The future of vehicle cybersecurity

www.pwc.com/jp

Introduction

The 2018 Digital Auto Report by Strategy& illustrates the fact that the digital revolution of vehicles has brought us to the approaching dawn of a new mobility society. The gap is closing between the convenience customers want and the services provided by the increasingly commercialized connected, autonomous, shared, electric (CASE) technologies. The next generation of the mobility society is taking shape. Meanwhile, the changing mobility society is not necessarily shaped by technology alone; the speed of change is in part being decided by the policies and regulations of each nation. One of the factors behind these changes is the increased anxiety over cybersecurity.

As has been said often in recent years, the convenience of cars has improved with their being connected to networks. However, they have at the same time become open to the threat of cyberattack. This has already been identified as an issue by original equipment manufacturers (OEMs) and suppliers, and new cybersecurity measures activities are being implemented, particularly at the vehicle development phase. In addition, major automotive organizations have published policies and guidelines regarding vehicle cybersecurity. The initiatives by the United Nations Economic Commission for Europe (UNECE) World Forum for Harmonization of Vehicle Regulations (WP.29), and the joint work by the International Organization for Standardization (ISO) and SAE International are considered particularly important. An international standard being developed by the latter is ISO/SAE 21434-Road Vehicles, which is the main focus of this report.

WP.29 is a worldwide regulatory forum within the institutional framework of the UNECE. It is deliberating the regulation of cybersecurity measures. ISO/SAE 21434 is an international standard regarding vehicle cybersecurity that is slated to be completed sometime around 2020. It is expected that ISO/SAE 21434 will define standards for the management and implementation of cybersecurity measures covering road vehicles, their systems, components, software and external devices connected to vehicles via networks. Though the standard is voluntary, it will have a considerable impact upon the industry as it will be referred to by WP.29, which is examining drawing up regulations.

It is quite feasible that the regulation and standardization of such cybersecurity measures will make it necessary for businesses to implement additional cybersecurity measures. While cybersecurity measures are essential from the perspective of securing user safety, blindly implementing them could lead to the emergence of disadvantages to users such as rocketing vehicle and mobility service costs and the postponement of releases. It is therefore vital, having first obtained a correct understanding of the cybersecurity measures called for by international standards and regulations, to maximize the effectiveness and efficiency during the course of implementation.

The topic of the report presented here is ISO/SAE 21434, and in it we will review the cybersecurity measures that will be required in the future.

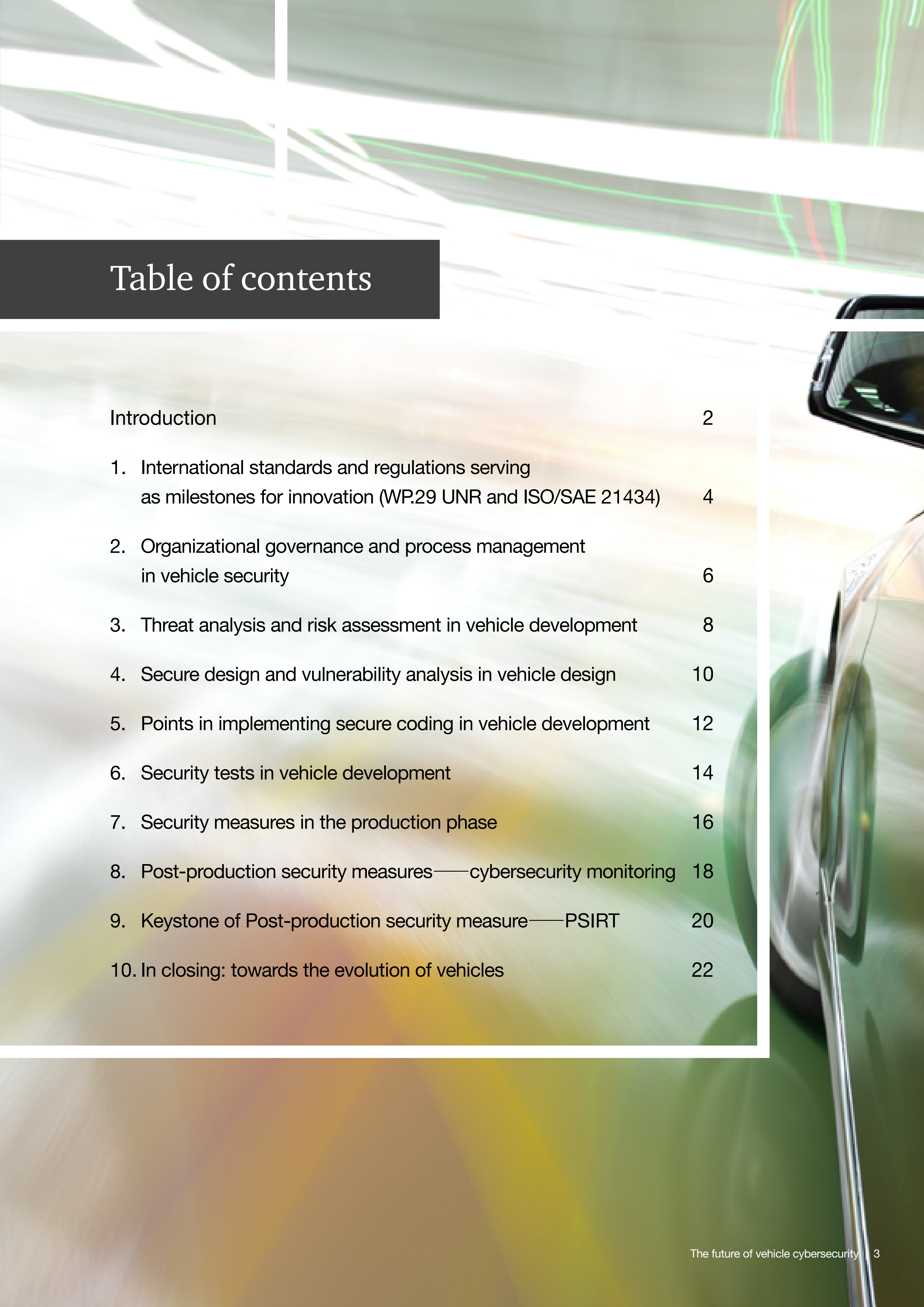


Table of contents

1 International standards and regulations serving as milestones for innovation (WP.29 UNR and ISO/SAE 21434)

In this chapter we will consider WP.29 UN Regulations (UNR) and ISO/SAE 21434, which will become the policies for vehicle security.

WP.29 UNR

WP.29 UNR is a UN Regulation created by the World Forum for Harmonization of Vehicle Regulations (WP.29), a regulatory forum within the institutional framework of the UNECE. It regulates the requirements for cybersecurity in the development, production and post-production of vehicles. There are several WP.29 working parties, at which debate is conducted on each theme. At one of these, the Working Party on Automated/Autonomous and Connected Vehicles (GRVA) is vice-chaired by Japan and one of its meeting bodies, the Task Force on Cyber Security is co-chaired by Japan and the UK. Japan is playing a leading role in international standardization of vehicle cybersecurity.

The GRVA Task Force on Cyber Security is tasked with examining the cybersecurity requirements for vehicles. The Task Force's main item of deliberation, regulations on cybersecurity, requires authentication from the two perspectives of both processes and products. The cybersecurity regulations will serve as an addition from a cybersecurity perspective, which is based on the hitherto vehicle authentication systems of the 1958 Agreement[*1] and the 1998 Agreement[*2].

On the process side, it is planned that the approval authorities will approve OEMs' processes (authentication and auditing of systems and mechanisms) at an initial stage and then again every three years. This means that, unlike the hitherto mentioned vehicle approval systems, not only will the quality of vehicles developed be approved but the quality of the organizational activities of OEMs developing and producing vehicles will also be reviewed. Consequently, OEMs will be required to create processes that involve every division related to the development and production of vehicles. On the product side, a need will arise to demonstrate that the vehicles are developed and produced in accordance with the above-mentioned approved process.

The following is an outline of the security requirements regarding processes and products.

Process requirements

- OEMs shall establish and introduce a Cyber Security Management System (CSMS*) at the development, production and post-production phases.
- Processes shall be applied to approve the identification, evaluation, categorization and treatment of risks regarding vehicles and vehicle management and to ensure the processes are maintained.
- The security of vehicles must be tested.
- Processes shall be used to monitor, detect and manage cyberattacks on vehicles.
- Processes shall be used to identify cyber threats and vulnerabilities, and to deal with newly emerging issues.

Product requirements

- The information required under the regulation must be collected and verified through the full supply chain.
- Appropriate design and test information shall be maintained.
- Appropriate security measures shall be implemented in the design of the vehicle and its systems.
- Methods for cybersecurity support in the post-production phase shall be implemented.

[*1] Agreement concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations

[*2] Agreement on UN Global Technical Regulations

ISO/SAE 21434

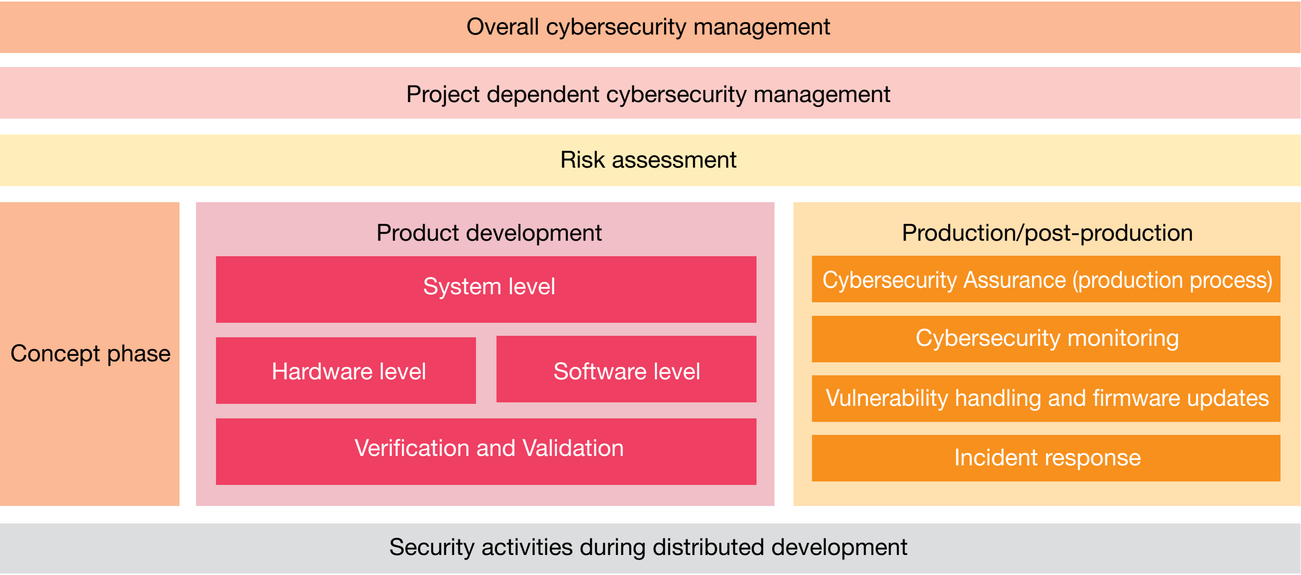
The objective of ISO/SAE 21434 is to define the cybersecurity processes throughout the entire vehicle life cycle. The "entire vehicle life cycle" means all the activities concerning development and operation of the vehicle, which starts with the planning and research of the vehicle, and is followed by its design, implementation and verification and its subsequent production and operation in the field (i.e. when the vehicle is on the roads) and eventual decommissioning. It will become necessary for cybersecurity initiatives to be taken in the course of these activities. It is expected that through this process cyberattacks and the damage arising from cyberattacks can be reduced.

ISO/SAE 21434 is largely composed of the following seven elements (See Diagram 1).

1. Overall security management: formulates policy or strategy specializing in or emphasizing cybersecurity, preparation of systems and processes, and activities to foster a culture of security and awareness; defines activities such as the creation and maintenance of quality management systems, and the evaluation of tools used from a security perspective.
2. Project dependent cybersecurity management: defines cybersecurity organization and responsibilities in projects, cybersecurity plans, vulnerability handling and management, and efficacy evaluation of measures implemented
3. Risk assessment: defines activities for cybersecurity risk analysis, rating and treatment based on general risk management methods
4. Concept phase: defines processes and activities implemented during the concept phase of vehicle development
5. Product development phase: defines additional cybersecurity processes and activities concerning the existing development processes and activities during vehicle development
6. Production/post-production phase: defines cybersecurity effects that should be implemented during post-product development production and operation
7. Security activities during distributed development: defines interaction on customer/supplier relationships and responsibilities across the entire supply chain

In the following chapters we will cite case studies requiring attention upon implementation from among the above cybersecurity activities and make some suggestions about how they should be managed.

Diagram 1: The seven components of ISO/SAE 21434


Overall cybersecurity management
Project dependent cybersecurity management
Risk assessment
Concept phase
Product development
System level
Hardware level
Software level
Verification and Validation
Production/post-production
Cybersecurity Assurance (production process)
Cybersecurity monitoring
Vulnerability handling and firmware updates
Incident response
Security activities during distributed development

Source: Created by PwC based on ISO/SAE DIS 21434 (as of February 2020)

2 Organizational governance and process management in vehicle security

The purpose of vehicle cybersecurity activities is to manage (minimalize) cybersecurity risk to vehicles. This requires the implementation of appropriate security measures throughout all the organizations involved during the life cycle of a vehicle. In order to execute these, systems that can manage security risk are created by defining "organizations" and "processes" with an awareness of security measures. The activities to create organizations and processes to implement these sorts of security measures is called "cybersecurity management."

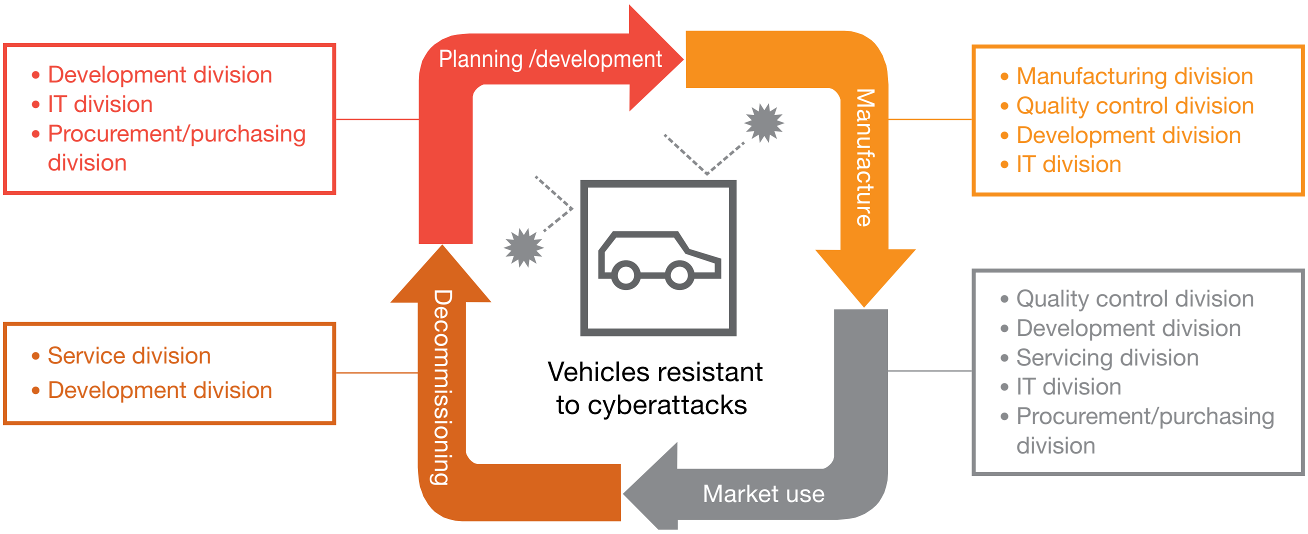
Organizational governance

We will start by explaining the management of "organizations." In order to implement the requisite and adequate cybersecurity activities as an organization throughout the entire life cycle, there is a need for the organization that has general control over all cybersecurity activities to put governance into effect (see Diagram 2). The bottom-up security measures which are based on the on-site staff efforts may be effective on a sporadic basis but tend to be inefficient from a cross-organizational perspective. Therefore, it is essential that cybersecurity activities are regarded as a part of corporate management, and that governance is promoted.

It is necessary that the organizational policies, objectives, and strategies are defined in organizational governance. Similarly, in cybersecurity the stipulation of cybersecurity policies, objectives and strategies is fundamental. In order to stipulate appropriate objectives and strategies there is a requirement to accurately understand the cybersecurity environment in which vehicles are placed. In particular, the cybersecurity environments of vehicles and their components has dramatically changed in recent years, and it is therefore vital that the latest means of attack and trends in security measures are understood.

There is one point to note -- the utilization of security technologies for the IT and Web systems at the front of the security field. In the field of products including the vehicles driven by the end-users, since providing responses post-production is not easy, an emphasis is placed on creating product quality prior to production. On the other hand, revising IT/Web systems after their launch is a comparatively undemanding task. It is due to this disparity in the initiatives and mechanisms involving product quality that the vehicle industry is careful about applying IT/Web technologies. While this is a correct judgment from the vehicle development perspective, it does raise the risk that the industry could be left behind by evolving IT. The reason why vehicle security measures have become necessary in the first place is because vehicles are evolving due to the latest IT, and because the changed environment now necessitates the appropriate use of the very latest cybertechnologies. It is likely that, since the use of the latest security technologies involves difficult decisions, there will be a need for posts such as Chief Security Technology Officers (CSTO) in order to clarify where the

Diagram 2: Organizational management for cybersecurity activities across the entire life cycle



responsibility for use of security technology lies within organizations.

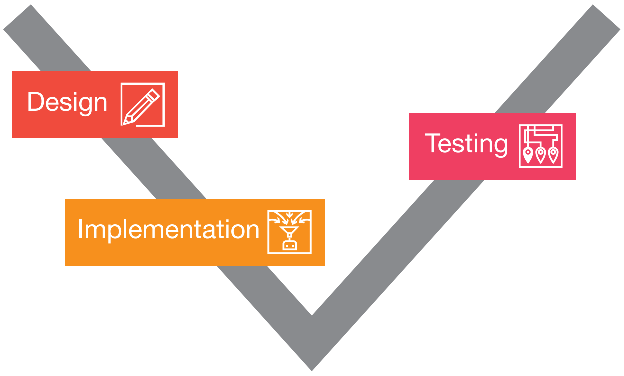
After clarifying objectives, strategies and technical responsibility, it becomes necessary to prepare to execute strategies. Securing budgets and personnel and preparing a system to launch cybersecurity activities are all of particular importance. At the same time, there is a need for milestones regarding cybersecurity within the organization such as regulations and guidelines. This is the other element of cybersecurity management, namely "processes."

Active responses to cyberattacks

The development of vehicles process can be broadly split into two elements from the vehicle development perspective. One is the product development phase process (including the concept phase), and the other is the production, operation and maintenance phase process.

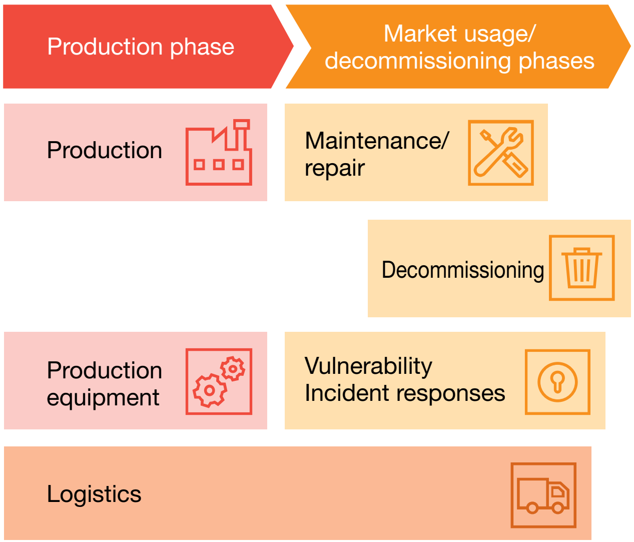
During the product development phase the security measures requirements for planning/design/implementation and verification are defined. As is the case with organizational management, having paid due consideration to the features of vehicles and their societal/utilization environments, the latent cybersecurity threats in the development of a vehicle are identified, and the starting point is the stipulation of the developed products' security goals and objectives. Once the security goals across the entire product development phases have been stipulated, the products are steadily developed in line with the security goals stipulated for the design and implementation processes. The products will be verified in the testing phase to confirm whether or not the security goals have been achieved (see Diagram 3). OEMs and suppliers are traditionally very strong in the product development phase and the same process is used here.

Diagram 3: Security activities during the product development phase



Regarding production, operation and maintenance, activities are defined in order to maintain a secure state for the development of vehicles (see Diagram 4). In the production process there is a need for mechanisms to maintain the security quality envisaged at the time of the development of every vehicle. It should be noted that in recent years there has been progress in measures such as building-in encryption keys during the production phase as security measures, and attention must be paid to the demands for more secure environments. During the operation and maintenance processes there is a need for monitoring activities to check whether or not vehicles are or have been under cyberattack, whether any damage has been incurred, and whether any faults (vulnerabilities) that make vehicles more susceptible to damage have been discovered. There is also a need for a swift response once a problem has been detected. In the past, vehicles have required incident responses arising from breakdowns and decrepitude. However, due to the fact that cyberattack response is a field in which OEMs and suppliers have hitherto not taken measures, these activities are particularly important for effective security.

Diagram 4: Security activities during the production, operation and maintenance phases



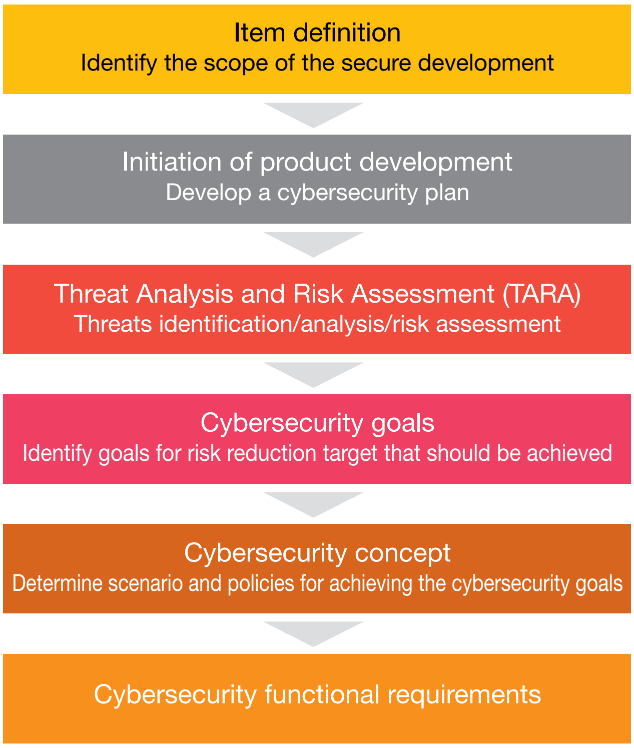
3 Threat analysis and risk assessment in vehicle development

As mentioned above, the basic approach in securing cybersecurity consists of risk management (minimization) initiatives. However, since reducing all risks to an absolute zero is not a practical proposition, it is essential that the limited security measure resources are appropriately allotted and that through each product life cycle activity risk is reduced to an acceptable level. This necessitates, having first comprehensively ascertained risks, that treatment levels proportionate to the severity of risks are stipulated and measures taken according to the priority. In this chapter we will make some observations about "Threat Analysis and Risk Assessment" (TARA) in the concept phase, the phase that is the starting point for risk management activities throughout the entire product life cycle.

Outline of security activities during the concept phase

Overview of the cybersecurity activities during the concept phase of vehicle development is as shown in Diagram 5.

Diagram 5: Security activities during the concept phase



Item definition
Identify the scope of the secure development

Initiation of product development
Develop a cybersecurity plan

Threat Analysis and Risk Assessment (TARA)
Threats identification/analysis/risk assessment

Cybersecurity goals
Identify goals for risk reduction target that should be achieved

Cybersecurity concept
Determine scenario and policies for achieving the cybersecurity goals

Cybersecurity functional requirements

With regards to the specific content of activities, many hints can be taken from current development business pursuant to the ISO26262 standard[*1] "Road vehicles - Functional Safety," but an initiative especially unique to cybersecurity is TARA.

Threat Analysis and Risk Assessment (TARA)

TARA refers to the three processes of "identifying assets," "identifying threats," and "risk assessments," implemented during the concept phase as a series of activities for risk management.

Identifying assets

First of all, a system structure is organized according to the development target use case and information that can be referred to, and information assets and functional assets to be protected are enumerated.

During the concept phase, before the examination of the design, it is not uncommon to encounter cases where assets and where they are to be stored remains undecided. For example, if a vehicle will be equipped with electronic payment functions, some sort of assumption has to be made and analysis carried out regarding undetermined elements such as whether the credit card information necessary for payments is stored in the vehicle or in a back-end server, and whether that information is highly confidential card member data or tokenized data.

These sorts of points need to be clearly specified in the course of design, and are required to be managed during the remaining phases. Furthermore, in order to narrow down the prerequisites, adequately incorporating technological and systematic restrictions in the prior process of "item definition" is effective.

As can be seen, the activities during the concept phase require technology to promote analyses based on limited prerequisites and information.

[*1] ISO 26262: Functional safety standards for road vehicles. As guidelines for safe design in vehicle development, OEMs and the suppliers of on-board devices and so on are required to conform to these standards.

Identifying threats

All the latent security threats are specified from among each identified asset. Furthermore, where necessary the conditions under which these threats may arise are analyzed and clarified. In security that takes into consideration malicious third parties, there is a need for specialist knowledge regarding the approaches and methods employed by actual attackers (hackers). As structural approaches for securing homogeneity in this work involving highly individual skills, and for ensuring a certain level of coverage regarding threat identification, there are threat analysis methods proposed by various bodies. However, as there is not at present a single integrated method, each organization needs to select the method best suited to its characteristics and the circumstances of its development process, or use several methods in combination. For example, the STRIDE*2 threat classification, which does not depend on detailed design, can be used to identify threats initially. Then, in order to make a more detailed analysis of conditions in which threats may emerge, "attack trees" (described later) can be used to show specific methods of attacks and their feasibility.

Risk assessments

Risk level is calculated from a set of common evaluation criteria, and the degree of priority of measures (risk reduction) is decided upon, according to these calculations for each type of risk. The usual IT security indicators such as severity and exposure in the event that a risk actually occurs can be used as evaluation criteria, however the security of vehicles also necessitates the consideration of any impacts to safety. As shown in Diagram 6, while configuring four risk levels according to a severity and exposure matrix, this school of thought requires the highest level, level 4, be assigned to any risks which threaten safety, regardless of exposure level. In contrast, from a perspective of IT security alone even serious risks can be easily avoided or stemmed by a physically manipulated functional safety mechanism, and there are cases in which the actual severity is not particularly high. In such cases, it becomes necessary to consider the perspective of controllability from functional safety.

In addition, the ISO/SAE 21434 currently under review, is examining the introduction of Cybersecurity Assurance Levels (CAL) as a management unit for the entirety of the product life cycle. CAL is a classification equivalent to the Automotive Safety Integrity Levels (ASIL) in the ISO 26262 functional safety standards that stipulates several levels of security targets to be met. Security measures to be applied upon design, implementation and/or operation are also specified and are required in order to meet the targets corresponding to CAL. Organization are required to conduct management in order to eventually reach all the targets stipulated by CAL throughout each process of the product life cycle.

Diagram 6: Sample four-level risk calculation table

		Exposure		
		Low	Medium	High
Severity	Very low	1	1	2
	Low	1	2	3
	Medium	2	3	4
	High	3	4	4
	Critical (impact on safety)	4	4	4

*2 STRIDE: A classification method for identifying threats. Threats are identified through the use of the six classifications of Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege.

References

"Status of Work in Process on ISO/SAE 21434 Automotive Cybersecurity Standard" [PDF 980KB]

SAE International. "SAE J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" 2016

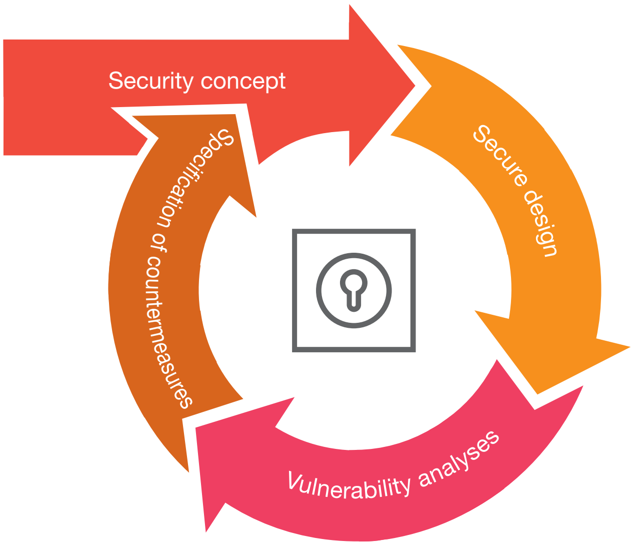
4 Secure design and vulnerability analysis in vehicle design

The results of TARA are used for risk analysis and management activities during the product development phase. During the concept phase, there are cases in which it is not possible to specify the conditions for the emergence of unspecified risks in design and implementation or the requisite measures. As these types of risk may be identified as the development process proceeds, there is a need for repeated risks analyses to be conducted at each system, hardware and software development phase, and for risk management to be implemented. In this chapter we will focus on the product development phase and make observations about activities during the system and component design phases. In this report, risk analysis related to "vulnerability" as a specific threat exposure based on design information is referred to as a "vulnerability analyses" in order to distinguish them from the TARA covered in the previous chapter.

Outline of security activities during the design phase

During the concept phase, cybersecurity goals are configured by identifying threats and by risk assessments, and a cybersecurity concept is stipulated that serves as a policy to be achieved. In the product development phase, an overall design is created first as a system adhering to the cybersecurity concept. Furthermore, in order to improve the security quality of design, vulnerability analyses are carried out. In the event that vulnerabilities which could become significant threats are discovered, necessary countermeasures are specified, and improvements made to the design (see Diagram 7).

Diagram 7: Security activities during the design phase



Secure design

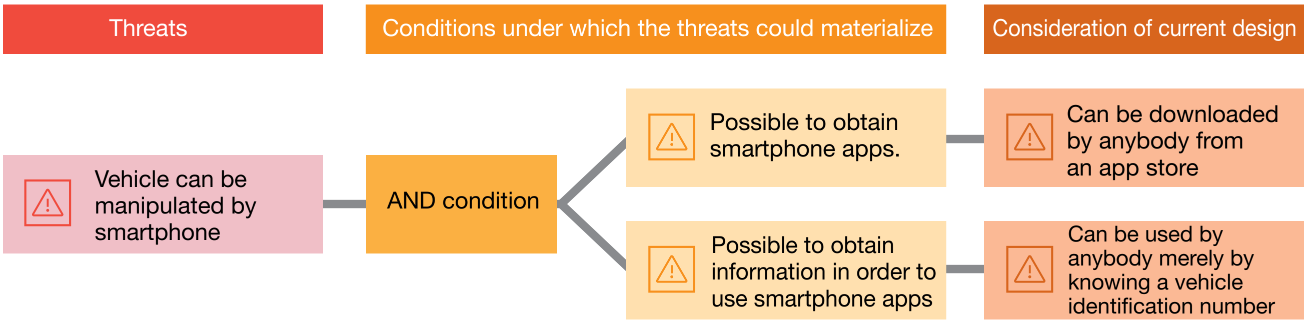
In the first stage, a design of the entire system is mapped out, based on the security concept. Security quality during the design phase is vital as it forms the foundations for security quality through the whole scope of product development. For example, base elements of systems such as the main hardware and OS to be used are often decided upon at early phases such as the system design phase. In the event that changes have to be made due to the discovery of vulnerabilities in the parts at the core of OS and other systems at subsequent phases such as software design, the design changes inevitably become widespread. Additionally, if vulnerabilities are identified at even later processes such as implementation and testing, this often necessitates going back to previous phases and "reworking." Vulnerabilities unintentionally incorporated during the design phase can have considerable impacts in terms of overall production costs and time. Improving security quality during the design phase helps to reduce the discovery of vulnerabilities and leads to efficient development with a minimum of refactoring. In order to promote this sort of efficient development, vulnerability analyses regarding design are conducted, and security quality is improved by enforcing the cycle shown in Diagram 7 of reflecting measures in design.

Vulnerability analysis

Vulnerability analysis is an activity which is performed to check whether there are any vulnerabilities that it would be possible for an attacker to abuse. These analyses use methods such as attack trees (see Diagram 8).

Initially, a consideration is made of the conditions required for the identified threats to materialize. Then, by examining whether there is any possibility of attacks being executed under the current design, the presence of vulnerabilities is appraised. The analysis of connected services such as smartphones and servers require not only analyses for vehicles as shown in Diagram 8, but also analyses that include related systems.

Diagram 8: Example of vulnerability analysis using attack trees


Threats
Conditions under which the threats could materialize
Consideration of current design
Vehicle can be manipulated by smartphone
AND condition
Possible to obtain smartphone apps.
Possible to obtain information in order to use smartphone apps
Can be downloaded by anybody from an app store
Can be used by anybody merely by knowing a vehicle identification number

Specification of corresponding measures and reflection to the design

In the event that vulnerability analysis uncovers vulnerabilities in a product, the results of the risk assessment implemented at the concept phase should be cross-checked and a decision made on whether the risk of the vulnerabilities is unacceptable, and the corresponding measures examined. In addition to altering designs so that attacks cannot be mounted, corresponding methods also include an approach in which systems can be monitored, and functions added that enable detection, response and recovery. It is possible to adapt this approach against low-emergency threats that will not immediately lead to a dangerous state of affairs even if an attack takes place. Corresponding measures are thereby decided upon from among several choices based on comprehensive appraisals of risk, development costs and schedule.

This cycle of vulnerability analyses, examination of corresponding measures and reflection in design is constantly repeated until the vulnerability dissipates or is reduced to an acceptable level. In doing so, there is also a need to consider the emergence of new cases of vulnerability as a result of changes in design. Furthermore, it is not only when designing an overall system but also when making more specific designs such as hardware and software design that implementing these activities assures security quality.

Vulnerabilities that occur at the design phase and at the implementation phase

It is essential that attention is paid to the fact that secure design alone cannot handle every single vulnerability. Diagram 9 illustrates some of the vulnerabilities that can arise at the design phase and the implementation phase.

Diagram 9: Examples of vulnerabilities arising at the design phase and implementation phase

Vulnerabilities arising at the design phase	Vulnerabilities arising at the implementation phase
■ Authentication function defects ■ Use of third party software with vulnerabilities ■ Keeping important data in storage with low tamper resistance*1	■ Buffer overflow*2 ■ SQL Injection*3 ■ Directory traversal*4

Vulnerabilities such as buffer overflow and SQL injections shown in Diagram 9 that are the result of coding at the implementation phase cannot be found during the design phase. Vulnerabilities that cannot be detected at the design phase require measures at the implementation phase.

*1 Tamper resistance: The degree of endurance against attempts by outside parties to steal important information.

*2 Buffer overflow: A malfunction caused by the transmission of amounts of data that are so large they overwrite the memory zones of a program.

*3 SQL Injection: The use of security defects in which hackers execute their own SQL commands (commands to the database) in order to maliciously manipulate the database.

*4 Directory traversal: A method in which by traversing to directories, directories and files to which access would ordinarily be denied are maliciously accessed.

5 Points in implementing secure coding in vehicle development

Here we will make some observations about the secure coding that should be conducted in the software implementation phase in line with: the threat analyses and risk assessments in the concept phase; the secure design in the development phase; and the specifications drawn up according to the results of vulnerability analyses and measure implementation activities.

Secure coding is the writing of software programs that are robust and able to withstand cyberattack. Vulnerabilities that occur at the design phase and at the implementation phase were covered towards the end of Chapter 4, and secure coding is a measure aimed at vulnerabilities that arise during the implementation phase.

Among the software levels included in the product development phase that is one of the seven elements of ISO/SAE 21434 illustrated in Diagram 1 of Chapter 1, this activity is the most elaborate.

The importance of secure coding

The reason that secure coding is so important is because even if measures are taken against vulnerabilities arising at the design phase, the occurrence of vulnerabilities at the implementation phase due to secure coding errors can lead to critical damage. For example, it is possible that typical examples of vulnerabilities that occur during the implementation phase such as buffer overflow and SQL injection will lead to the unintended execution of code by third parties.

Moreover, in terms of overall software vulnerabilities there are more reports of vulnerabilities occurring at the implementation phase than at the design phase, and secure coding is therefore vital from a perspective of the "quantity" of vulnerabilities.

Secure coding practices

Diagram 10 illustrates the secure coding practices. Before proceeding with the coding tasks, it is essential to formulate an overall plan that corresponds to the characteristics of the project (including the information the product will handle, priority of functions, costs and delivery time).

Diagram 10: Secure coding practices

Task	Outline
Formulation of overall secure coding plan	An overall secure coding plan is formulated. Examinations are made of methods to check robustness of source code level programs (such as the use of static code analysis tools and peer reviews[*1]).
Secure coding training	Personnel learn about the overview of secure coding, and problems that occur in the event of violations.
Formulation of coding rules	Based on coding standards generally used in the car industry such as CERT-C/C++[*2] and MISRA-C/C++[*3] additional in-house rules are formulated where necessary.
Formulation of plan for using static analysis tools *When using static analysis tools	Static analysis tools to check the robustness of source code level programs are selected, and a plan for the implementation and responses to static analyses is formulated.
Coding	Coding is carried out. By using the warning messages of developmental tools, the robustness of programs can be assured to a certain extent.
Checking of robustness of the program at source code level	Tools are used for static analyses and source code reviews, and the robustness of the programs at source code level is checked. If problems are detected at this stage source code revision and checking is repeated until satisfactory.

[*1] Peer reviews: a quality assurance method for examining deliverables and making improvements through the views of people in the same (or similar) positions and occupations.

[*2] CERT-C/C++: coding guidelines for the creation of secure software. The guidelines stipulate around 300 rules.

[*3] MISRA-C/C++: C/C++ programming language coding guidelines created specifically for the purpose of functional safety in vehicles. Rules regarding security were also published in the year 2016.

Issues and troubleshooting during secure coding

Most organizations use some sort of static analysis tool to check the robustness of the source code of their applications. However two major issues can occur at this stage: one is that so many problems are identified that full responses cannot be made, and the other is that judging whether or not misdetections have been made is an arduous task.

In order to solve these problems, there are many instances in general software development in which responses are made according to the degree of severity (critical/high and moderate/low) shown by static analysis tools. For example, with regards to critical/high issues it is possible for risk to be tolerated where possible after conducting revisions or risk analyses, while there are also times when a policy of not appraising misdetections is pursued in moderate/low cases.

On the other hand, in the case of the car industry, in the event that problems detected by static analysis tools are not corrected, even problems that are judged as being low in severity by static analysis tools could lead to life-threatening damages. Due to this, it is difficult to automate responses according to the degree of severity shown by static analysis tools.

So, what sort of solutions are available in the development of software for the vehicle industry?

The solutions that PwC suggests to our clients are to “deal with all of the problems detected by tools,” and in order to do so, to “think about measures for dealing with all problems.” When we say “deal with,” we specifically mean “appraise misdetections” and “make revisions.”

The points here are, in the first place to “avoid the creation of weak code as much as possible” and to “systematically deal with the problems detected by analytical tools.” The following can be cited as specific measures for doing so:

- Implement training in secure coding
- Use static analysis tools from the early stage of the development phase
- Incorporate CI tools[*4] with static analysis tools, and automate the use of static analysis tools

[*4] Continuous Integration (CI): tools for the continuous implementation of source code building (processing of the creation of executable files and distribution packages), and testing. By combining static analysis tools with tools that support automatic building functions like Jenkins and others, it is possible to implement static analyses in time with automatic building.

6 Security tests in vehicle development

In this chapter we will introduce the security tests that are a measure taken at the testing phase for implemented vehicles and onboard products.

Security test categories by objective

Security tests broadly include the twin concepts of vulnerability tests and penetration tests.

Vulnerability tests

As discussed in earlier chapters, initiatives relating to security are conducted at the conceptual, development and implementation phases. At each phase threat analyses are carried out, and based upon the results of the secure design and secure coding are implemented. The tests to check whether or not the measures aimed at threats foreseen in the upstream processes are being appropriately implemented are vulnerability tests. Due to these characteristics vulnerability tests enable the creation of checklists as the envisaged threats and measures are clear in advance, and explanations are also possible to a certain extent regarding their coverage.

Penetration tests

Penetration tests, on the other hand, stipulate targets to be met regarding attacks, and conduct simulated cyberattacks (for evaluation purposes) in order to meet those targets.

Penetration tests do not demand coverage. Rather, their objectives are to see if arbitrary code execution in a specific electronic control unit (ECU) is possible, and if they are not possible, how close to the target the attack went, and what were the reasons and factors behind the failure to reach the target. Because penetration tests are conducted without any consideration paid to the various upstream process initiatives, much is expected of their ability to unveil unforeseen threats in the upstream processes, or in other words, areas that have been overlooked in the upstream process. To put it another way, each test item implemented during a penetration test could be included in a vulnerability test.

This means that these tests exactly recreate the conditions in which the world's hackers use every conceivable means to obtain their goals quite regardless of the security measures taken by the manufacturers and conduct evaluations from the hackers' perspective.

As Diagram 11 shows, there are differences in the thinking behind vulnerability tests and penetration tests, and one does not encompass the other. Since cost considerations make the implementation of every security test for every product an unrealistic prospect, it is important to select test subjects according to the particular product model and functional differences from other similar models.

Diagram 11: Outline of vulnerability tests and penetration tests

	Objective	Merits	Demerits
Vulnerability tests	To check the state of adequacy of envisaged threats in upstream processes.	Coverage can be explained to some extent.	Cannot evaluate unforeseen threats in upstream processes or state of measures that have not been examined.
Penetration tests	Set a target, see if it can be attained, and clarify the reasons and factors if it is not attained.	The tests can evaluate threats in upstream processes that have not yet been envisaged. Actual examination results regarding upstream processes can be evaluated.	Difficult to explain coverage. Some of the test items may duplicate those of vulnerability tests.

Security testing perspectives

Both vulnerability tests and penetration tests can be considered as means to test subjects which can be applied to both hardware (HW) and software (SW) testing.

Hardware Security tests

There are several levels for testing hardware (HW), and one that can be considered is a test on the standard external interfaces provided by a product. For example, network connection interfaces such as Ethernet ports (LAN ports), WiFi and Bluetooth, external device interfaces such as USB ports, media inputs such as CDs/DVDs and the buttons installed on hardware housing are all expected candidates for testing. Although these sorts of interfaces can all be used in a standard manner by users according to the vehicle manual and therefore easier to test, there is a possibility that meaningless tests will be carried out if their internal workings are not understood. The testing of standard interfaces can in fact be one of the most difficult areas.

Further testing can be carried out by dismantling housing and the investigation and analysis of internal printed circuit boards. For example, the various types of chips, the details of silk printing and whether it is available or not, the presence or otherwise of debug ports, and investigation and analysis of signs of pin use prior to production can all be suitable targets for testing.

Conducting these kinds of investigations and analyses is beneficial in maintaining product specifications, and while the discovery and detection of debug ports is itself both a large risk and simultaneously enables developers to access internal information, they can be beneficial in the implementation of continuous testing. Moreover, when, as a result of such analyses, chips which store firmware with telecommunications functions are identified, it would be possible to conduct tests to analyze whether the firmware can be extracted from the chips and whether or not the firmware can be analyzed.

Software security tests

As with HW, there are a number of levels of tests for software (SW), the most fundamental of which can be to manipulate the user interface (UI) provided to users and run checks on whether security functions can be bypassed or commands that compromise security executed. In addition, if an interface connecting to a network is supplied, possible tests include checking to see if unnecessary services are being activated, whether or not there are any known vulnerabilities in the software used, and conducting a virtual attack on them to see if the attacks are feasible.

In the case of these sorts of tests, they can become haphazard affairs if they are conducted by external parties without a grasp of internal specifications and it may be difficult to implement efficient tests. Hence methods are envisaged that include analyzing the firmware extracted in HW tests and the implementation of SW tests in which the internal specifications are made clear beforehand. Diagram 12 shows a compilation of examples of the content of HW and SW tests.

Diagram 12: Examples of HW and SW test content

Examples of HW test content	Examples of SW test content
• External manipulation of interface, irregular input • Dismantling of housing, analysis of print substrate information (chips, usage, debug ports) • Removal of chips, extraction of firmware	• Manipulation of user interface (UI) • Scans via network, vulnerability tests • Firmware analysis • Implementation of cyberattacks on vulnerabilities (ethical hacking)

Security tests in the overall secure development life cycle

The question of whether all these sorts of tests should be conducted through vulnerability tests or through penetration tests depends upon how far-reaching and of what nature the threats envisaged to upstream processes are, the extent of measures and how they have been incorporated. Put another way, we could say that the tests conducted to check the adequacy of measures against threats envisaged in upstream processes are vulnerability tests; the tests conducted to check the adequacy and appropriateness of envisaged scenarios themselves are penetration tests.

It is imperative that these sorts of security tests are formulated in response to the initiatives across the entire development process, and not just to examine implementation policy and content during the testing phase alone.

7 Security measures in the production phase

Thus far we have made observations with a focus on security activities at the design, implementation, testing and product development phases. In this chapter we will shift our focus from the security of the product itself, to the security activities that are necessary in the production phase; the essential phase for the completion of the product.

The necessity for security activities in the production phase

Hitherto, although production plants have used their own network and control-related system facilities, they have still been susceptible to malware. In more recent years, as the IoT including smart factories has progressed, a wide range of devices are connected to production plant networks. Furthermore, an increasing number of generic OS and applications are being used in systems themselves. It could be said that changes in the environment such as these have heightened the risks of becoming a target of malware.

Additionally, as vehicles have become connected to networks, the use of encryption technologies such as telecom encryption and message authentication has increased. One impact of this is that there has also been an increase in electronic control units (ECU) that require the internal storage of the encryption keys that play a vital role in encryption technology. These encryption keys have to be stringently managed at production plants, and mechanisms to assure that they have not been leaked or manipulated is required.

Furthermore, the Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA, is expected to become law in the future and is as important as the ISO/SAE 21434. The recommendation contains requirements for the implementation of CSMS[*1] throughout the entire development life cycle including the production phase. It is therefore expected that in the future, security activities at production plants will become mandatory under both law and international standards.

It is thus that the need for security activities during the production phase is becoming ever more heightened from the various perspectives of the progress of IoT at production plants, the evolution of vehicles and law and international standards.

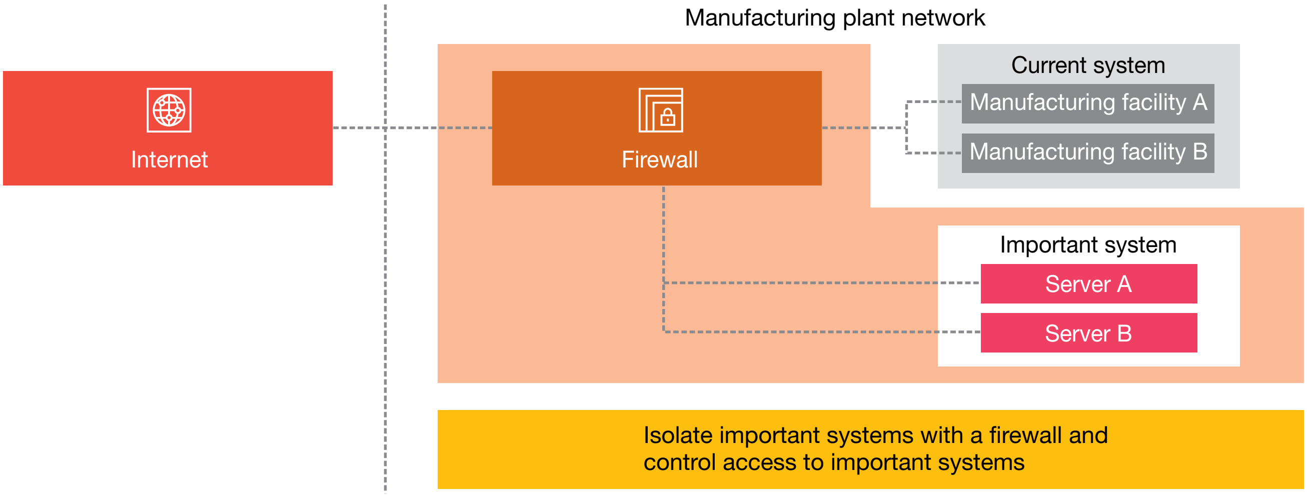
What security measures are required in the facilities at production plants?

Until recently very few production facilities at plants were connected to external networks, and it is thought that there are instances in which security measures have not been adequately implemented. If these sorts of inadequately equipped facilities become connected to external networks the production facilities with weak security will become targets for attacks. And since their entire network will be exposed to security risks it is essential that security measures are put into place for each production facility and network.

However, bringing up all facilities to the same level of security involves a vast amount of work and can be very expensive. Effective security management can be achieved by separating facilities from the networks, controlling access between networks by using devices such as firewall or the like, and implementing the security measures required by each individual facility (see Diagram 13).

[*1] Cyber Security Management System (CSMS): a management system for controlling security aimed at industrial automation and control systems.

Diagram 13: Examples of important access controls for systems



Encryption key control systems requiring more robust measures

Telecommunications encryption and message authentication use data called "encryption keys" (see Diagram 14). If attackers are able to gain these encryption keys they will be able to decipher encrypted transmissions and impersonate vehicles. It is therefore vital to stringently manage them through safe storage in production facilities and in vehicles themselves.

Since it is envisaged that each type of vehicle and each vehicle itself will use a unique encryption code, there is a need for a management system that links and manages encryption codes with each vehicle and device and writes encryption keys inside devices. As mentioned above, since if an encryption key is leaked it can have a tremendous impact on vehicles, the system handling the encryption keys must secure robust security of a higher level than ordinary production facilities.

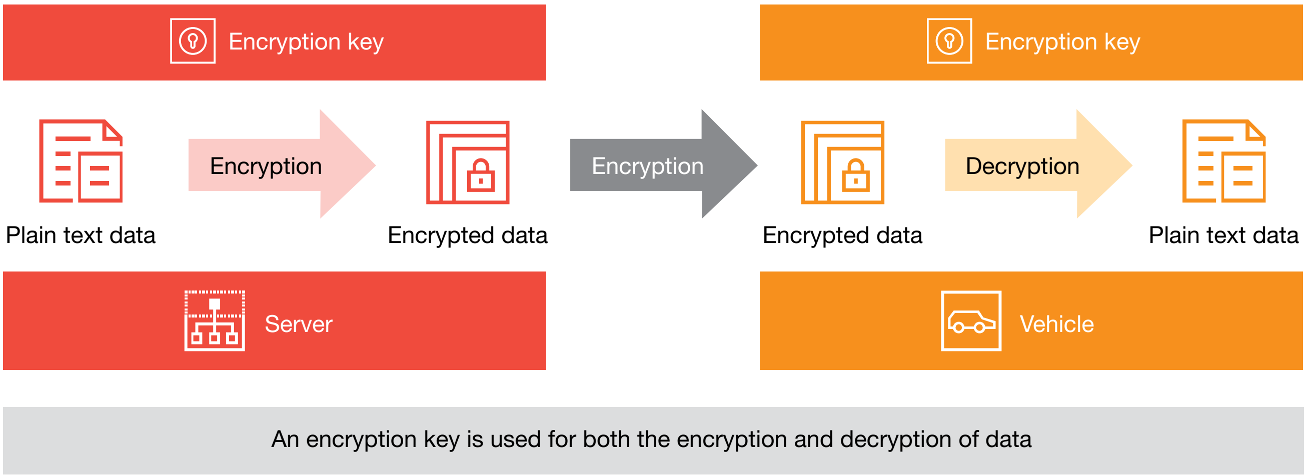
Examples of security measures for encryption key control systems

- Strengthening physical security such as managing access to server rooms
- Stronger system access control using multi-factor authentication
- Encryption key management using HSM[*2]
- Strengthening system log monitoring relating to encryption key control

As can be seen, encryption key management requires more robust security measures. In an environment in which an existing system and an encryption key system are intermingled on the same network, unless they are all brought up to the same level of security attacks may be made on the system which target the weakest security level and the encryption key control system on the expose the whole network to attack. Therefore, as mentioned above, the isolation of networks and access control must be implemented, and it is vital that the necessary and sufficient security structures are created in each system.

[*2] Hardware Security Module (HSM): secure hardware for storing important data in data centers such as encryption keys.

Diagram 14: Outline of encryption processing



8 Post-production security measures – cybersecurity monitoring

In this chapter we will consider the ideal security activities required after the production of vehicles.

Security activities are essential even after production

Activities to improve quality safety in vehicle development hitherto have consisted of activities implemented during the development and production phases prior to production. As introduced in previous chapters, pre-production security measures are just as important as security activities to improve product quality. However, from a security perspective, there are several reasons that necessitate the implementation of measures even after production. The background to this is the presence of hackers who actively attack products.

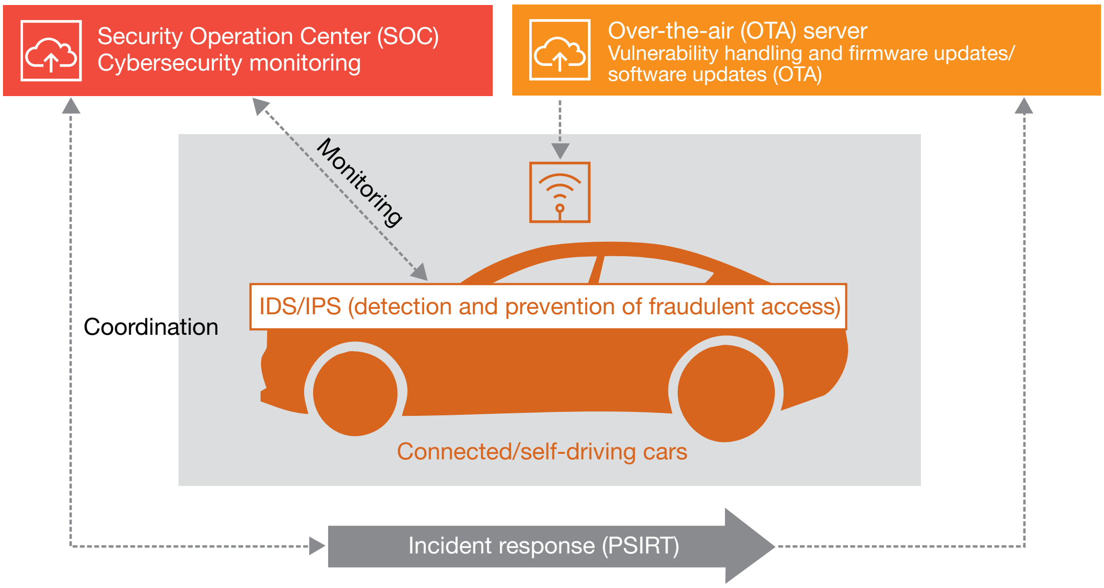
Hackers may develop new methods of attack. It is also possible that a measure that was adequate at some phase prior to production becomes unable to prevent a newly discovered method of attack. In order to cope with active hackers who actively encourage the evolution of attacks, the need arises for security measures that track the changing security environment after production.

Overall view of security activities during the post-production phase

The security measures that should be implemented after production are the activities of cybersecurity monitoring, vulnerability handling, firmware updates, and incident responses indicated in ISO/SAE 21434 (see Diagram 15). Cybersecurity monitoring is the activity of monitoring vehicles and detecting attacks on them. Vulnerability handling and the firmware updates use updated firmware when a vulnerability is detected after production and restore vehicles back to a safe state. The objective of incident response is to prevent the occurrence of damage according to the details of attacks after they have been detected. The system that plays the central role here is the Product Security Incident Response Team (PSIRT).

Similar activities have been conducted thus far in the IT sector. Just how far the contents of activities in the IT sector and the knowhow that can be applied to vehicles is an important question to consider.

Diagram 15: Overall image of post-production security activities


Security Operation Center (SOC)
Cybersecurity monitoring
Over-the-air (OTA) server
Vulnerability handling and firmware updates/
software updates (OTA)
Monitoring
Coordination
IDS/IPS (detection and prevention of fraudulent access)
Connected/self-driving cars
Incident response (PSIRT)

Cybersecurity monitoring activities

Cybersecurity monitoring is the collection and analysis of cybersecurity incidents, threat information, vulnerability information and cybersecurity information pertaining to in-house products. Cybersecurity information can be broadly split into two categories: external information provided by governmental organizations and security vendors, and in-house information such as vulnerability information discovered during in-house assessments.

If information is obtained externally, there is a need to make appropriate selections from among the diverse fee-paying and free-of-charge information available, and to pursue the collection of information in a continuous and timely manner. As of 2019, the number of reported attacks on vehicles is not yet particularly high. However, there are many reports of vulnerability information about products installed on vehicles. There is a need to create an operational system for steadily obtaining such information, deciding whether the reported information is relevant to one's own company, and accurately appraising the degree of influence it may have.

One type of information that can be obtained internally is the vulnerability information that has been discovered during in-house assessments and security tests. If such information is discovered, the requisite repair work and its incorporation in to the products becomes necessary. There is a more detailed commentary on this in the section on vulnerability handling and firmware updates in the next chapter.

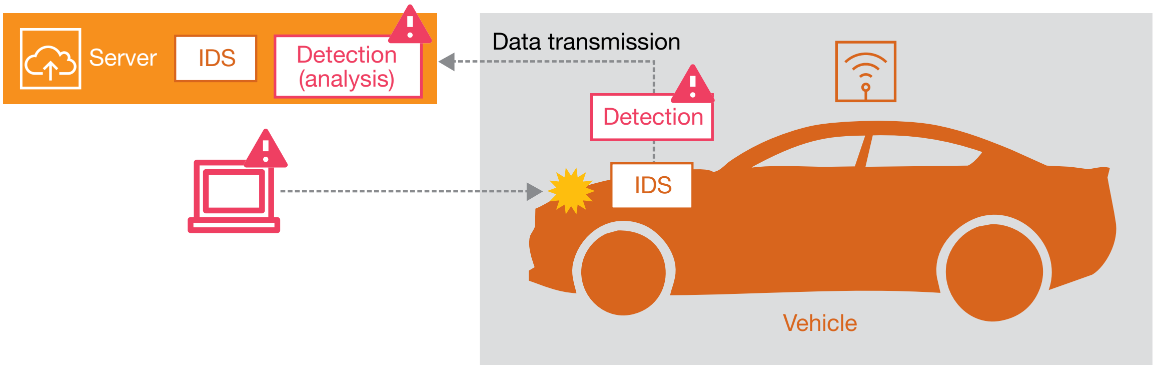
In addition, the introduction of on-board intrusion detection systems (IDS) and a security operation center (SoC)/security information and event management (SIEM) as in-house measures for obtaining attack information is being pursued, with the aim of detecting attacks on one's own company product without having to rely on externally-sourced information.

On-board IDS and SoC for vehicles, which are useful in collecting attack information

On-board IDS are components or software installed in vehicles as devices to detect attacks in real time on a vehicle or its components. On-board IDS are available as network-type or host-type, and analyze the data passing through a vehicle's network, transmission data to components and the behavior of component-operated software, thereby detecting attacks that could potentially damage vehicles. In order to handle the attacks of hackers, activities cannot be launched without the identification of the advent of attacks. Therefore, IDS can be described as a particularly important technology bearing in mind the above-mentioned presence of active attackers.

Furthermore, the usage of on-board IDS in combination with the operation of an SoC for vehicles is also under ongoing examination. As on-board IDS are inside vehicles and operated by a limited range of resources, they are not well-suited to the analysis of complicated and vast amounts of data. Therefore, a structure is adopted in which on-board IDS conduct just simple analyses while the requisite data is transmitted to an SoC prepared in a cloud environment, to which the task of more complex analysis is left (see Diagram 16). The SoC performs the role of analyzing the vast volumes of data sent in from multiple vehicles and capturing any signs of attacks. Furthermore, in preparation for an event in which an SoC discovers an attack on any vehicle, instructions are sent from the SoC to the vehicle in question, and through the combined creation of functions that launch measures such as shielding of communications, vehicles are immunized against future cyberattacks.

Diagram 16: Real time detection and handling of attacks on vehicles



9 Keystone of Post-production security measure——PSIRT

Here we will consider vulnerability handling, firmware updates and incident response in which PSIRT activities play the main role among post-production security activities.

Looking back on security activities in the post-production phase

As explained in Chapter 8, vehicle and vehicle system security measures are related to many stakeholders and must be followed throughout the entire vehicle life cycle. The system that performs the core role in security measures during the (after sales) market usage phase, i.e. once the vehicles take to the roads, is the product security incident response team (PSIRT). The main activities of PSIRT are the cybersecurity monitoring, vulnerability handling, firmware updates, and incident responses as defined in ISO/SAE 21434 .

Activities in vulnerability handling and firmware updates

Vulnerability handling and firmware update activities are implemented if the cybersecurity information, such as security incidents, threat information or vulnerability information related to the company's product, collected through cybersecurity monitoring activities contains vulnerability information which requires to be handled.

The details of the newly acquired vulnerability information are evaluated, and in order to rapidly make the necessary responses, it is required that a company have evaluation criteria in place beforehand. The evaluation criteria for vulnerability information are created by each company with reference to the evaluations[*1] of standardization authorities, but there is also a need for criteria from which comprehensive evaluations can be made according to the impact framework (safety, financial, operational and personal information) and "probability of occurrence" (feasibility of abusing the vulnerabilities and the time required). For example, in the event of vulnerabilities such as "the possibility of random fraudulent CAN[*2] messages being transmitted to a vehicle's onboard control network" or "its automotive navigation system being rendered unusable," because of the great difference in safety impacts, if their probability of occurrence are the same, it is the former vulnerability that is considered to be the more serious (see Diagram 17).

In order to appropriately evaluate the impact it is absolutely essential to manage the information about what sort of software (open source software (OSS), in-house software or third party software) and which versions are being used, as well as which protocols and to be able to swiftly and accurately ascertain the scope of influence of vulnerability information.

[*1] In Japan, the Japan Computer Emergency Response Team (JPCERT) publicizes the results of evaluations of vulnerabilities using a common vulnerability scoring system (CVSS)

[*2] Controller Area Network (CAN): a standard for the communications networks that connect electronic circuits and various equipment inside vehicles.

Diagram 17: Vulnerability evaluation standards matrix

Severity of risks caused by vulnerabilities = Impact × Probability of occurrence

		Impact				
		0	1	2	3	4
Probability of occurrence	1	Low	Low	Medium	Medium	High
	2	Low	Low	Medium	High	High
	3	Low	Medium	High	High	Critical

Vulnerability evaluation standards matrix (image)
In line with the impact and probability of occurrence evaluation scores, the severity of vulnerabilities is ranked as critical, high, medium or low.

The relationship between the threat analyses conducted at the concept phase and at the product development phase are extremely important in the evaluation of vulnerability information. External attacks on vehicle systems frequently exploit not just one but multiple vulnerabilities. There are some cases in which certain threat scenarios, originally categorized during the threat analysis as having a low possibility and deferred until later, can suddenly emerge as high-priority threats due to the discovery of other new vulnerabilities. When new information on vulnerabilities appears, there is a need to check what their impact upon already completed threat analyses will be, and to protect against them with the appropriate measures.

Incident response activities

There is a need for incident response activities providing external explanations while collaborating in-house, centering on PSIRT, not only when new vulnerability information is detected but in the following cases too. In situations in which damage has already been caused (for example, the leakage of personal information owned by the company through abuse of vulnerabilities, or the falsification of information configured by the company) and in situations in which there is an extremely high possibility of damage occurring (for example, when researchers make the existence of an attack method through which one's company's products can be remotely controlled, or when similar products with the same structure as the company's products are hacked, is made public).

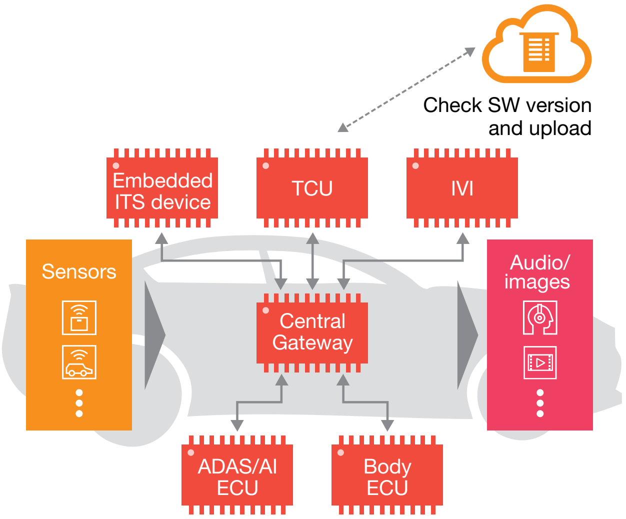
In the case of incident response, the PSIRT collaborates with the product development division, quality control division, IT division and other in-house stakeholders. The PSIRT team takes the severity of damage, possibility of collateral damage and its scale into consideration and implements incident triage (the allocation of priority levels according to the emergency level of the incident). Incidents that are deemed to be high-priority require the implementation of responses according to the pre-determined incident handling flow, after an emergency report has been made to the appropriate management level. Although the PSIRT play the lead role in this series of processes, it is desirable that preliminary drills are conducted as it is vital that each division is well-versed in procedures in order to provide a smooth response.

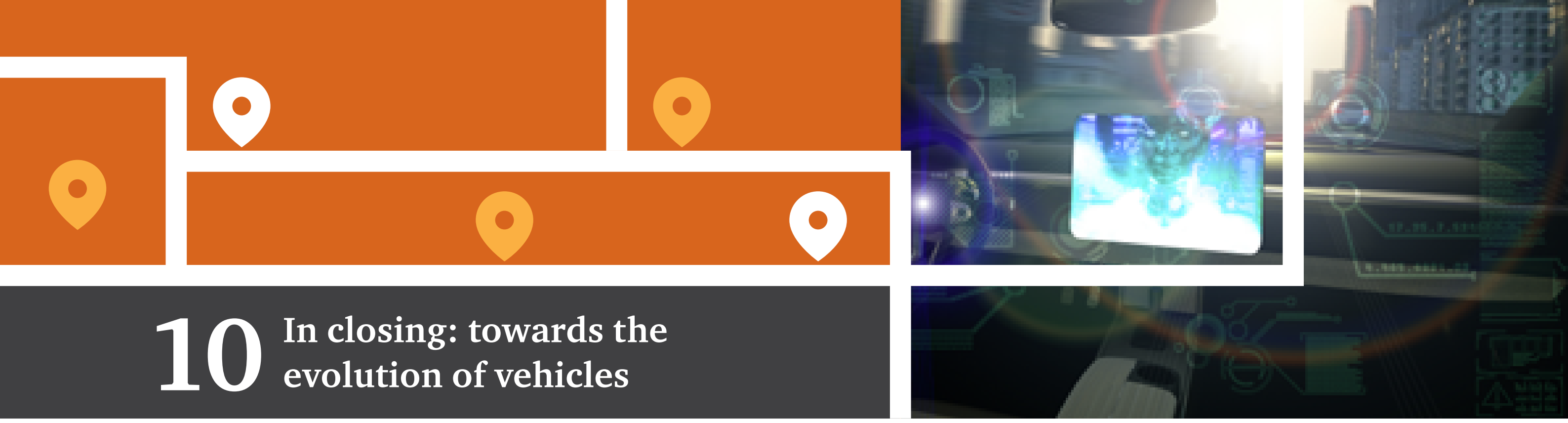
Once the cause of an incident has been detected and the measures to prevent (or minimize) damage have been clarified, it is essential that a diverse range of stakeholders are collaborated with and measures implemented. Care is required in cases in which user conduct and consent is required in order to make some sorts of alterations to their vehicles or vehicle systems (such as usage methods, configurations, software).

For example, there is a difference in the impact for vehicle owners in the following events: 1) the firmware has to be updated at a registered dealer due to a firmware vulnerability, that enables arbitrary CAN messages to be remotely sent, and 2) the same updates can be performed OTA. The latter case puts much less burden for the owner and easier to implement. In other words, there is a need for mechanisms enabling smooth and rapid updating of products after sale, in a sustainable manner.

The mechanism for these sorts of updates (see Diagram 18) must be examined and implemented at the concept and product development phases, and the PSIRT must use its experiences in handling vulnerabilities and incidents to offer appropriate suggestions and perform the role to provide information during the concept and product development phases.

Diagram 18: OTA firmware update system





10 In closing: towards the evolution of vehicles

In the precious chapters we have made some observations on the security activities required during vehicle development, production and post-production, based on the insights obtained from the ISO/SAE 21434. In this closing chapter we will review the observations made about security activities in their entirety and confirm once more the coordination and collaboration between each security activity. In conjunction with this review, we will also offer some thoughts about the future of vehicle cybersecurity, as in the title of this report.

Security activities across the entire vehicle life cycle: From the users' perspective

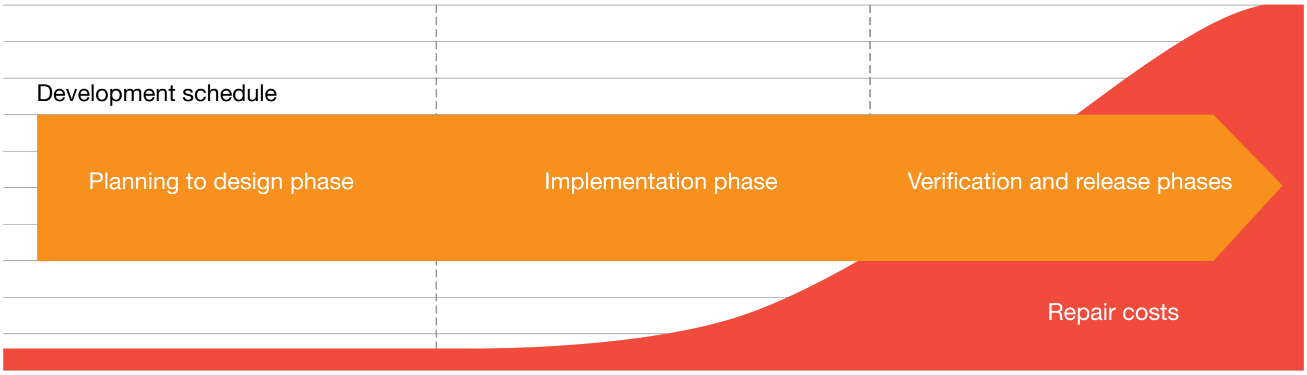
The objective of ISO/SAE 21434 is to define the cybersecurity processes throughout the entire vehicle life cycle. The "entire vehicle life cycle" means all the activities concerning development and operation of the vehicle, which starts with the planning and research of the vehicle, and is followed by its design, implementation and verification and its subsequent production and operation in the field (i.e. when the vehicle is on the roads) and eventual decommissioning. It will become necessary for cybersecurity initiatives to be taken in the course of all these activities.

There are several factors which drive the need for security activities across all the processes and activities of the vehicle life cycle. One of these factors is that throughout the entire vehicle life cycle there is ample room for the unwanted proliferation of vulnerabilities that become security risk factors (defects from the security perspective). It is feasible that such vulnerabilities may occur during the product development phase and the production phase. In addition, if a vulnerability does affect a process, in order to redress that vulnerability after production a need arises for security activities that have been introduced after the vehicle has been released to the market. The possibility that users may be confronted with cybersecurity damages cannot be discounted if a vehicle remains vulnerable. In order to prevent damage to users, it is essential that security activities are implemented throughout the entire vehicle life cycle.

Security activities throughout the entire vehicle life cycle: From the OEMs' perspective

One of the other reasons that it is possible to cite the need for security activities throughout the entire vehicle life cycle is the improvement in efficiency of security measures. It is known that taking measures in each process rather than immediately after vulnerabilities or factors through which vulnerabilities arise is something that incurs considerable costs (see Diagram 19). This is because the later the processes in product development are, the more the deliverables such as the design documents, source codes and test data created increase. Vulnerabilities that could cause problems in these deliverables must be discovered and measures which will not affect other areas that have already been developed must be implemented. The demands for the implementation of security activities throughout the entire vehicle life cycle made in the ISO/SAE 21434 is not made solely from the notion of protecting users from security damage; it also serves as a pointer for rationalization, which is a beneficial activity from the perspective of OEMs. It is important that OEMs understand the fact that conducting activities throughout the entire vehicle life cycle is the best option for the benefit of the whole society surrounding vehicles, from the point of view of both users and makers.

Diagram 19: Repair costs that rise in conjunction with the progress of development process



Security measures through a single chain

We have sorted through the significance of activities through the entire vehicle life cycle in this report and will now make some observations on the coordination between security activities in each phase of that life cycle. The report has covered security activities in the concept phase, design phase, implementation phase, testing phase, production phase and post-production phase. In the course of these activities it is usual for the person-in-charge at each phase to be a different person, and the person-in-charge (implementer) and the person with final responsibility also are not usually the same person.

Does it then follow that the people in charge and the responsible persons are different at each phase, due to each security activity being an independent activity? It does not, because in reality the security activities conducted at each phase are not wholly independent but are intricately linked to the phases that come before and after them. For example, it is essential that the threats identified during the concept phase undergo follow-up checks during the security testing phase, and that they are evaluated as testing items where necessary. Furthermore, these threats must be monitored during the post-production monitoring activities. It is in this manner that the activities drawn together for each of the product life cycles should in fact be activities conducted in mutual and intricate collaboration.

Even if the person-in-charge and the responsible person for security activities in each separate phase are different they need to understand that the activities are all mutually linked, and that the sharing of information and enhancing collaboration between person in charge and those with final responsibility is a security objective that should always be aimed for.

The future of vehicle cybersecurity

The future of vehicles as seen in the connected vehicles and autonomous driving, is a new value demanded by society. The arrival of vehicles that deliver this new value is clearly something that will improve lifestyles and society as a whole.

On the other hand, as can be seen through the various observations made in this report, there is a need to steadily pursue cybersecurity measures at each phase of the product life cycle in the future development of vehicles. Even if there is a defect in or inadequacy in just a single part of security activities it is possible that it could be a factor that leads to security damage to the vehicle or the owner.

If security activities are not conducted correctly, even though new vehicle owners may benefit from new services, they will at the same time be exposed to security threats. The members who will build the next-generation mobility society, or in other words, those who will create the vehicles of the future, have a duty to both provide value to users and promote activities towards vehicle security. The right to create the new vehicles of the future can only be earned by promoting vehicle security activities.

PwC Japan Group Contacts

PwC Japan Group
https://www.pwc.com/jp/ja/contact.html

Authors

Ken Okuyama
Senior Manager, PwC Consulting LLC

Junichi Murakami
Director, PwC Consulting LLC

Hiroshi Nodomi
Manager, PwC Consulting LLC

Tomohiro Yasui
Manager, PwC Consulting LLC

Kenta Sawa
Senior Associate, PwC Consulting LLC

Mariko Yoshida
Senior Associate, PwC Consulting LLC

Kei Kamei
Senior Associate, PwC Consulting LLC

Supervior

Kazuhiro Hayashi
Partner, PwC Consulting LLC

www.pwc.com/jp

PwC Japan Group represents the member firms of the PwC global network in Japan and their subsidiaries (PricewaterhouseCoopers Aarata LLC, PricewaterhouseCoopers Kyoto, PwC Consulting LLC, PwC Advisory LLC, PwC Tax Japan, and PwC Legal Japan). Each firm of PwC Japan Group undertakes its business as an independent and separate corporate entity.
To address complex and diversified business challenges, PwC Japan Group consolidates expertise of assurance, deal advisory, consulting, tax and legal services as well as enhances its structure in order to cooperate organically. As a professional service network with a total number of more than 8,100 partners and staff, PwC Japan Group provides quality client services to meet their needs and expectations.
At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 276,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

The electronic edition can be downloaded at the following URL: www.pwc.com/jp/ja/knowledge/thoughtleadership.html
Issued on January, 2020 Issue No.: I202005-01

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.