Cyber security compliance (ISO/SAE 21434) for in-vehicle semiconductor products

Toshiba Electronic Devices & Storage Corporation

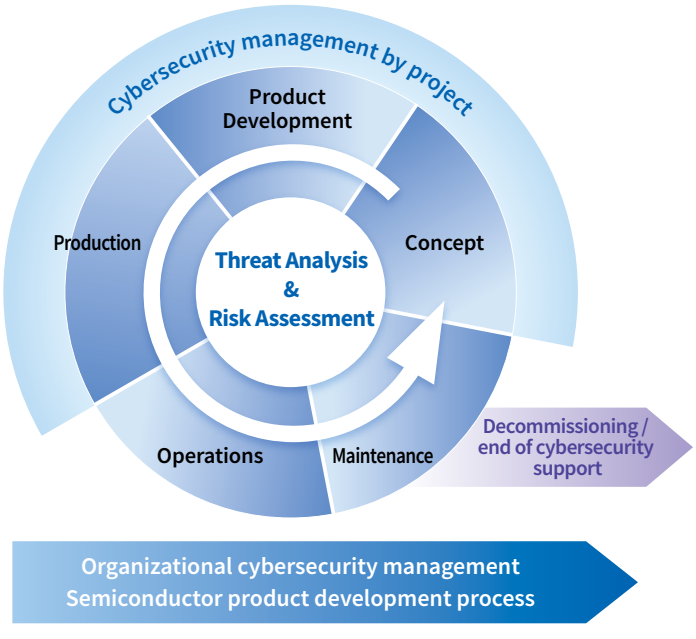
In addition to CASE*1, which is the goal of the automotive industry, as automobiles are being transformed into mobility services, such as the promotion of MaaS*2 occurring primarily in developed countries, and as software is becoming an increasingly prominent aspect of automobile functions, strengthening cybersecurity measures for in-vehicle E/E systems*3 is an urgent issue. In international law, WP.29 of the United Nations Working Group has already approved and enacted regulations for vehicle cybersecurity (UN Regulation No.155 [UN-R155] and No.156 [UN-R156]). These regulations require Cyber Security Management System (CSMS) and Software Update Management System (SUMS) certification in order for automobile manufacturers to get vehicle type approval, and throughout the supply chain, semiconductor suppliers are also required to provide evidence of CSMS and SUMS compliance and explanations of management methods.

CSMS compliance is achieved in large part by complying with ISO/SAE 21434, the international standard for automotive cybersecurity engineering. This standard defines the procedures necessary to achieve sustainable security throughout the entire product life cycle, from planning,*4 through concept, product development, production, operations, maintenance, and decommissioning / end of cybersecurity support, as shown in the diagram below.

We develop and sell semiconductor products for in-vehicle E/E systems such as powertrain, safety, and body systems. Through the establishment of development processes and internal regulations that conform to ISO/SAE 21434, we ensure CSMS compliance for the entire product life cycle of these automotive E/E system semiconductors that we supply, thereby contributing to continuous security risk management for automobiles.

In regard to the development process, using the existing semiconductor product development process ISO 9001 as a base, we have implemented an automotive grade hardware and software quality management process based on IATF 16949 and Automotive SPICE, a functional safety management process based on ISO 26262, and a cybersecurity management process based on ISO/SAE 21434 as an add-on to the other processes, allowing us to achieve seamless cybersecurity support throughout the development process. Our ISO/SAE 21434-conforming development process has been evaluated for compliance with standards by an external agency and we have received certification. We have achieved continuous monitoring of security threats and response to incidents through cooperation with Toshiba Group's CSIRT/PSIRT activities. Going forward, in order to meet SUMS compliance, we will implement development process conformity with ISO 24089, which was officially issued recently, and provide semiconductor products that help to keep automotive systems up-to-date and secure.

*1 CASE = Connected, Autonomous, Shared, Electric
A medium-term strategy used by automakers to transform into mobility service providers.
*2 MaaS = Mobility as a Service; a next-generation mobility service that seamlessly connects conventional public transportation with ride sharing, bicycle sharing, etc. using IT.
*3 In-vehicle E/E systems = automotive Electric/Electronic systems
*4 Cybersecurity plan included in cybersecurity management by project



Management of cybersecurity risks throughout the product life cycle