合させる場合のセーフティケースの利用とその評価” [61]

Figure 6-6 GSN diagram of ISO 26262 (Part4-6) experimentally created by IPA/SEC

Figure 6-7 shows technical safety requirements extracted from Figure 6-6. Strategy: S_4 positions Clause 6 “Specification and management of safety requirements” of Part 8 of ISO 26262 as Context: C_9.


Goal: G_2
Specification of technical safety requirements
is described according to standards
Strategy: S_4
Make arguments based on the conditions required for the description of technical safety requirements specification
Context: C_9
Part 8, Clause 6
Goal: G_9
Consistency between the initial architecture assumptions used in safety analysis and
the initial architecture assumptions assumed in the description of technical safety requirements specification is maintained because the same documents are used
Goal: G_13
Description method based on ASIL assigned is adopted
For ASIL A and B, (++) informal notation
For ASIL C and D, (++) semi-formal notation
And ...
Evidence: E_2
Door lock system
System test specification document 2012/05/08
Context: C_10
Matters pointed out
In the document, all the descriptions of functional safety requirements are in natural language.
For ASIL C, the use of semi-formal notion such as UML, etc., is desirable

Source: Prepared based on “既製システムを ISO 26262 に適合させる場合のセーフティケースの利用とその評価” [61]

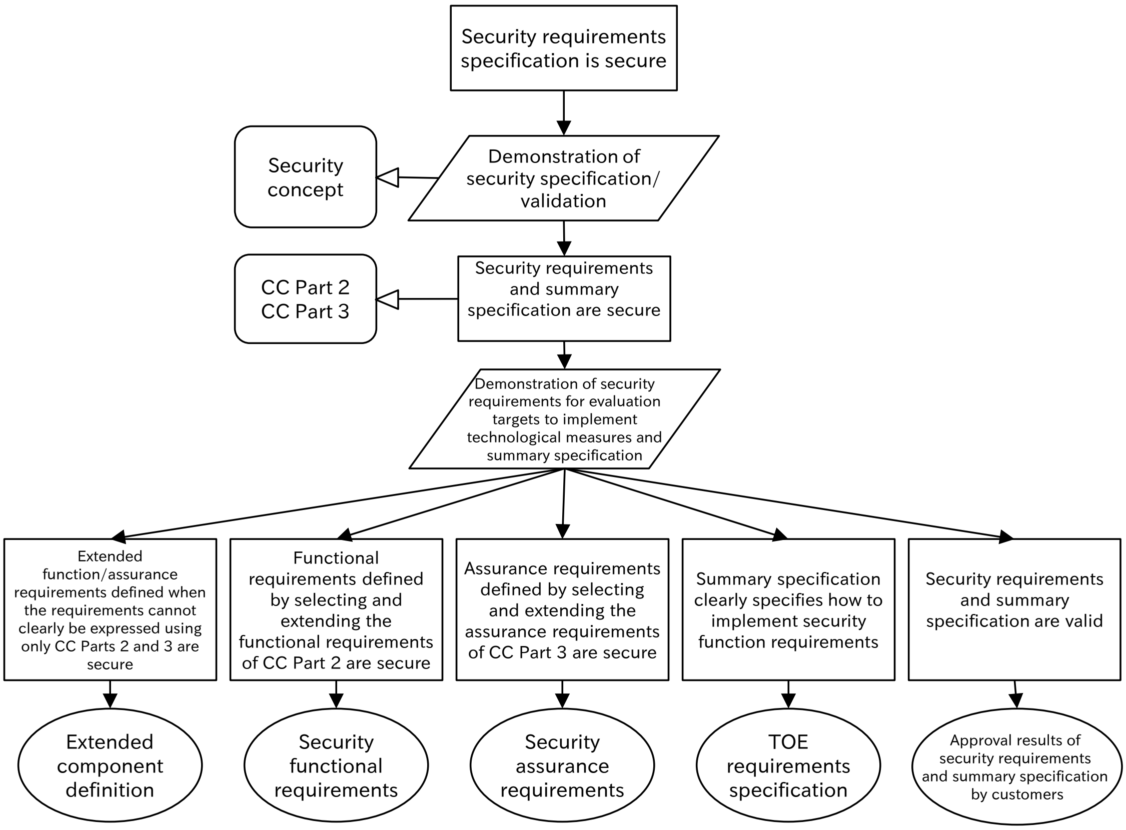
Figure 6-7 GSN diagram of the portion of “technical safety requirements specification” in ISO 26262 (Part4-6)

As explained above, the goals, arguments, risk treatment, and rationale of safety design are described in GSN. A graphical representation of the entire relationship is expected to make reviews by the quality control department and ordering party easier.

In medical devices sector, a report validating the safety of mobile infusion pumps (devices for injecting chemicals into the body regularly) that are already in common use in the U.S. by using Assurance Case has been published [62]. It is a research demonstration, but is at a practical level, and its widespread use is expected in the future.

(2) Concrete examples on security

When obtaining Common Criteria certification (see 5.3(1), p.64), “CC-Case” is proposed as a method for determining security specifications using Assurance Case [63]. In Common Criteria certification, security design specification documents for target products, Security Target (ST), are required. In CC-Case, ST creation (setting and validation) processes are described while Common Criteria certification standards are modeled and positioned as contexts. This makes creation of ST that complies with Common Criteria certification standards and confirmation of validation by evaluation bodies easier. Figure 6-8 shows an example of Assurance Case for the phase of security requirements specification, in which the methods of implementing security function requirements on actual systems are specified, in CC-Case.


Security requirements specification is secure
Demonstration of security specification/ validation
Security concept
CC Part 2
CC Part 3
Security requirements and summary specification are secure
Demonstration of security requirements for evaluation targets to implement technological measures and summary specification
Extended function/assurance requirements defined when the requirements cannot clearly be expressed using only CC Parts 2 and 3 are secure
Functional requirements defined by selecting and extending the functional requirements of CC Part 2 are secure
Assurance requirements defined by selecting and extending the assurance requirements of CC Part 3 are secure
Summary specification clearly specifies how to implement security function requirements
Security requirements and summary specification are valid
Extended component definition
Security functional requirements
Security assurance requirements
TOE requirements specification
Approval results of security requirements and summary specification by customers

Source: Prepared based on "CC-Case～コモンクライテリア準拠のアシュアランスケースによるセキュリティ要求分析・保証の統合手法", Institute of Information Security, etc. [63]

Figure 6-8 Assurance Case for security requirements specification phase in CC-Case

In addition, the U.S. Department of Homeland Security gives examples of Security Assurance Case for verifying security of system development through software development life cycles. Both give concrete Assurance Case and can be used as effective cases.

(3) Examples of visualization in design verification

When developed software is evaluated by customers, not only "test records" and "bug curves" but also "visualization" and presentation of internal review records of the development processes enable explanation of "development content" that include internal structure and implementation methods of software. In addition, "visualization" and presentation of "assumptions of developers" in refining the requirements of customers and "test item selection processes" in creating test specifications also enable explanation of “development processes” . Through these, new values can be presented to customers.

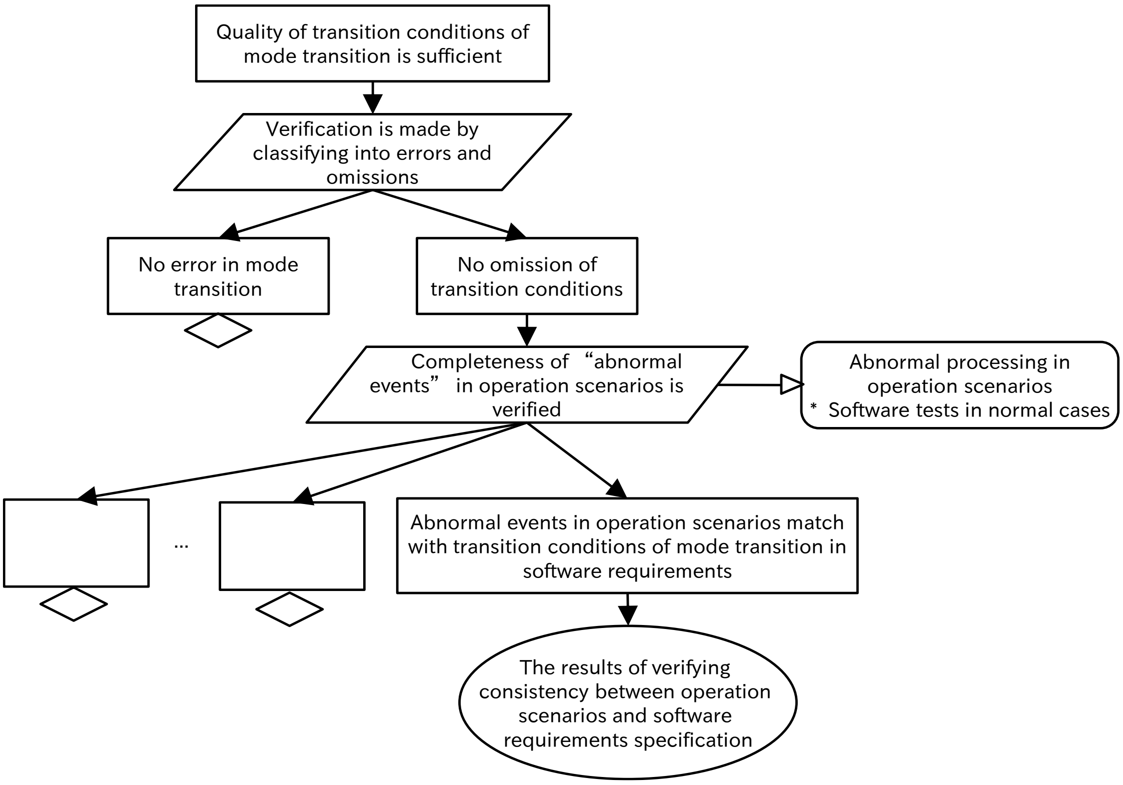

Quality of transition conditions of mode transition is sufficient
Verification is made by classifying into errors and omissions
No error in mode transition
No omission of transition conditions
Completeness of “abnormal events” in operation scenarios is verified
Abnormal processing in operation scenarios
* Software tests in normal cases
…
Abnormal events in operation scenarios match with transition conditions of mode transition in software requirements
The results of verifying consistency between operation scenarios and software requirements specification

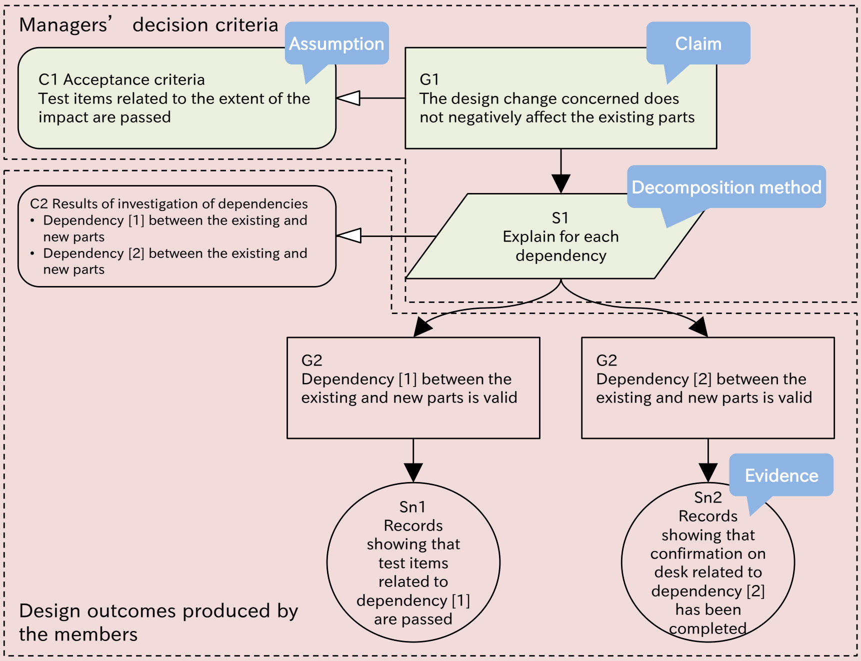
Figure 6-9 Examples of visualization in design verification

At present, evaluation of software design quality is mainly carried out through reviews by experts, but “visualization” of these reviews can enable sharing “evaluation processes” based on knowledge of experts with young developers. Active discussions focused on “visualized” documents between developers lead to improved design quality and reduction of rework in post-processes. Assurance Case is a method that enables “visualization” of logical relationships among “contexts (assumptions including implicit requirements)” , “strategies (strategies from reviewers' point of view)” , and “goals (items to be verified)” , and is effective for “visualization” of above-mentioned “development content” , “development processes” , and “evaluation processes” of software. This method allows customers to evaluate software quality from new aspects, and is expected to have various effects, including sharing of experts’ knowledge/skills, further improvement of design quality, etc.

Column 6 Methods that allow busy managers to review design content in greater depth

Nobuhide Kobayashi
Denso Create, Inc.

With the recent increased interest in safety and security, in addition to a general trend toward large-scale systems, managers at the forefront of development are required to have extensive knowledge to be able to view the entire system as well as in-depth knowledge to be able to make appropriate decisions on the validity of design outcomes produced by the members. It is difficult, however, for busy managers to have deeper knowledge than the members, therefore, they might have to review the validity of design outcomes based on only the compliance status of processes..


Managers' decision criteria
Assumption
Claim
C1 Acceptance criteria
Test items related to the extent of the impact are passed
G1
The design change concerned does not negatively affect the existing parts
Decomposition method
C2 Results of investigation of dependencies
• Dependency [1] between the existing and new parts
• Dependency [2] between the existing and new parts
S1
Explain for each dependency
G2
Dependency [1] between the existing and new parts is valid
G2
Dependency [2] between the existing and new parts is valid
Evidence
Sn1
Records showing that test items related to dependency [1] are passed
Sn2
Records showing that confirmation on desk related to dependency [2] has been completed
Design outcomes produced by the members

Case of visualization of content of outcomes

In the figure above, managers' decision criteria are linked to the design outcomes of the members so as to eliminate the above-mentioned situation and enable managers to determine the validity of design content in greater depth. The members who understand the design content explain it by breaking it down into appropriate detail based on the results of investigation (C2). This enables managers to be aware of the existence of outcomes (Sn2) that do not meet the acceptance criteria (C1) that the managers consider appropriate. As in this case, managers who can describe the ideal outcomes expected by customers and the members who have full knowledge of the content of the outcomes make up for each other's weaknesses through GSN to enable busy managers to make reviews in greater depth.

6.4 SafSec for simultaneous certification of safety and security

Obtaining individual certifications of safety and security standards require considerable efforts and costs, and therefore simultaneously obtaining both of them is extremely difficult. SafSec is a framework for efficiently obtaining both certifications through utilizing Assurance Case.

SafSec is created by Praxis High Integrity Systems Ltd. (now Altran Praxis) with support from the UK Ministry of Defence (MOD), and covers the UK safety standard Def-Stan 00-56 and international security standard ISO/IEC 15408 (Common Criteria), etc. In SafSec, the ability to provide reliable services is referred to as “dependability” and factors that lead to undesirable situations such as hazards and threats are referred to as “loss” in creating Assurance Case (Dependability Case). The SafSec concepts integrate the concepts of safety and security domains and exclude duplicated portions, thereby enabling the creation of documents that can commonly be used in obtaining safety and security certifications.

Table 6-5 Relationship of SafSec concepts

SafSec concepts	Safety domain concepts	Security domain concepts
Assurance requirement	SIL	EAL
Causal analysis	FTA, FMEA	Threat/vulnerability analysis
Dependability Case	Safety Case	ST(Security Target)
Dependability specification	Safety requirements	Security Objectives
Loss	Hazard	Vulnerability
Risk	Frequency and severity	Frequency and severity

Source: Prepared based on “セーフティとセキュリティ規格の同時認証方法論について”, National Institute of Advanced Industrial Science and Technology [57]

At present, SafSec has various issues. For example, methods used for hazard analysis and threat analysis are different, and therefore they cannot be expressed in a single Dependability Case. For this reason, it is necessary to create a Dependability Case first and then make changes to convert to respective Assurance Cases for safety and security standards certifications, thus requiring more efforts and costs than before in some cases.

6.5 Framework of Dependability Assurance Case

In March 2015, “DAF for SSCD (Dependability Assurance Framework for Safety-Sensitive Consumer Devices)”, an Assurance Case framework for consumer devices formulated by IPA/SEC, was adopted as a standard by an international standardization organization OMG (Object Management Group) [64]. This framework is a development methodology for ensuring high levels of safety, reliability, and availability of consumer devices, including automobiles, robots, smart houses, etc., and the structure is as shown in Table 6-6.

Table 6-6 Structure of DAF for SSCD

Abbreviation	Full name	Outline
DCM	Dependability Conceptual Model	Definition of Dependability Conceptual Model
DPM	Dependability Process Model	Definition of Dependability Process Model
DAC	Dependability Assurance Case	Assurance mechanism using Dependability Case

Source: Prepared based on “コンシューマデバイス機能安全規格が正式に OMG 標準規格へ”, IPA [65]

DCM expresses the structure of the existing functional safety standards in an easy-to-understand manner by visualizing it as a conceptual model, and is created using ISO 26262 (Parts 1-3) as reference. DPM provides development processes for ensuring dependability, and is characterized by the inclusion of repeated verification processes. DAC is a template for creating “Dependability Assurance Case (documents consisting of perspectives for achieving dependability, implementation means, evidence of implementation, etc.)”, and provides a proposed Dependability Assurance Case for engine stall of an automobile on which discussions are proceeding ahead of others.

This framework is highly compatible with Japanese-style *Suriawase* (adjustment-based) development, and can be used as reference for improving safety and reliability of consumer devices.

Conclusion

In the “Smart-society”, devices and systems around us work with each other through networks to create new services and values in our living environment. However, new issues also arise in the “Smart-society”, including threats spreading over networks, etc. Therefore, safety and security treatment is required more than ever in the development of devices and systems.

This document explains the methods of safety and security analysis and design in the “Smart-society”, and presents a method (Assurance Case) for enabling third stakeholders to understand/share them by visualizing the design quality. We hope this document can be of some help in effectively taking safety and security measures against current and future hazards.

Appendix References

[1] IPA/SEC, “組込みシステムの安全性向上の勧め（機能安全編）”, http://www.ipa.go.jp/sec/publish/tn05-011.html.

[2] Ministry of Education, Culture, Sports, Science and Technology, "外来語の表記”, 1991. http://www.mext.go.jp/b_menu/hakusho/nc/k19910628002/k19910628002.html.

[3] Japan Technical Communicators Association, "外来語（カタカナ）表記ガイドライン 第 2 版”, 2008. http://www.jtca.org/ai_collaboration/katakana_wg/katakana_guide.pdf.

[4] Ministry of Economy, Trade and Industry, Japan, "消費生活用製品安全法”, http://www.meti.go.jp/policy/consumer/seian/shouan/contents/shouan_gaiyo.htm.

[5] IPA, "情報セキュリティマネジメントと PDCA サイクル - リスクアセスメント”, 2015. https://www.ipa.go.jp/security/manager/protect/pdca/risk_ass.html.

[6] SESAMO Project, "SECURITY AND SAFETY MODELLING FOR EMBEDDED SYSTEMS, ISSE Workshop, 2014”, 2014. http://sesamo-project.eu/sites/default/files/downloads/publications/02-isse14-sesamo.pdf.

[7] Railtrack, “Engineering Safety Management Issue 3, Yellow Book 3, Volume 1 and 3, Fundamentals and Guidance”, 2000.

[8] IPA, "「情報処理システム高信頼化教訓集（IT サービス編）」2014 年度版”, http://www.ipa.go.jp/sec/reports/20150327_1.html.

[9] Connected Consumer Device Security Council, "生活機器の脅威事例集”, https://www.ccds.or.jp/public_document.html.

[10] Trend Micro, "急増する POS システムへの攻撃と POS マルウェアファミリ”, http://blog.trendmicro.co.jp/archives/9902.

[11] Ministry of Economy, Trade and Industry, Japan, "リスクアセスメント・ハンドブック実務編”, http://www.meti.go.jp/product_safety/recall/risk_assessment.html.

[12] IPA, "共通フレーム２０１３の概説”, https://www.ipa.go.jp/files/000027415.pdf.

[13] B. Nuseibeh, "Twin Peaks”, http://www.ics.uci.edu/˜andre/ics223w2006/nuseibeh.pdf.

[14] Ministry of Economy, Trade and Industry, Japan, "消費生活用製品向けリスクアセスメントのハンドブック第一版”, http://www.meti.go.jp/product_safety/recall/risk_assessment.html.

[15] IPA, "米国における STAMP（システム理論に基づく事故モデル）研究に関する取り組みの現状（前篇）”, https://www.ipa.go.jp/files/000038950.pdf.

[16] IPA, "米国における STAMP（システム理論に基づく事故モデル）研究に関する取り組みの現状（後編）”, https://www.ipa.go.jp/files/000039623.pdf.

[17] IPAセミナー (Japan Manned Space Systems Corporation), "安全解析手法STAMP／STPAの概要と事例紹介”, http://sec.ipa.go.jp/seminar/20140121.html.

[18] JEMIMA, "機能安全規格の技術解説”, 2013. http://tech.jemima.or.jp/doc/func_safety_201311.pdf.

[19] Written and edited by Society of Practical Study on R-Map / Union of Japanese Scientists and Engineers, "製品安全, リスクアセスメントのための R-Map 入門(第 1 版)”, 10 5 2011. https://www.juse.or.jp/reliability/introduction/03.html.

[20] NITE, Product Safety Technology Center,, "100 の事例から製品事故リスクを低減する､NITE の｢製品事故 100 選｣”, 2014. http://www.nite.go.jp/data/000055687.pdf.

[21] Ministry of Economy, Trade and Industry, Japan, "組込みシステム産業の課題と政策展開”, 16 11 2011. http://www.jasa.or.jp/et/ET2011/visitor/images/pdf/S1_web_data111116.pdf.

[22] Japan Society for the Promotion of Machine Industry, "機械の安全・信頼性に関するかんどころ”, 2011. http://www.jspmi.or.jp/system/file/3/839/document.pdf.

[23] Seiko Shirasaka, "アーキテクト～アーキテクトは何ができるのか～”, 2012.

http://home.jeita.or.jp/page_file/20121205162200_Vrq3c4OemA.pdf.

[24] Kevin Soo Hoo, "Tangible ROI through Secure Software Engineering, .Security Business Quarterly,. Vol.1, No.2, Fourth Quarter, 2001".

[25] Microsoft, "セキュリティ上の脅威の評価", https://msdn.microsoft.com/ja-jp/library/ms172104%28v=vs.80%29.aspx.

[26] Microsoft, "Security Planning Through Threat Analysis", 12 2007. https://msdn.microsoft.com/ja-jp/library/cc756184%28v=ws.10%29.aspx.

[27] MITRE, "CAPEC (Common Attack Pattern Enumeration and Classification)", http://capec.mitre.org/.

[28] EVITA Project, "Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios", 2009. http://www.evita-project.org/Deliverables/EVITAD2.3.pdf.

[29] IPA, "自動車の情報セキュリティへの取組みガイド", 2013. http://www.ipa.go.jp/security/fy24/reports/emb_car/.

[30] Nobukazu Yoshioka, National Institute of Informatics, "セキュリティ要求工学技術とその実効性", http://www.fuka.info.waseda.ac.jp/rewg-sub/workshop/201305/IPSJ-REWS-SSE-intro.pdf.

[31] Telecom-ISAC Japan, "セキュリティ情報提供", https://www.telecom-isac.jp/public/security.html.

[32] Mitsubishi Research Institute, Inc., "米国のセキュリティ情報共有組織（ISAC)の状況と運用実態に関する調査", 3 2010. http://www.nisc.go.jp/inquiry/pdf/fy21-isac.pdf.

[33] Yasuhiko Nagai, Hitachi, Ltd., "情報システムに対するセキュリティ国際標準化の動向と日立製作所の対応", http://www.hitachihyoron.com/jp/pdf/1999/06/1999_06_10.pdf.

[34] IPA, "共通脆弱性評価システム CVSS 概説", 20 3 2014. http://www.ipa.go.jp/security/vuln/CVSS.html.

[35] IPA, "脆弱性の深刻度評価の新バージョン CVSS v2 への移行について", 30 11 2009. http://www.ipa.go.jp/security/vuln/SeverityLevel2.html.

[36] Takao Okubo, Institute of Information Security,, "MASG", https://www.jstage.jst.go.jp/article/ipsjjip/22/3/22_536/_pdf.

[37] Yasuyuki Tahara, et al., The University of Electro-Communications, "KAOS によるセキュリティ要件の獲得・分析", 情報処理 Vol.50 No.3, p. 203, 2009.

[38] National Institute of Informatics, "安全要求分析", 2014. http://www.topse.jp/syllabus/09/html/sre_12014.htm.

[39] IPA, "セキュアプログラミング講座", http://www.ipa.go.jp/security/awareness/vendor/programmingv2/clanguage.html.

[40] JBMIA, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs, Japan, "旅券冊子用 IC のためのプロテクションプロファイル -能動認証対応-", 15 2 2010. http://www.ipa.go.jp/security/jisec/certified_pps/c0247/c0247_pp.pdf.

[41] IPA, "IEEE 2600.1™-2009:運用環境Ａにおけるプロテクションプロファイルの IEEE 標準規格(日本語訳)", 18 1 2012. http://www.ipa.go.jp/security/publications/ieee/index.html.

[42] IPA, "組込みシステムのセキュリティへの取組みガイド（2010 年度改訂版）", 2010. http://www.ipa.go.jp/security/fy22/reports/emb_app2010/.

[43] IPA, "IT セキュリティ評価及び認証制度", https://www.ipa.go.jp/security/jisec/index.html.

[44] IPA, "国際承認アレンジメント（CCRA）", 2015. http://www.ipa.go.jp/security/jisec/ccra/.

[45] IPA, "CCRA/ICCC 2014 報告, P.11, cPP とは", 2014. https://www.ipa.go.jp/security/jisec/seminar/documents/CCRAReport_20141022.pdf#page=11.

[46] IPA, "海外のプロテクションプロファイルの翻訳", 2014. http://www.ipa.go.jp/security/publications/pp-jp/index.html.

[47] Local Authorities Systems Development Center (LASDEC), "地方公共団体における情報システムセキュリティ要求仕様モデルプラン（Web アプリケーション）", 2012. https://www.j-lis.go.jp/lasdec-archive/cms/12,28369,84.html.

[48] IPA, "脆弱性対策：ファジング", http://www.ipa.go.jp/security/vuln/fuzzing.html.

[49] CSSC Certification Laboratory, "ISASecure® EDSA 認証とは", http://www.cssc-cl.org/jp/about_edsa/index.html.

[50] Oil&GasUK, "Piper Alpha: Lessons Learnt, 2008", http://www.oilandgasuk.co.uk/cmsfiles/modules/publications/pdfs/HS048.pdf.

[51] The Japan Society of Naval Architects and Ocean Engineers, "大規模海上浮体施設の構造信頼性および設計基準研究委員会報告書", http://www.jasnaoe.or.jp/research/dl/report_p-8.pdf.

[52] European Air Traffic Management, Safety Case Development Manual, European, 2006.

[53] The United Kingdom Ministry of Defence (MOD) Ministry of Defence, Defence Standard 00-56, Issue 4, 2007.

[54] ISO, ISO 26262, Road Vehicles – Functional Safety, 2011.

[55] FDA, "Infusion Pumps Total Product Life Cycle Guidance for Industry and FDA Staff", 2 11 2014. http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm209337.pdf.

[56] Adelard LLP, "Claims, Arguments and Evidence (CAE)", http://www.adelard.com/asce/choosing-asce/cae.html.

[57] Kenji Taguchi, National Institute of Advanced Industrial Science and Technology, "セーフティとセキュリティ規格の同時認証方法論について", http://www.ipa.go.jp/files/000044156.pdf.

[58] D-Case, "D-Case チーム", http://www.dcase.jp/.

[59] OMG, "Structured Assurance Case Metamodel (SACM), Version 1.0", http://www.omg.org/spec/SACM/1.0/.

[60] G. W. Group, "GSN Standard", http://www.goalstructuringnotation.info/.

[61] IPA/SEC, "既製システムを ISO26262 に適合させる場合のセーフティケースの利用とその評価", 2013. http://www.ipa.go.jp/files/000026856.pdf.

[62] Software Engineering Institute, "Towards an Assurance Case Practice for Medical Devices", http://www.sei.cmu.edu/reports/09tn018.pdf.

[63] Institute of Information Security, Nagoya University, "CC-Case～コモンクライテリア準拠のアシュアランスケースによるセキュリティ要求分析・保証の統合手法", http://lab.iisec.ac.jp/˜tanaka_lab/images/pdf/kennkyukai/kennkyukai-2013-09.pdf.

[64] OMG, "Dependability Assurance Framework For Safety-Sensitive Consumer Devices (DAF) 1.0", http://www.omg.org/spec/DAF/.

[65] IPA, "コンシューマデバイス機能安全規格が正式に OMG 標準規格へ", SEC journal 41, p. 37, 2015.

Index

This guide book is created by the Working Group on Visualization of Quality in Supply Chain, Software Reliability Enhancement Center (SEC), Technology Headquarters, Information-technology Promotion Agency (IPA).

Editors (titles omitted)

Chief editor	Atsuhiro Goto	Institute of Information Security
Members	Toshio Asanagi	Toshiba Information Systems (Japan) Corporation
	Hiroki Umeda	Japan Aerospace eXploration Agency (JAXA)
	Masayuki Okuhara	Fujitsu Limited
	Mitsunori Kaneda	Tokyo Metropolitan Industrial Technology Research Institute
	Takeshi Kushibiki	Japan Quality Assurance Organization (JQA)
	Nobuhide Kobayashi	Denso Create, Inc.
	Kenji Taguchi	National Institute of Advanced Industrial Science and Technology
	Akihisa Morikawa	WITZ Co., Ltd.
	Hikohiro Yen P Lin	Panasonic Corporation
Secretariat	Motoshi Suzuki	IPA/SEC (Panasonic Corporation)
	Manabu Nakano	IPA/IT Security Center (Panasonic Corporation)
	Keiko Nishio	IPA/SEC
	Shinji Miyahara	IPA/SEC
Support	Ubiteq, Inc.	

July 29, 2016 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 https://www.ipa.go.jp/sec