FOR IMMEDIATE RELEASE

Hitachi and Hitachi Automotive Systems develop an automated safety requirement verification technique for automotive control systems

Tokyo, September 26, 2016 --- Hitachi, Ltd. (TSE: 6501, "Hitachi") and Hitachi Automotive Systems, Ltd. ("Hitachi Automotive Systems") today announced the co-development of technology that automatically verifies safety requirements for automotive control systems with computers by coding requirement specifications*1 to simplify and unify expressions in the verification process conducted by car manufacturers and automotive suppliers. This technique enables the time required to verify that all the safety requirements are present to be reduced to one-tenth.*2 Hitachi and Hitachi Automotive Systems are aiming to realize greater development efficiency while maintaining safety and reliability of automotive control systems. This technology can also contribute to the development of autonomous vehicles being pursued by respective car manufacturers.

Automotive control systems are becoming increasingly large and complex with developments such as autonomous driving. This also incorporates greater risks in the unfortunate event that a malfunction occurs. Malfunction in the automotive control systems pose a danger not only to the driver and any passengers but also pedestrians and the surrounding environment in general. ISO 26262, an international standard for functional safety, was established to ensure that such risks are sufficiently reduced in the development of automotive control systems. In the development of automotive control systems, the first specifications to be defined are the main function (e.g. autonomous driving system) and the safety function, in the event a malfunction occurs in the control system underlying the main function (Fig.1). To conform with ISO 26262, it is necessary that all safety requirements are noted in the requirement specifications, and presented to third-party certification organization or car manufacturers.

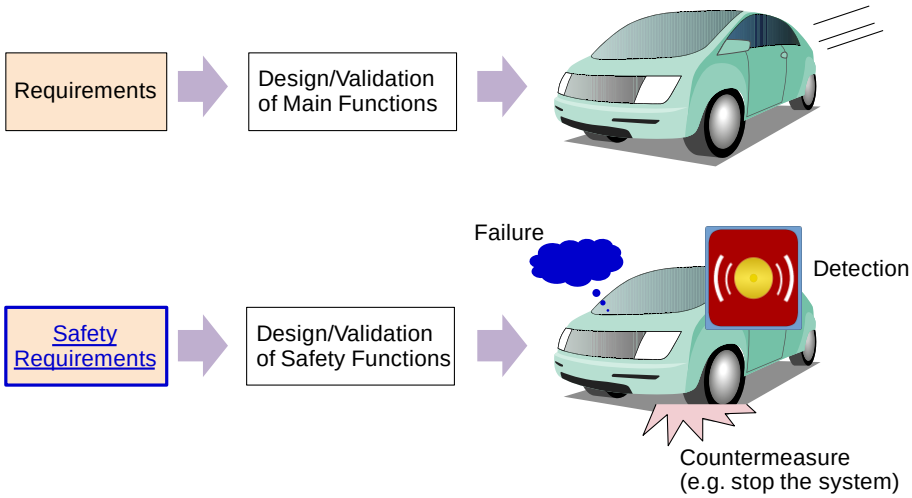

Figure 1 Safety requirements

Conventionally, safety requirements are written in a given language like English or Japanese. This presented challenges even to design engineers with domain knowledge to confirm the details of safety requirements and conduct verifications as a single word or expression may have several meanings or interpretations allowing ambiguity and inconsistent expressions as well as increasing the risk of missing requirements.

To resolve such challenges, Hitachi and Hitachi Automotive Systems developed a technique that encodes safety requirements (described as logical expression) to eliminate ambiguity and automatically verifies that all safety requirements are present. This technology was developed with the cooperation of the Aoki Laboratory in Security and Networks Area, School of Information Science, Japan Advanced Institute of Science and Technology.

1. **Elimination of ambiguity and automatic verification of safety requirements**
   The information to be input into the verification tool was clarified by expressing the safety requirements as strict mathematical logic expressions (propositional logic***3**) instead of conventional language descriptions (cf. Fig.2 Point (A)). Further, as the safety requirements are expressed in a syntax composed of simple mathematical expressions, the process of reading and writing safety specifications has been made easier for engineers. Safety requirements are defined first at a high-level for safety requirements inherent to the system, and then by detailed structural or functional requirements at a lower level for ECU,***4** sensors, actuators (electrical devices such as cut-off switches), communication paths, software, etc.***5** to realize that safety. Thus, the number of requirements increases with increasing detail. The verification tool automatically checks both the higher-level requirements that define the functionality of the control system as well as the lower-level detailed requirements that define how those functions will be achieved, and determines whether requirements are complete.

2. **Reuse of verified requirements for automatic generation of new requirements**
   Details of safety requirements may be similar between similar systems or between different components in the same system. It is therefore possible to reuse a part of a logical expression that has been verified as complete as a common pattern (cf. Fig.2 Point (B)). For example, when Sensor-B is used under the same condition as Sensor-A, and Sensor-B needs the same error detection as Sensor-A. The new requirements for Sensor-B can be automatically generated by setting the parameters for Sensor-B using the pattern created from the requirements for Sensor-A. By using an already verified pattern, design efficiency is raised as the newly generated requirement contains all necessary components, and a new requirement does not need to be defined.

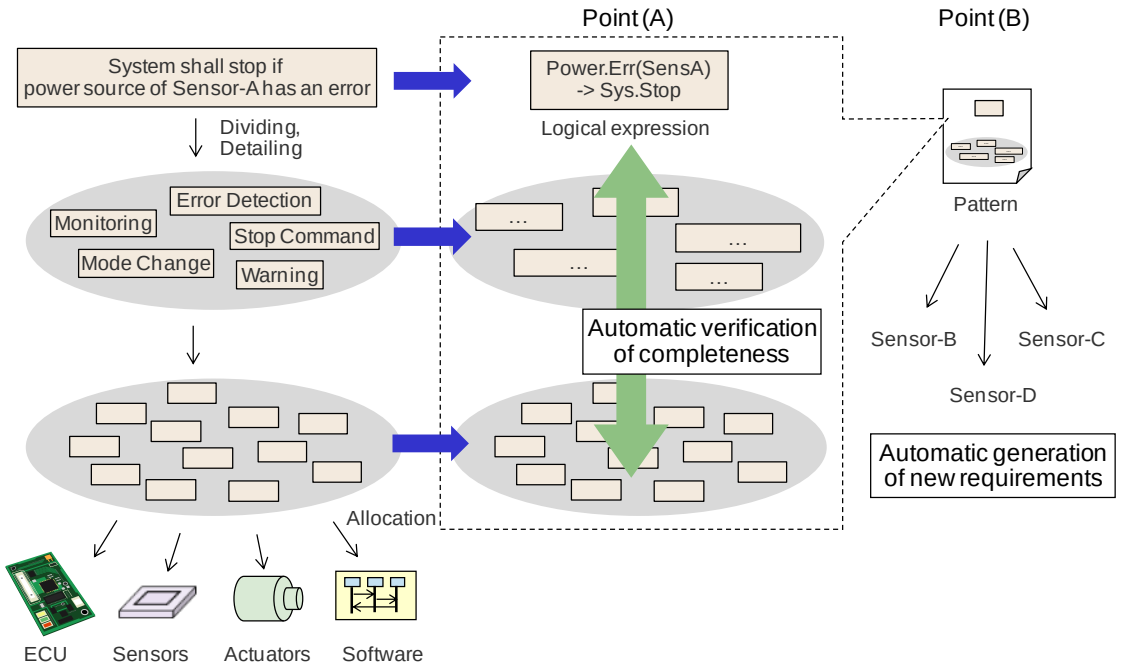

Figure 2 Outline of the technique developed

When this technique was applied to an EPS*6 system, an automotive control system, it was confirmed that the technique can describe and verify all requirements that appeared in the safety requirement specification for the EPS. Furthermore, the volume of the description was decreased by 30% compared to the original description in English, and verification time was decreased from 60 minutes for an inspection to 6 minutes for automatic verification by a computer. The technique was reviewed a third-party testing and certification company, TÜV SÜD, and found to be effective in conforming to ISO 26262.*7

By expanding applications and disseminating this technology which ensures the highly efficient maintenance of safety and reliability in automotive control systems, Hitachi and Hitachi Automotive Systems hope to contribute to the increasingly rapid advancements of the automotive industry.

*1 A description of intended purpose or demand by users or environment
*2 Hitachi survey result relative to time required for conventional verification.
*3 A branch of mathematical logic
*4 Electronic Control Unit
*5 Safety measure should be appropriate and safety requirements should represent the safety measure.
*6 Electric Power Steering: a mechanism to assist drivers steer with electric power such as motors.
*7 The feasibility report was received from TÜV SÜD Japan Ltd. in August 2016.

About Hitachi, Ltd.
Hitachi, Ltd. (TSE: 6501), headquartered in Tokyo, Japan, delivers innovations that answer society's challenges. The company's consolidated revenues for fiscal 2015 (ended March 31, 2016) totaled 10,034.3 billion yen ($88.8 billion). The Hitachi Group is a global leader in the Social Innovation Business, and it has approximately 335,000 employees worldwide. Through collaborative creation, Hitachi is providing solutions to customers in a broad range of sectors, including Power / Energy, Industry / Distribution / Water, Urban Development, and Finance / Government & Public / Healthcare. For more information on Hitachi, please visit the company's website at http://www.hitachi.com.

About Hitachi Automotive Systems, Ltd.
Hitachi Automotive Systems, Ltd. is a wholly owned subsidiary of Hitachi, Ltd., headquartered in Tokyo, Japan. The company is engaged in the development, manufacture, sales and services of automotive components, transportation related components, industrial machines and systems, and offers a wide range of automotive systems including engine management systems, electric power train systems, drive control systems and car information systems. For more information, please visit the company's website at http://www.hitachi-automotive.co.jp/en/.

# # #

Information contained in this news release is current as of the date of the press announcement, but may be subject to change without prior notice.
