A Collaborative Design Method for Safety and Security Engineers

Taito Sasaki, Takashi Hamaguchi and Yoshihiro Hashimoto
Nagoya Institute of Technology, Japan
t.sasaki.176@nitech.jp
hamaguchi.takashi@nitech.ac.jp
hashimoto.yoshihiro@nitech.ac.jp

Abstract: The number of cyberattacks has been increasing not only on information systems but also on physical systems. Safety must be considered as an influence of cyberattacks. Vulnerabilities exploited in cyberattacks continue to occur day by day even if systems were developed securely. Security engineers must eliminate vulnerabilities even if the vulnerabilities occur after the developed systems are released. Vulnerabilities must be managed throughout system life cycle. But it takes time to apply its security patch. Safety engineers are required to ensure safety even when vulnerabilities exist. Therefore, collaboration between safety and security (S&S) engineers is necessary to manage corresponding S&S in operation process. S&S should be considered simultaneously in early stage of development process. Collaborative discussion is useful to mitigating risk of reworks. It is an example of reworks by inadequate S&S discussion that the braking system might be redesigned to promote the response in order to compensate for the delay caused by encryption. Therefore, this paper proposes common models effective for the collaboration throughout system life cycle. A management approach using the models is also proposed. Common model is represented by data flow diagram (DFD) because a module under cyberattacks can adversely affect other modules only through data flows. In the proposed method, the three improvements contribute to supporting management throughout system life cycle. Firstly, the models are applied to safety analysis and security analysis. Secondly, vulnerability occurrence is managed at the level of modules. System structures are designed based on modules. Module abnormalities caused by cyberattacks on the vulnerabilities are managed as causes of safety corruption. To indicate critical points for system to be considered, the points from a safety perspective must be identified. Processes and information are traced from the points in DFD. Finally, a module, which performs sets of functions, is outsourced. For each module, it must be considered who will manage vulnerabilities. The proposed method is illustrated using a development of a self-driving wheelchair as an example. In this paper, the collaborative design method for S&S engineers of products and their management based on modules are described to ensure safety even when unexpected vulnerabilities exist.

Keywords: cybersecurity, safety, collaborative design, system life cycle, vulnerability, management

1. Introduction

Cyber threats are regarded as significant issues for not only information systems but also physical systems. Cyberattacks can cause invalidation of safety functions, service outages, deterioration of product quality, or life-threatening incidents. Conventionally, in development phase of physical systems, safety is focused on, but not security. In information systems, the products are developed with care not to include vulnerabilities that can be exploited in cyberattacks.

However, in both developments, new vulnerabilities continue to occur day by day even if systems were developed securely. “The number of vulnerabilities registered in Common Vulnerabilities and Exposures (CVE) exceeds 18,000 a year and continues to increase” (Omo, 2021). Throughout system life cycle, it is necessary to consider that vulnerabilities will occur and continue to be managed. When a vulnerability is detected by security engineers, it should be eliminated. But it takes time to apply its security patch. Safety engineers are required to ensure safety even when vulnerabilities exist. An example of the vulnerability responses is as follows: When a vulnerability is detected in a module, it must be decided whether the operation is stopped or continued without the module. To make such decision, collaboration between safety and security (S&S) engineers is necessary.

If conventional development is applied, security is considered after development based on safety. Security requirements might lead to reworks. For example, encrypting communications causes a risk of delaying brake response. The braking system might be redesigned to improve the risk. To avoid reworks, S&S should be considered simultaneously. In addition, some measures are effective for both S&S. In terms of cost, it is also effective to consider S&S simultaneously.

“In the actual field, few engineers are familiar with both S&S” (IPA,2018). Therefore, collaboration between S&S engineers is required. However, engineers in S&S domains have different perspectives, cultures, and backgrounds. There are hurdles to achieve effective collaboration.

This paper proposes a management approach using common models. The communication using the models is expected to promote collaboration.

In Section 2, a systematic approach for system life cycle safety and security management is proposed. In Section 3, the proposed approach is illustrated using a development example of a self-driving wheelchair.

2. A life cycle management approach for safety and security

In system development, "V-model represents the phase of implementing while disassembling from the whole plan to detailed parts, the phase of proceeding with verification and validation while integrating partial elements into the overall structure" (JSA, 2020). Although V-model usually represents only system development process, some V-models to deal with system life cycle were proposed (Graessler, 2018). A new V-model with deep discussion of safety against cyberattacks is needed. To keep consistent management throughout life cycle, common models which could be utilized in whole process must be designed. In this paper, a method to design such models is proposed. Figure 1 shows the process flow over the lifecycle in order design, implementation, verification, operation, considering security and safety. In implementation process, modules are developed to satisfy specifications by applying secure coding. The first step in verification process is module validation. It verifies not only that the module meets specifications, but also that the supplier is capable of continuing to manage vulnerabilities that may occur in the module in the future. The following steps are verification using integration test and system test. In operation process, maintenance and upgrades are continued in order to ensure safety even when unexpected vulnerabilities exist. In the term of design process, all conditions to succeed the management of implementation, verification and operation must also be designed.

2.1 Overview of design process

System behaviour should be represented by inter-object communication. A module under cyberattacks can adversely affect other modules only through data flows. Hence, data flow diagram (DFD) is suitable as one of the representations of system. The same measure can be effective regardless of whether the failure is caused by a breakdown in safety or security. If such measures are taken, S&S can be considered simultaneously. Some measures can continue service even when malfunctions occur. Others can stop service safely. The discussion about such measures is the discussion about the structure of multiplexing and so on. Although the protection measures for safety or security are also discussed, these measures are not discussed in this paper. For example, in the case of safety, there is the selection of material, strength, thickness, and the margin of the motor and brake. For security, there is the introduction of anti-virus, firewalls, whitelists, and so on.

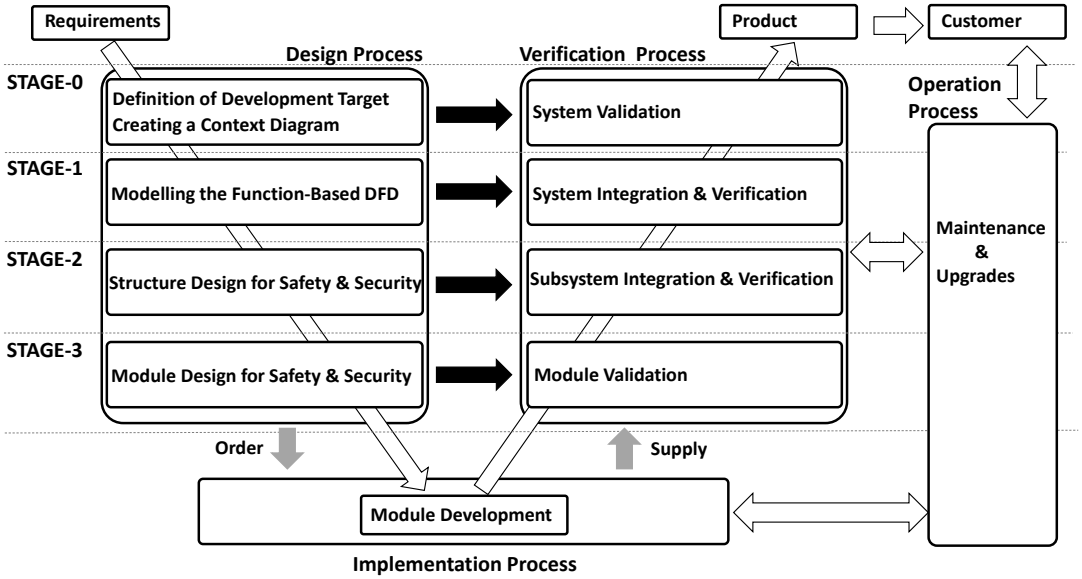

Figure 1: Life cycle process for safety and security

According to the flow shown in Figure 1, the design method of the model structure in the design process is described below.

2.1.1 STAGE-0

In STAGE-0, it is necessary to gather information related to system development. STAGE-0 defines the requirements for system development, such as the scope of the development system, environment, users, and service scenarios. It is important to identify and clarify the scope of development. If the requirements for system development are unclear, the development is delayed, or the quality of the deliverable doesn't meet the customer's expectations. As a result, the risk of the collision may become a reality. To avoid such a situation, it is necessary to identify and clarify the scope of development depending on the situation.

In addition, a context diagram based on definitions to visualize the situation is created. From this development phase, a common model is required for safety engineers and security engineers to be involved in the development and consider each risk. The context diagram is created as a common model at the context level. The context diagram describes the prerequisites of things assumed as a system. Because of a simple model, they can understand the status of development targets and possible external entities. This common model can contribute to lowering the hurdles for communication between development members. Engineers also table descriptions of the context to keep records and reduce cognitive discrepancies. Using this common model and descriptions, the safety engineers and security engineers can reach common ground from the initial phase and reduce the discrepancy in recognition.

The created model is a visual representation model that doesn't require a technical point of view or knowledge. This model does not represent the entire system. Therefore, it is desirable to add what you noticed from each viewpoint of development members to the model as necessary and to clear the entire system.

2.1.2 STAGE-1

In STAGE-1, engineers model the function-based DFD up to the granularity of information needed, to discuss the necessary level of S&S. In STAGE-0, they define the requirements for system development and table descriptions of the model. Based on such information, they organize the functions to be developed necessary to meet customer requirements. Then they evaluate the validity of the deployed functionalities to the ambiguous customers' demands and model the deployed functionalities as a DFD model.

2.1.3 STAGE-2

In STAGE-2, structure discussion such as multiplexing is conducted to realize the required levels of safety and security in each function discussed in STAGE-1. The first step is to consider countermeasures that can be taken even if a function fails. Such measures should be effective regardless of the cause, whether it is a safety failure or a security failure. For multiplexing, both the function and the communication between functions are subject to consideration. With regard to security, not only multiplexing but also diversity is necessary. In the next, safety analysis and security analysis on the designed structure are executed simultaneously.

2.1.4 STAGE-3

In STAGE-3, module construction to be outsourced is focused on. Modules, which perform sets of functions, are designed. Generally, the supplier should manage vulnerabilities in the outsourced module during implementation process. During operation process, unexpected vulnerabilities might occur in the module. If the module was a black box for system developer, that outsource module implementation to supplier, it is difficult for system developer to manage the vulnerabilities. The contracts of outsourcing specify whether the supplier continue to manage vulnerabilities after implementation process. If not continued, the supplier should provide not only outsourced module but also enough information including all design documents to manage unexpected vulnerabilities. If continued, the supplier should provide not only outsourced module but also proof of ability to continue the management. In addition, if system developer considers that the module is critical for safety, the system developer might require the supplier to provide the necessary information to ensure the safety of the module. During operation process, vulnerabilities within all modules, regardless of contract type, must be monitored.

When vulnerabilities are detected, the response to them should be considered in the design process. Regardless of the type of unexpected vulnerabilities, the consideration of the response is simplified by assuming that the module is unavailable while the vulnerabilities exist. Even when some modules are unavailable, operations might be able to continue with the other modules. Or it might be necessary to shut down the entire operation. Thus, the response is designed on the basis of modules.

3. Explanation of the proposed life cycle management approach using an example

Section 3 shows an example of the application of the proposed approach to the development of a self-driving wheelchair for shopping mall service.

3.1 STAGE-0 in design process

STAGE-0 defines the development target and creates a context diagram to identify the scope of the development system.

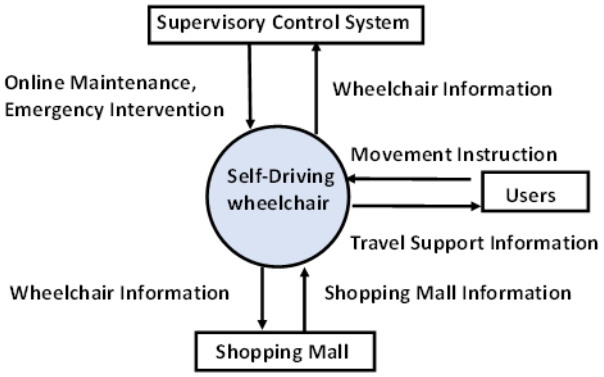

Figure 2: The context diagram of the situation between the self-driving wheelchair and external entities

Table 1: Description of specific elements in Figure2

Element	Description	
Shopping Mall Environment	Database(DB)	System History Log
		Data such as MAP and route
		User's personal data
		Facility usage status
	Facilities, Equipment	Shopping mall structure
		Shopping mall facilities
	Fluid Things	People (adults, children, the elderly)
		Obstacles (carts, trash cans, poles, signboards, dropped objects, etc. that are not on the map)
Users	Users are handicapped or elderly people who can come to shop but have difficulty walking for a long time. Those who already live in wheelchairs are likely to have their own wheelchairs. Therefore, these people can be excluded from consideration.	
Supervisory Control System	People and Systems that execute online maintenance or emergency intervention	

Some information about order side requirements, users, service scenarios, development targets, and shopping mall environments are described.

<Order Side Requirements>

Some ordering side's requirements are as follows.

1. The wheelchair can automatically move to a destination specified by the user.
2. The wheelchair can be used without installing lines on the floor.
3. The wheelchair can automatically return to the parking lot after service.
4. Safety and Security of the wheelchair and its users must be ensured.
5. Maintenance for Safety and Security must be ensured during operation process.

<Wheelchair User>

6. Users are handicapped or elderly people who can come to shop but have difficulty walking for a long time. Those who live in wheelchairs are likely to have their own wheelchairs. Therefore, these people can be excluded from consideration.

<Overview of Services Scenarios>

7. A user who gets on the self-driving wheelchair at the specified location in the shopping mall selects the desired destination in the shopping mall from the map on the tablet terminal. Then, the wheelchair transfers the user to the user's destination. After arriving at the destination, a clerk supports the user's shopping. The user can also manually move around to shop or eat. If the user wants the wheelchair to transfer automatically, the user selects the destination in the shopping mall from the map on the tablet terminal again when you leave the store. When the user finishes using the wheelchair and gets off, the wheelchair will return to its designated location.

<The Shopping Mall Environment>

8. The shopping mall environment can include databases, facilities, equipment, fluid things, and so on. In this example, the control of the self-driving wheelchair is assumed in a normal state, not in an abnormal situation such as a disaster. In addition, for example, the risk of falling on steep slopes can be excluded from consideration, in the shopping mall.

<Development Target>

9. The Product is a self-driving wheelchair. The electric wheelchair body and sensors required for self-driving are regarded as outsourced modules. Although the specifications of test items are designed by the system developer, the design and implementation of the modules are consigned to suppliers. The main target to develop is the self-driving control system.

<Out of Scope>

10. In STAGE-0, it is important to identify scope of the development. In some cases, it might be effective to mention out of scope. In this development, it is exempted from development that the self-driving wheelchair goes up and down the floor by elevator. Since the self-driving wheelchair needs to link with the elevator system for calling or designating a destination, it is given up to install an elevator boarding system.

Figure 2 shows the context diagram created to understand the situation between the self-driving wheelchair and external entities. In terms of safety, risks of collisions with shoppers, fall on stairs, and so on can be discussed. In terms of security, risks such as wheelchairs being tampered with, stolen, etc. can be discussed. In Table 1, the specific elements in Figure 2 are explained.

3.2 STAGE-1 in design process

In STAGE-1 the function-based DFD up to the granularity of information needed is generated. The context diagram is deployed until the main functions of the self-driving wheelchair are identified. By using a method such as quality function deployment (QFD) (Akao, 1997) as a method of developing functions from order side requirements, the functions have been deployed to the following sets of functions. Figure 3 shows the DFD model based on the functions.

11. Interface for specifying the target position
12. Capability to detect the position of the wheelchair itself
13. Capability to plan a movement route to the target position
14. Motion control to move the wheelchair along the specified route
15. Function to correct deviation from the route
16. Capabilities to detect unplanned events or the excessive tilt of the wheelchair and stop or decelerate
17. Function to make an emergency stop by people in the vicinity
18. Map information to determine proximity to walls, stairs, and so on
19. Capabilities to scan for obstacles or falling areas in the vicinity
20. Function to identify the user without receiving personal information

The function of identifying the Users without receiving personal information (j) is in the issue of information security. In this paper, this function is excluded from discussion because safety is focused on.

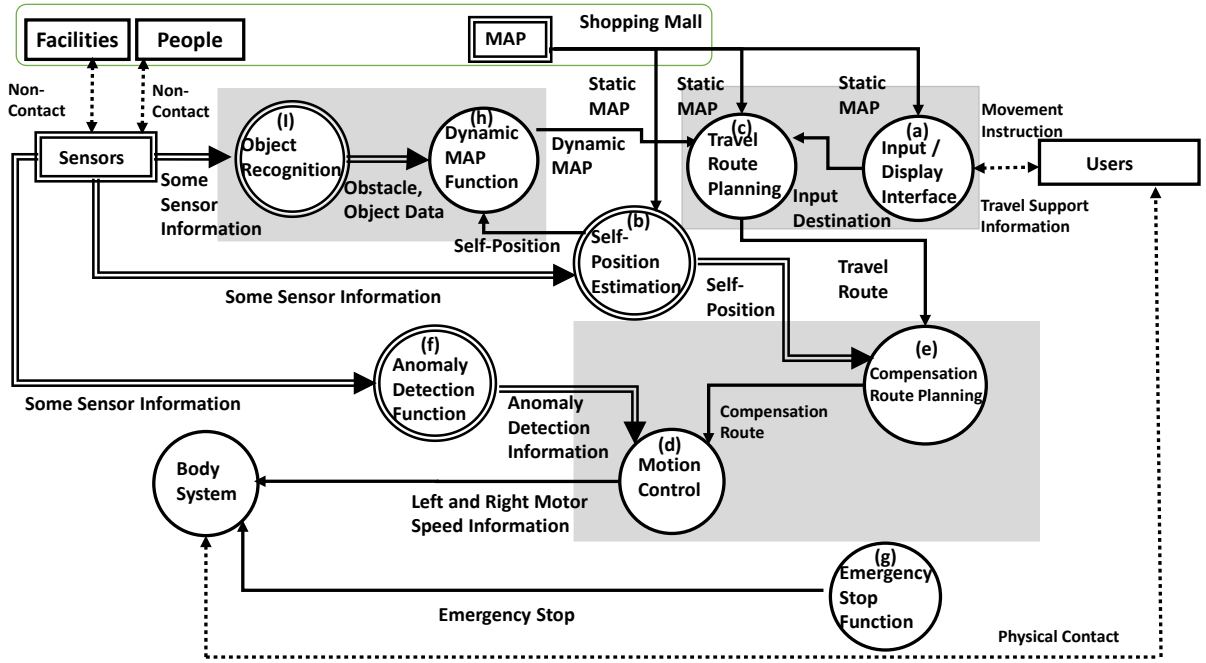

Figure 3: Function-Based DFD & structure with module

3.3 STAGE-2 in design process

In STAGE-2, it is determined how to structure the functions in the model from the viewpoints of S&S domains. This stage focuses on the functions that are important for ensuring safety. Here, the "risk that normal self-driving cannot be performed due to an abnormality in the self-driving control system" is taken as an example. In terms of safety, the causes of failure are erosion, corrosion, environmental stress, malfunction, maloperation, and so on. In terms of security, the causes of failure are malware targeting vulnerabilities, remote operation from the internet, denial of service (DoS) attacks, physical destruction, and so on. Since the system involves human lives, safety is the top priority. From Figure 3, S&S engineers can agree with the idea that the communication of "Left and Right Motor Speed Information" from "Motion Control" (d) to "Body System" of the wheelchair is the critical point that affects the safety of the whole system. A cover might be provided as an anti-breakage (Safety) and anti-disconnection (Security) measure for communication cables. From this example, it can be understood that the same measures can be effective whatever the type of causes of the failure.

Even self-driving systems should incorporate elements that humans can contribute to safety. "Emergency Stop Function" (g) in Figure 3 allows the system to stop and ensure safety in the event of a system malfunction.

From here, the procedure for simultaneously analyzing safety and security is explained according to Figure 3. The reason why the outputs of a function become abnormal is either the existence of abnormality in the inputs, a failure in the function, or a cyberattack. The analysis goes back from the critical point to the input side. Since the critical point is "Left and Right Motor Speed Information", its cause can be traced back to "Motion Control" (d). The causes of abnormal output are breakage or disconnection of the cable and falsification of communication, etc. The next function is "Motion Control" (d). The causes in it are computer module failure and program bugs, etc. in terms of safety, and deletion and falsification of data or program, etc. in terms of security. The next target of analysis is either "Anomaly Detection Information" or "Compensation Route". The self-driving wheelchair cannot move without routes. Therefore, "Compensation Route" is important for "Motion Control" (d). A measure is taken to prevent cyberattacks on this communication by making it a linkage within the program, rather than using communication lines. This measure is expressed with a grey square in Figure 3. There are other measures such as installing a firewall on the communication line or applying encryption to the communication. The next target is "Anomaly Detection Information". Anomaly detection is achieved by using multiple functions such as cameras and radar. In this way, even if one function is lost, anomaly detection can be achieved with other functions. This multiplexing measure is represented by double lines in Figure3. The above discussion will be deployed thereafter. Figure 3 shows the structure determined in the above discussion.

3.4 STAGE-3 in design process

In STAGE-3, each circle and grey square shading is assigned to a module. The suppliers of “Anomaly Detection Function” (f) modules did not accept to pass design documents or sources. And they contracted to continue vulnerability management in operation process. From the supplier of “Emergency Stop Function” (g) module, all design documents and sources were supplied. Because the module of “Motion Control” (d) and "Compensation Route Planning" (e) is important, the system developer implemented it by itself.

3.5 Implementation process

This process is executed by suppliers. Supplier should implement similar V-shaped development.

3.6 Verification process

In verification process, the test items determined in design process are checked. In STAGE-3, the test items for the vulnerability management in operation process are included.

3.7 Operation process

In operation process, all modules should be monitored whether unexpected vulnerabilities occur in them. When it is detected, the system developer informs the customer when the patch will be provided and suggest how to respond until applying the patch. The response based on modules was already designed on STAGE-3 in design process.

4. Conclusions

This paper's topic is S&S management throughout system life cycle. Especially, the response to vulnerability in operation process was focused on. This paper doesn't deal with secure development, such as secure coding, which aims for the product to be secure at the point of release. The purpose of the proposed security management is to ensure safety even when unexpected vulnerabilities exist in operation process. To achieve the purpose, from design process, it is necessary to collaborate between S&S engineers. This paper sought to manage continuously safety throughout system life cycle by presenting a management approach using common models based on DFD. A module under cyberattacks can adversely affect other modules only through data flows. Therefore, DFD is applied. In the proposed method, the three improvements contribute to supporting management throughout the system life cycle. Firstly, systems are represented by DFD. The models are applied to both safety analysis and security analysis. Communication using common models is expected to promote collaboration. Secondly, vulnerabilities are regarded as causes of safety corruption. Safety engineers must consider how abnormalities of the module which contains a vulnerability affect system safety. They must evaluate its risk and respond it. Security engineers must consider detection of vulnerabilities in modules, development of their security patches and their application. Both engineers collaborate to design system structure based on modules. To indicate the points to be considered, critical points from a safety perspective are identified. Processes and information are traced from the points in DFD. Finally, a module, which performs sets of functions, is outsourced. For each module, it must be considered who will manage vulnerabilities throughout system life cycle. If module developers don’t want to continue vulnerability management after release, they are required to provide enough information to manage unexpected vulnerabilities in their module. In this case, the provided information is verified. Product developer should decide whether to manage the modules by itself or to outsource the management. If module developers continue vulnerability management, their management system is verified. In operation process, all modules are monitored whether new vulnerabilities occur in them. When vulnerabilities are detected, to ensure safety, the response will be implemented on a module-by-module basis.

The proposed method with collaboration between safety and security from design process is desired to contribute to the advancement of safety management against cyberattacks throughout system life cycle.

References

Akao, Y1997) “QFD: Past, Present, and Future”, International Symposium on QFD ’97, Linköping

Graessler, I., J. Hentze and T. Bruckmann (2018) “V-models for Interdisciplinary Systems Engineering”, International Design Conference-Design 2018, Design Process, pp747-756

Information-technology Promotion Agency Japan (IPA) (2018) Control System Safety and Security Requirements Study Guide (Basic) https://www.ipa.go.jp/files/000064728.pdf

Japanese Standards Association (JSA) (2020) JIS X 0170:2020 System Life Cycle Processes

Omo, K (2021) Trends and Considerations in the Number of CVEs (2021 Edition) Part1
https://security.sios.com/security/cve-total-info-20211203.html