Cyber Security Measures in Automated Driving Systems

March 30, 2018
Panel on Business Strategies for Automated Driving
0. Introduction (1/2)

External Communication Risks of Automated Driving Systems

- For the advanced automated driving that is supposed to be commercialized in the early 2020’s, cyber security risks caused by outside connection to the network inside the vehicle are imaginable.

Vehicles will connect to the outside by many communication methods (Wireless: dotted line / Wired: solid line)
0. Introduction (2/2)

Policy of Cyber Security Measures for Vehicles

- Amid the advances of automated driving and connected vehicles, it is essential to study and implement measures in consideration of the whole life cycle of the vehicle -- planning, development, use and disposal.
- While a balance between the manufacturing cost and selling price is required because security level improvements by themselves can lead to cost increases, a benchmark has not been developed yet.
- Therefore, since security requirements are tailored through research and development, after which global products are commercialized by setting rules (criteria and standards), it is necessary to formulate industrial guidelines. That is, the effectiveness of measures is improved and confidence in the industry as a whole is secured by (1) supporting safety verifications in design, development and use, and (2) preventing variations in the effectiveness of measures amongst manufacturers.

Communication security risks associated with automated driving and connected vehicles

Life cycle of the vehicle

- Planning
  - Product design
  - Design / Implementation

- Development
  - Manufacture
  - Countermeasure requirements
  - Component test

- Use
  - Applying normal use
  - Risk evaluation
  - System test

- Disposal
  - Maintenance
  - Use of second hands
  - Control of vulnerabilities and incidents
1. Current Study System

- For the in-vehicle security needed to ensure automated driving safety, including measures against cyber attack from outside of the vehicle, a progress schedule for promoting a common international development process and safety evaluation mechanism should be prepared within this fiscal year, hastening private-public efforts including human resource development (Growth Strategy 2017). The Panel on Business Strategies for Automated Driving summarizes the initiatives based on this.

- Research and development are being conducted by a wide range of government agencies such as the Cabinet Office, SIP, METI, MLIT and MIC. In addition, strategic initiatives concerning rules (criteria and standards) are being discussed in the Institute for Automated and Connected Vehicle Standardization.

- SIP-adus has implements White Hat Hacking via external communication in a large-scale demonstration and is preparing evaluation guidelines against attacks from outside of the vehicle.

- JARI is doing threat analyses (categorization of threats, influence on control and countermeasures) of vehicle interior systems based on the cases of use in JASPAR, and summarizes the requirements.

- From these initiatives, evaluation guidelines for OEM and suppliers will be formulated in JASPAR through industrial cooperation.

- However, while international criteria (WP29) are proposed mainly by JAMA and international standards (ISO/SAE21434) are proposed mainly by JSAE, the industry provides ideas to the proposals from other countries in order to steer discussions in a direction that does not bring disadvantages to Japanese industry.
2. Strategy concerning Rules (International criteria and International standards)

- No rules concerning security have been established yet. Therefore, each company has individually taken measures for the models to be launched around 2020 by referring to IT system standards.
- For the international criteria, recommendations had been promoted, but things are now turning to settings.
- Recently, many security guidelines and secure vehicles have been shown in each country. Close investigation of the necessary requirements should be brought forward in JAMA, JSAE and JASPAR, and the international standards concerning the development process including the design requirements are also being discussed with each country in the ISO/SAE JWG.

Before (Physical hacking risk) | Transition period (at present): 2020 model-year vehicles | 2020 and after (physical + external communication risks)
---|---|---
**International criteria**
Nothing in particular

**IT system standards including ISO15408 (CC) are used and measures are independently taken in each country**

- **2010**
  - Japan: JASO TP15002
  - Europe: AUTOSAR
- **2013**
  - Japan: JSAE (JAMA・JASPAR)
  - Europe: N3556 (Proposed by Germany)

<table>
<thead>
<tr>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015.3</td>
<td>Institute for Automated and Connected Vehicle Standardization</td>
</tr>
<tr>
<td>2016.5</td>
<td>Cybersecurity and data protection</td>
</tr>
<tr>
<td>2016.12</td>
<td>Cybersecurity and over-the-air issues</td>
</tr>
<tr>
<td>2016.11</td>
<td>Agreed to Guideline (ITS/AD)</td>
</tr>
<tr>
<td>2017.3</td>
<td>Guideline established (WP29)</td>
</tr>
<tr>
<td>2016.9</td>
<td>NHTSA Guideline</td>
</tr>
<tr>
<td>2017.9</td>
<td>Revised ver.</td>
</tr>
<tr>
<td>2018.6</td>
<td>NIST Cyber Supply Chain Risk Management</td>
</tr>
</tbody>
</table>

* Study of concrete requirements supplementary to the guideline and study for making regulations.
3. Overseas Trends (1/2)

- In addition to the 2nd Ver. of the NHTSA Guideline formulated in September 2017, legislation is being discussed also in the Senate and House.
- International standardization is proceeding together with the SAE, but rules may uniquely be controlled by decisions made in Washington.

**House-passed control (Self Driving Act): Was adopted in September 2017.**

- [Updating FMVSS concerning Level 3 or higher]
  - Developers of Level 3 or higher should submit a safety evaluation report based on the NHTSA guideline.
  - NHTSA formulates safety standards for Level 3 or the like, prepares the priority programs concerning research for the next 5 years and submits them to Congress or announces them officially.

- [Cybersecurity and privacy]
  - Manufacturers of Level 2 or higher should prepare a cybersecurity plan and privacy plan. (Submission to the government authority is not required.)

**Senate-passed control (AV Start Act):Is expected in the USA to be adopted during 2017.**

- [Cybersecurity]
  - Manufacturers of Level 3 or higher should formulate a cybersecurity plan. (Submission to the government authority is not required, but the government authority has the right to inspect it.) Manufacturers should prepare an outline that can be disclosed.
  - Federal offices cooperate on cybersecurity of Level 3 or higher. The Secretary of Transportation gives consumers information on cybersecurity. Manufacturers show the sources of such information via owners manual or the like.

- [Privacy]
  - The data access committee of Level 3 or higher is established in the Department of Transportation, and the committee submits deliberations and recommendations about ownership, management, access, etc. to Congress. The Government Accountability Office investigates the deletion of personal information after a loan spell of the rental cars or other rentals of Level 3 or higher, and reports suggestions to Congress.
  - NHTSA establishes the privacy data base to enable search for handling the privacy information.

**NHTSA: Revised version of Federal Automated Vehicles Policy is announced in September 2017.**

- [Outline]
  - Voluntary submission or announcement of 12-item safety evaluation report is required of manufacturers.

- [Cybersecurity of vehicles]
  - To minimize the risks of threats and vulnerabilities, robust products based on system engineering methods should be developed. Systematic and continuous safety risk evaluation should be included.
  - NIST21, NHTSA, SAE and AAM should review and introduce informative guidance and best practice design general rules.
  - The contents incorporated in the ADS including all actions, changes, selected designs, analyses, and relevant tests that enable tracking by NHTSA should be documented and a more robust control environment for document versions should be secured.
  - All incidents, misuses, threats and vulnerabilities that were proved by in-house test, consumer notifications, outside security investigations, etc. should be reported as soon as possible regardless of whether the company participates in Auto-ISAC or not. Furthermore, companies should make a robust plan against cyber-incidents and use the system engineering approach to cybersecurity in the design process. Systematic reporting and disclosure methods concerning the vulnerabilities should be studied.

- [Data recording]
  - For investigation at the time of collision and research & development to prevent collision scenarios, all available data should be recorded while protecting individual information so as to reproduce the conditions, for example, whether the vehicle was controlled by the system or the driver, and the data should be searchable. NHTSA starts the standardization of the data (format) in cooperation with SAE.

**NHTSA: Cybersecurity Best Practices for Modern Vehicles (October, 2016)**
China

- The China State Bureau of Quality and Technical Supervision in the Ministry of Industry and Information Technology establishes domestic information safety standards (14th item (*)) within China’s ICV industry standard system.
- Specifically, (1) basic technical research will be completed, a standard system will be established, a priority standard system for emergency rescue and communication security for vehicles will be formulated and prepared, and verification tests for the standards will be developed by the end of 2018. Furthermore, (2) the establishment of the 5G supported connected car industry series standard will be completed and the standards for information communication security and data security will be also prepared by 2020.

* Information security general-purpose test and evaluation method, technical requirements for the ECU, gateway and OBD interface, remote information service communication safety, etc.

Germany

- A rules strategy is being implemented, focusing related study around WP29 and ISO21434.
- Individual information and privacy are more highly regulated than Japan and data processing is regulated in the improved road traffic law.

Improved road traffic law (Enacted in June, 2017): New provisions concerning security are excerpted below.

Chapter VIa  Data processing in the vehicle
Article 63a  Data processing in the vehicle with highly or completely automated driving functions

(1) Vehicles based on Article 1a that defines “data processing in the vehicle with highly or completely automated driving functions” stores information on position and time that are calculated by the satellite positioning system if the vehicle handling changes between the driver and the system, which includes trouble such as TOR, failure and performance limit.

(2) Data stored based on Article 1 must be delivered at the request of the authority that handles punishments for driving infractions based on the state law. The delivered data are allowed to be stored and used by the relevant authority. The delivered data range should be the absolutely necessary matter for the relevant authority to check Clause 1 during its investigation. This does not affect the general rules about the handling of individual information.

(omitted)

(4) The data stored based on Clause 1 should be deleted after 6 months passes, excluding that of the relevant vehicle involved in the incident stipulated in Clause 1 of Article 7. In this case, the relevant data should be deleted after 3 years passes.

(5) The data stored based on the Clause 1 in combination with the incidents stipulated in Clause 1 of Article 7 can be delivered to a third party for accident investigation in an anonymized form.

UK

- There are statements requiring regulation in WP29. There is no OEM within the country, but the VCA of the certification organization works in collaboration with a private examination body (MIRA).

Key Principles of Cyber Security for Connected and Automated Vehicles (Released in August, 2017)
Hacking an automated driving vehicle may cause a serious accident. Therefore, it is recognized that a self-driving vehicle needs the same advanced IT measures as “financial institutions” and “aviation”, “rail” and “electric power” that are positioned as important infrastructure fields.

Self-driving vehicles of Level 3 or higher where the system drives the vehicle are not commercialized, and also include leading-edge technology. Furthermore, the electronic control system varies with each country and evolves rapidly. Therefore, areas of collaboration and competition are set to promote efforts.

Especially, the following items are being promoted as areas of collaboration between government and the private sector.

1. Preparation on an evaluation environment (testbed) so that vulnerabilities can be analyzed via collaboration amongst small and medium-sized suppliers
2. Multi-layer defensive design and standardization of the development for safe design
3. Building an information-sharing system on the operation side
4. Development of cybersecurity human resources, which are strongly needed

As areas of competition, each vehicle manufacturer is promoting the following initiatives.

1. Preparation on an evaluation environment (testbed) in order to analyze vulnerabilities based on the electronic control system of each company
2. Individual safe design within the standardized design and development process
4. Initiatives in technical development, information sharing and human resource development in Japan (2/5)

(1) Preparation of an evaluation environment (testbed) to promote the analysis of vulnerabilities

- In a METI and MLIT joint project, the building of a testbed that simulates the onboard computer network of a vehicle is promoted mainly for small and medium-sized suppliers, security vendors and research institutions to evaluate vulnerabilities (under construction in JARI as the “Research, Development and Demonstration Project for Social Implementation of Advanced Automated Driving Systems”).
- Using this testbed, small and medium-sized suppliers can verify the vulnerability evaluation when the Automated Driving System including their own products are hacked, and it is also expected that this testbed is applied to vulnerability analysis by research institutions and human resource development.
- From now on, it is necessary to design the conditions of use so that the users can use the testbed effectively.

Application, utility form and features of the testbed

- **Development of security evaluation and defense methods**
- **Security evaluation environment**
  - Simulated server system
  - Simulated vehicle system
  - Simulated peripheral environment
  - Attack

**<Features>**
- Open platform
- Security halls can purposely be produced.
- There is a lot of flexibility in setting the ECU.

**<Utility form>**
- Using the evaluation environment, security evaluation and defense methods (countermeasure techniques) are developed.
- Achieved results are shared with the relevant agencies.
4. Initiatives in technical development, information sharing and human resource development in Japan (3/5)

(2) Multi-layer defensive design and standardization of development for safety design

- Information by external communication is for auxiliary purposes to ensure redundancy. Even if no information is obtained or if information is masqueraded, multi-layer defense and failsafe design are being advanced in order to ensure security.

- The motor vehicle industry in Japan collaboratively works on safety design and also combines forces with METI and MLIT. Meanwhile, the industry holds the chairman post of the Development Process PG in the ISO/SAE JWG and is playing a key role in discussions about international standards for the development process including the design requirements.

**<Under normal condition>**

- External communication information
- Normal driving

**<Under masqueraded external communication>**

- External communication information
- The vehicle system immediately detects abnormalities and ensures safety based on sensor information. (The vehicle safely stops.)
  * Priority is given to sensor information.

**<When no information is given by external communication>**

- External communication information
- Normal driving or
  Ensuring safety based on the sensor information
  (The vehicle safely stops.)
  * Priority is given to sensor information.

Multi-layer defense design

- Communication protocol
- Central Gateway
- Control system
- Multi-layer defense

<Firewall>
Unfair information is blocked and only allowed information is given out.

<Message authentication>
No falsification of the message is confirmed.
4. Initiatives in technical development, information sharing and human resource development in Japan (4/5)

3. Building an information-sharing system on the operation side

- Unknown incidents, threats and vulnerabilities may occur on the operation side after introducing a vehicle on the market. Therefore, it is necessary to share such information within the industry, to prevent damage from spreading, and to improve the action level of the industry as a whole.

- Also, based on the METI cybersecurity management guideline, the J-Auto-ISAC WG was established in JAMA to share incident information concerning cybersecurity.

- In the future, it is necessary to pursue collaboration with the US-Auto-ISAC, IT industry and suppliers established in USA, and advance initiatives for rapid information-sharing and analysis.

Cyber security management guideline

10 important items>

1. Recognizing risks and formulating the action policy as an industry
2. Building risk management systems
3. Ensuring the resources (budgets, human resources, etc.) for taking measures
4. Understanding risks and formulating risk countermeasure plans
5. Building mechanisms to deal with risks
6. Implementing PDCA cycle in the measures
7. Preparing an emergency response system for when an incident occurs
8. Preparing restoration systems for incident damage
9. Taking measures and understanding conditions of the whole supply chain (including business partners and outsourcing companies)
10. Obtaining and effectively utilizing attack information by participating in information-sharing activities

J-Auto-ISAC Members

<table>
<thead>
<tr>
<th>Company name</th>
<th>Members of US A-ISAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toyota</td>
<td>✗</td>
</tr>
<tr>
<td>Honda</td>
<td>✗</td>
</tr>
<tr>
<td>Nissan</td>
<td>✗</td>
</tr>
<tr>
<td>Mazda</td>
<td>✗</td>
</tr>
<tr>
<td>SUBARU</td>
<td>✗</td>
</tr>
<tr>
<td>Suzuki</td>
<td>✗</td>
</tr>
<tr>
<td>Mitsubishi</td>
<td>✗</td>
</tr>
<tr>
<td>Daihatsu</td>
<td>✗</td>
</tr>
<tr>
<td>Isuzu</td>
<td>✗</td>
</tr>
<tr>
<td>Hino</td>
<td>✗</td>
</tr>
<tr>
<td>Mitsubishi Fuso</td>
<td>✗</td>
</tr>
<tr>
<td>Yamaha</td>
<td>✗</td>
</tr>
</tbody>
</table>

<Ref.> Measures in USA where information-sharing is developed

- 1998 Clinton’s EO 63
  Issued an instruction to share information to each of 18 important infrastructure fields
  ⇒ ISAC was established in each infrastructure
  (Banks, finance institutions, electric power, water and sewerage, traffic, communication, atomic furnace, arms industry and so on)

- 2003
  Established the National Council of ISAC that shares information with the above 18 fields in a cross-sectoral manner.

- 2013 Obama’s EO 13636
  Issued an instruction to formulate a framework for improving the cybersecurity level of the important infrastructure.

- August 2015 Established Auto-ISAC.
  Activities started in January 2016.
4. Initiatives in technical development, information sharing and human resource development in Japan (5/5)

(4) Development of cybersecurity human resources and application of white hat hacking

- Regarding the decisive shortage of cybersecurity human resources, highly advanced expertise is needed including the capacity for gathering the latest and unactualized information, understanding protective systems, and drawing up realistic measures.
- To cope with the above, human resource development courses and human resource development programs are carried out by collaboration amongst government, industry and academia.
- For the future, it is a question to build a more practical cybersecurity human resource development system because it is difficult to use the evaluation environment of each vehicle company. Therefore, the testbed that METI and MLIT prepared is expected to be utilized.
- In addition, it is necessary to take a proactive approach including scouting overseas human resources and intermediate recruitment. In so doing, it is essential not only to study the employment system for ensuring the needed human resources, but also to transmit the need for cybersecurity human resources at manufacturing sites and attractiveness of this job, by the coordinated activity of the industry.
- Furthermore, it is necessary to utilize the evaluation guideline concerning vehicle attacks from the outside that SIP is formulating from the standpoint of increasing security across the industry, and to cooperate with strong outside hackers in the future to discuss the implementation of White Hat Hacking.

IPA: Human resource development business in industrial cyber security center

- 2-day program (for executive directors of security offices)
- 1-year program (for young engineers)

<table>
<thead>
<tr>
<th>Short-term program</th>
<th>Long-term program</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-day training courses for responsible persons including CEOs, CIOs, CISOs and department heads are provided 6 times a year. (3 training courses for all industries and 3 industry-focused training courses)</td>
<td></td>
</tr>
<tr>
<td>Programs targeting the persons in charge of “core human resources” who connect business management and field service representatives</td>
<td></td>
</tr>
<tr>
<td>About one year of training imparts comprehensive knowledge in technological fields (OT and IT), management and business.</td>
<td></td>
</tr>
</tbody>
</table>

JSAE: Human resource development business

- Basic automobile engineering course
- Basic motorcycle engineering course
- Various courses
- Networking events for female engineers
- (Branch) technology networking events, lecture meetings, study tours
- Automobile cybersecurity courses

- Automobile engineering handbook
- Basic automobile engineering
- Symposium text, etc.
5. Progress Schedule to Promote a Common International Development Process and Safety Evaluation Mechanism

- Aim at sharing development and evaluation methods to improve development efficiency and ensure safety.
- Set the minimum required standards to realize the above, and aim to put evaluation environments (testbed) into practical use. Also, create an information-sharing system concerning incident response.

### Application target

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>International criteria (WP29)</td>
<td>ISO/SAE joint development</td>
<td>ISO21434</td>
<td>Proposal on standard requirements</td>
<td>Formulation of the guideline on the specifications level</td>
<td>Revision of standards and guideline</td>
<td>JSAE (JAMA • JASPAR)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>International standards (ISO/SAE)</td>
<td>Formulation of guideline</td>
<td>Study of specific requirements to for supplementing the guideline and technical study for establishing laws and regulations</td>
<td>Clarification of the requirements for laws and regulations</td>
<td>MLIT • NTSEL • JAMA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Formulation of industry requirements</td>
<td>Setting the minimum required standards</td>
<td>Formulation of the guideline on the specifications level</td>
<td>ISO/SAE joint development</td>
<td>ISO21434</td>
<td>JSAE (JAMA • JASPAR)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat analysis</td>
<td>Creation of in-vehicle common architecture</td>
<td>Categorization of in-vehicle threats by external communication and formulation of countermeasure requirements</td>
<td>Establishment of the evaluation method based on countermeasure requirements</td>
<td>METI(JARI)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research and development</td>
<td>Development of evaluation method and environment (testbed) system</td>
<td>Development of evaluation environment (testbed)</td>
<td>Raising the level</td>
<td>METI(JARI)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information-sharing system in operation</td>
<td>Start-up of J-Auto-ISAC WG</td>
<td>Expansion of the collaboration system for information-sharing</td>
<td>Creation of an ISO certification system</td>
<td>Evaluation and certification system</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Timeline

- **FY 2016**: Start-up of J-Auto-ISAC WG
- **FY 2017**: Expansion of the collaboration system for information-sharing
- **FY 2018**: Creation of an ISO certification system
- **FY 2019**: Raising the level
- **FY 2020**: Development of evaluation environment (testbed)
- **FY 2021**: Development of evaluation method and environment (testbed) system
- **March 2025**: Completion
- **March 2030**: Underway and policies

### Achievements

- Realization of Level 3 on expressways (Private use cars)
- Realization of Level 2 on general roads (Private use cars)
- Tokyo Olympics and Paralympics

### Research and Development

- **International criteria (WP29)**
- **International standards (ISO/SAE)**
- **Formulation of industry requirements**
- **Creation of in-vehicle common architecture**
- **Categorization of in-vehicle threats by external communication and formulation of countermeasure requirements**
- **Establishment of the evaluation method based on countermeasure requirements**
- **Revision of standards and guideline**
- **Creation of an ISO certification system**

### Policies

- **FY 2019**
- **FY 2018**
- **FY 2017**
- **FY 2016**
- **FY 2020**
- **FY 2021**
- **March 2025**
- **March 2030**

### Industry

- **SIP**
- **METI(JARI)**
- **JAMA**
- **JASPAR**
- **JAMA • JASPAR • JASPAR + Collaboration with the IT industry**

### Next Steps

- **FY 2022**
- **FY 2023**
- **FY 2024**
- **FY 2025**
- **FY 2026**
- **FY 2027**
- **FY 2028**
- **FY 2029**
- **FY 2030**

### Key Areas

- **Threat analysis**
- **Research and development**
- **Information-sharing system in operation**