Cybersecurity of automotive semiconductor products

Toshiba Electronic Devices & Storage Corporation

In addition to the movement in the automotive industry toward Connected, Automated, Shared & Service, Electric (CASE) vehicles[*1], the developed countries are promoting mobility as a service (MaaS)[*2], transforming automotive mobility services and facilitating software implementation of automotive functions. Under these circumstances, enhancing the cybersecurity of automotive electrical and electronic (E/E) systems is a pressing issue. To address this issue, the United Nations has developed automotive cybersecurity regulations—UN Regulation No. 155 (UN-R155) and No. 156 (UN-R156). These regulations require automobile manufacturers to obtain certificates for cybersecurity management systems (CSMS) and software update management systems (SUMS) in order to obtain vehicle type approval. Semiconductor suppliers are also required to provide evidence of CSMS and SUMS compliance and explanations of management methods.

Most of the CSMS compliance requirements can be satisfied by complying with ISO/SAE 21434, an international standard for automotive cybersecurity engineering, which defines the procedure necessary to achieve sustained security throughout the product's life cycle shown below in the figure "Cybersecurity risk management throughout a product's life cycle." Most of the SUMS compliance requirements can also be satisfied by complying with ISO 24089, an international standard for automotive software update engineering, which defines the procedure necessary to ensure the integrity and authenticity of software updates in the sequence of software update activities shown below in the figure "Software update risk management."

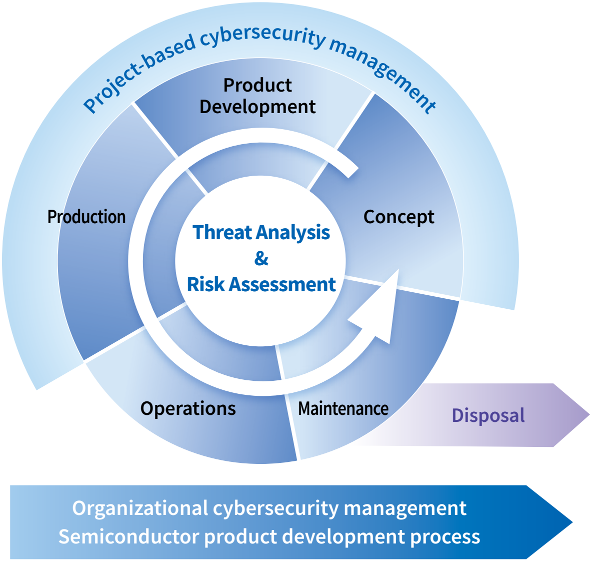
Toshiba Electronic Devices & Storage Corporation has established in-house regulations and development processes compliant with ISO/SAE 21434 and ISO 24089 to guarantee that its semiconductor devices for powertrain, safety, body electronics, and other E/E applications are compliant with CSMS and SUMS, aiming to contribute to continued security risk management in automobiles.

Our development processes with seamless cybersecurity solutions are based on the conventional ISO 9001 process and incorporate an automotive hardware and software quality management system based on IATF 16949 and Automotive SPICE®, a functional safety management process based on ISO 26262, and an add-on cybersecurity management process[*3] based on ISO/SAE 21434 and ISO 24089. Furthermore, we have established cybersecurity incident response procedures, including those for continuous cyber threat monitoring and software updating, which are implemented in cooperation with Toshiba Group's CSIRT and PSIRT activities. Our newly established development processes have been certified by an external organization for compliance with ISO/SAE 21434 and ISO 24089.

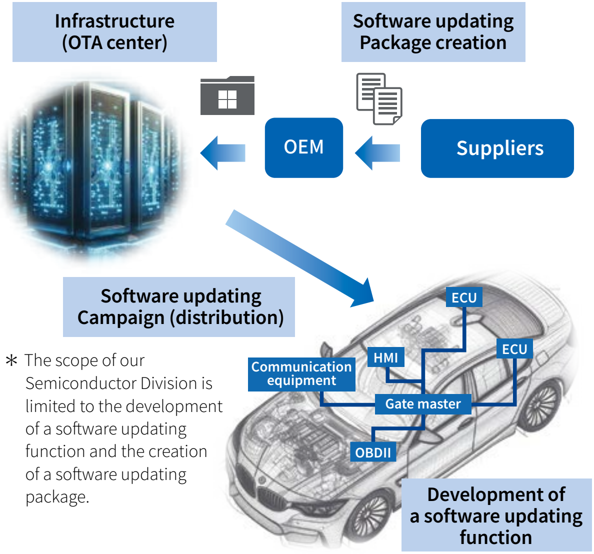
We will continue to utilize these development processes to develop and offer automotive semiconductor devices that will help maintain automotive E/E systems in up-to-date and secure conditions.

[*1] It is used as a mid-term strategy by automobile manufacturers aiming to transform into mobility service providers.
[*2] It is a type of next-generation service that seamlessly connects conventional public transportation systems with ride- and bicycle-sharing services using IT.
[*3] Our cybersecurity management process is not compliant with processes of ISO 24089 that are outside the scope of the Semiconductor Division: the Infrastructure-level and software update campaign.

• Automotive SPICE® is a registered trademark of the Verband der Automobilindustrie e.V. (VDA)


Project-based cybersecurity management
Product Development
Concept
Production
Threat Analysis & Risk Assessment
Operations
Maintenance
Disposal
Organizational cybersecurity management
Semiconductor product development process

Cybersecurity risk management throughout a product's life cycle


Infrastructure (OTA center)
Software updating Package creation
OEM
Suppliers
Software updating Campaign (distribution)
ECU
HMI
ECU
Communication equipment
Gate master
OBDII
Development of a software updating function

* The scope of our Semiconductor Division is limited to the development of a software updating function and the creation of a software updating package.

Software update risk management