FUNCTIONAL SAFETY OF ROAD VEHICLE INFOTAINMENT SYSTEMS

KÖZÚTI JÁRMŰ INFOTAINMENT RENDSZEREK FUNKCIONÁLIS BIZTONSÁGA

DÉVÉNYI Géza[1]

Abstract

This paper investigates the challenges arise due to the increasing performance and complexity of In-Vehicle-Infotainment (IVI) systems. Mass production road vehicles implement more and more highly automated driving functions. The IVI-systems are interconnected with these functions as well as are in close interaction with the driver. Therefore, the IVI-systems are considered as safety-critical. The proper interaction with the driver can play a significant role in the controllability of hazardous driving situations. The requirements on providing valid information, e.g. geolocation, to other critical functions make the IVI-systems safety-critical. IVI-system malfunctions of self-driving vehicles can have the potential to lead to the violation of critical transportation infrastructure. The compromise of critical IT-infrastructures, e.g. cloud-based navigation, can have the potential to lead to malfunction of the IVI-system of self-driving vehicles.

Keywords

automated road vehicle, critical infotainment system

Absztrakt

A cikk a közúti jármű infotanment rendszerek (IVI) növekvő teljesítményéből és komplexitásából eredő kihívásokat taglalja. A sorozatban gyártott közúti járművek egyre több magas szinten automatizált vezetési funkciót valósítanak meg. Az IVI rendszerek összeköttetésben vannak ezekkel a funciókkal valamint szoros interakcióban vannak a jármű vezetőjével is. Ezekből adódóan az IVI rendszereket egyre inkább biztonságkritikusnak tekintik. A vezetővel történő megfelelő interakció alapvető szerepet tölthet be veszélyes vezetési helyzetek kezelésében. Ez mellett a más kritikus funkciók számára történő valós információk (pl. geolokáció) szolgáltatása is kritikus feladat. Önvezető autók IVI rendszerének hibás működése kritikus szállító infrastruktúrák veszélyetetéséhez vezethet. Kritikus IT infrastruktúrák (pl. felhő alapú navigáció) veszélyeztetése is magában hordozhatja annak lehetőségét, hogy az önvezető járművekben hibás IVI rendszer működéshez vezessen.

Kulcsszavak

automatizált, közúti jármű, kritikus, infotainment, rendszer

[1] geza.devenyi@yahoo.com | ORCID: 0000-0002-2513-0886 | Head of Quality and Safety / Minőségügyi és funkcionális biztonságtechnikai vezető | NNG Lld.

INTRODUCTION

The new road vehicles continuously implement more and more automated driving related features. The ultimate goal of the technology development in the automotive industry is to produce fully autonomous cars, that can drive everywhere in all conditions. Until reaching that advanced state, the technology will have to get over several maturity level. Due to the nature of the automotive business, the technical complexity of the autonomously driving cars and the related critical infrastructures, the continuous development is impossible without properly analyzing the whole context. This paper briefly describes the main IVI system components, highlights the automotive context and the relation to critical infrastructures.

BUILDING BLOCKS OF IVI-SYSTEMS

A general sketch of a premium passenger car can be seen in Figure 1. Not all these system blocks can be found in each passenger car. Some blocks are new developments, and some have already undergone major changes. [1] The main function of the IVI is still providing a Human Machine Interfaces (HMI) in the vehicle. The development of a HMI is a complex, interdisciplinary challenge. [2] As per in other vehicle domains, as well as in the IVI domain, the electronics and the software were the most innovative technological areas in the last decades.

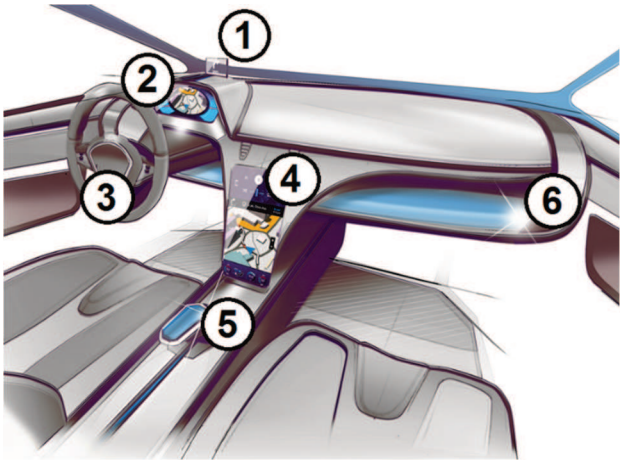

Figure 1 [3] Passenger car In-Vehicle-Infotainment system

The brief description of the building blocks listed below as per numbering in Figure 1**.**

The head up display (1) is a small transparent panel to project a limited amount of information on, mainly to inform, alert or warn the driver. This component is one of the latest developments in the automotive IVI systems. It is usually a compact, digital component. The instrument cluster (2) is one of the original building parts of the IVI systems. It also presents critical information to the driver, e.g. vehicle speed, information on the engine condition. The new premium category cars are already fitted with Liquid Chrystal Display (LCD). Due to reliability purposes, e.g. the safety critical warning functions have not always integrated in the LCD screen but are still using individual (Light Emitting Diode) LEDs.

The steering wheel controls (3) include several buttons and switches integrated in the steering wheel for the comfort of the driver. Vibrating effect can also built in the steering wheel to provide a diverse way of warning for the driver. This warning function can already be considered as safety critical. The head unit (4) can function as the actual brain of the IVI system. For all future cars, it will include a touch screen and a reasonably powerful hardware is able to meet performance requirements of the installed Operating System (OS). It usually includes a Global Positioning System (GPS) receiver for the navigation and a Subscriber Identification Module (SIM) card for the mobile connection. Its control can be fully touchscreen integrated depending on the design of the concerned brand and car type. This control integration tendency supports the cost reduction by removing the hardware buttons and switches. Since the head units by now can implement a hypervisor and can run several OS, the software architecture became hierarchical and complex. This aspect is becoming essential, as the safety critical part of the OS has to be free from interference with other non-safety critical parts of the OS or other OSs. The architecture of future IVI systems will be modular to comply with the technical complexity and the increasing number of the software suppliers. This sort of modularity will demand mature development processes as in the design phase as well as in the integration phase. The control panel (5) is placed in the center console and interconnected with the head unit. Even though the increasing number of features integrated in and controlled by the head unit, lots of Original Equipment Manufacturers (OEM) keep this block, as this is the easiest and safest to use controlling components while driving. It is usually pure electronics, fully integrated component and therefore has no demanding requirements for the system and the software level development processes. The microphones and speakers (6) are the general audio components of the IVI. Their importance and the concerning requirements on the reliability and the quality are increasing as voice recognition features develop. At this stage, the speakers generally have a significant role in the driver warning part of the safety concept.

DRIVING AUTOMATION

SAE J3016 – Levels of driving automation

Program managers and vehicle level designers have to make decisions on the level of the vehicle driving autonomy from the concept phase of the development. In order to provide a common terminology for the industry, the Society of Automotive Engineers (SAE) International issued the J3016 standard. [4] The standard defines six levels of driving automation as per Table 1. It shows the responsibility of the environment monitoring and the driving at each level. Level 0 refers to the lowest level of automation, meaning there is no driving automation at all. Level 5 refers to the highest level of automation, meaning full autonomy. At this level both the environment monitoring and the driving functions are carried out by the system under any circumstances. It means, that there is neither pedals nor steering wheel in the vehicle.

Level	Environment monitored by	Driver	Example
0	Human	Human	Lane departure warning
1	Human	Human	Lane centering OR adaptive cruise control
2	Human	Human	Lane centering AND Adaptive cruise control same time

Level	Environment monitored by	Driver	Example
3	System	Human OR System	Traffic jam chauffeur
4	System	System	Local driverless taxi
5	System	System	Same as Level 4 but in all conditions

Table 1: SAE J3016 Levels of driving automation

Advancement of the autonomous driving technology

Gartner hype cycle [5] is a visual representation of the advancement, adoption and application of different emerging technologies. It was developed and introduced by the research and Information Technology (IT) firm Gartner Inc. The hype cycle has been used by Gartner since 1995. Figure 2 shows the hype curve with its dedicated phases and the positions of Autonomous Driving Level 4 and 5 in 2019.

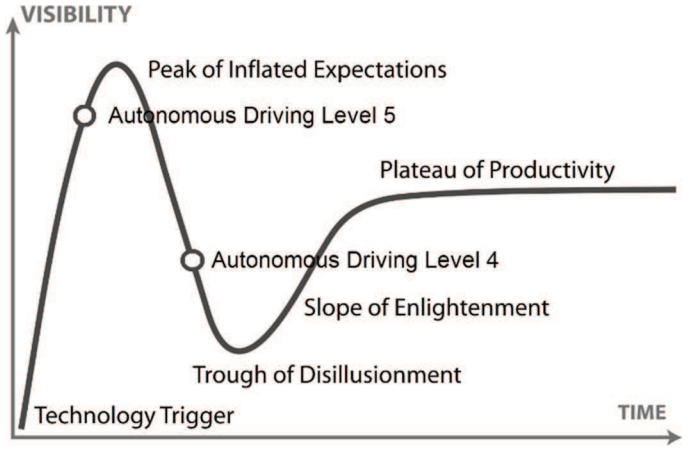

Figure 2: The hype cycle

The horizontal axis represents the time with no definite scale. The vertical axis represents the visibility of the individual technologies, also with no definite scale. The main purpose is to show the actual position of the individual technologies and their relative positions. The positions of the technologies can be compared to their positions in the previous years. The advancement of the technologies along curve can be varying. Some technologies simply disappear before reaching the Plateau of Productivity. Some technologies are not recognized in the early phases. Anyway, the autonomous driving technologies have been in the highlight of the researchers, the automotive developers as well as the marketing sector. Therefore, there has been plenty of information available on this field. Table 2. lists and briefly describes the phases of the hype cycle.

No.	Phase	Description
1	Technology Trigger	The initiation of a potential technology breakthrough. Early concepts can trigger significant publicity. Usable products no necessarily exists. Business model is unproven.

No.	Phase	Description
2	Peak of Inflated Expectations	Early publicity start delivering news on failures besides the success stories. Some companies take action; most don't
3	Trough of Disillusionment	Interest drops as implementations fail to be proven. Several technology developers quit. Investment continues only for the products meet the requirements of early adopters.
4	Slope of Enlightenment	Successful concepts outline sustainable business models. The technology becomes more understood. New generation products arise from survivor technology developers. More enterprises fund pilot projects. Conservative companies remain cautious.
5	Plateau of Productivity	Mainstream adoption starts increasing. Supplier assessing criteria become more established. Broad market applicability and relevance are clearly paying off. If the market size is big enough than the technology can further grow.

Table 2: The phases of the hype cycle

As per the 2019 hype cycle the autonomous driving level 4 technology is well over the Peak of Inflated Expectations period and is getting close to the bottom of the Trough of Disillusionment phase. Perceptions with regard the autonomous driving can change quickly. The speed of the autonomous driving technology development directly depends on other technologies such as sensors, Three-Dimensional (3D) sensing cameras, Artificial Intelligence. Fatal road accidents of self-driving cars can significantly slow down the social acceptance of the technology. According to Gartner's study, neither Level 4 nor Level 5 will not reach the Plateau of Productivity in ten years.

SMDR categorization system

For some problems, the standard categorization of levels of driving automation cannot cover each aspect in the consideration. For analyses of highly automated and connected road vehicles, IT security also has to be taken into account. In such case, a specific Storage-Maintenance-Driving-Routing (SMDR) [6] categorization can be applied as per Table 3. The SMDR categorization was developed at Óbuda University, Budapest, Hungary.

Categories	Category S	Category M	Category D	Category R
Abstract category	Property	Thing	Relation	Control
Aspect of vehicle	Storage in vehicle	Technical operation	Moving the vehicle	Traffic control
Problem	**Storage**	**Maintenance**	**Driving**	**Routing**
Level 1	Objects	Traditional maintenance	Traditional driving	Static routing
Level 2	Creatures, special objects	Controlled maintenance	Controlled driving	Dynamic routing
Level 3	Humans	Periodic maintenance	Automatic driving	Central routing
Level 4	Hazardous material	Automatic maintenance	Convoy driving	Community routing

Table 3: SMDR categorization of automated vehicles

THE AUTOMOTIVE CONTEXT

Production Volume

The number of the produced cars is by order of magnitudes higher than that of other safety critical systems, e.g. power plants or airplanes. Any critical problem resulting in a recall of a car type can cost a lot for the OEM. On the other hand, the big car factories require huge investments, which can return in decades only. Therefore, the industry is traditionally very cost sensitive, setting extremely tight budget for the development.

Supply Chain

The supply chain extends around the globe and is very complex. The responsibility sharing between the parties is based on actual contracts, but the players have to comply with the global quality standard IATF16949 [7] by International Automotive Task Force. Taking into account the increasing number of the software suppliers, the standard requires the software suppliers to build competency to carry out self-assessments on their own software development processes.

Technical complexity

The complexity of the in-vehicle communication network continuously increased as many new Electronic Control Units (ECU) were implemented and connected to the vehicle Controller Area Network (CAN). The volume of the software implemented in the ECUs boomed along with the number of required features and the performance of the electronics hardware. A new premium car has over 100 million Lines of Code (LoC). As a comparison, a Boeing 787 has 3 million or less LoC. [8]. Such level of complexity raises specific requirements on the architectural design (at the system, software and hardware level), on the component interface specification, on the related integration test specification as well as on the actual integration process.

Vehicle lifecycle

The OEMs traditionally have a very conservative approach on the verification and the validation of new technologies. For that reason, OEMs want to see a product with fully validated feature set by the Start of Production (SoP) This is a reasonable requirement to reduce the risk of a recall campaign. On the other hand, IVI systems have an increasingly stronger customer requirement to be able to add new system features after the SoP. The vehicle domains are more depending on the actual hardware, e.g. chassis, power line, usually can't be upgraded with new features. The developers therefore will have to specify hardware that is more powerful and a properly modular software architecture. Taking also into account the increasing technical complexity, the full system validation before SoP is getting a bigger challenge. This is also an important area, where OEMs and the IVI software suppliers will have to come to a compromise. Some features might be released with a lower but still reasonable level of validation and might be upgraded based on the field experiences. Tesla cars are already able to remotely update its software accordingly. [9]

Cultural differences

Due to the implementation of the direct User Interface (UI) the IVI is unique among the other vehicle domains. It is feature rich compared to the chassis or the power line domain. Since the UI is always, an essential part of the vehicle's level safety concepts, the developers have to take into account the target market cultural background. Developers

working for global markets have to develop competence to deal with this aspect, which is time demanding for the organization.

Personalization

Mobile users are used to their phone's personal settings and want to keep using the familiar UI while driving or travelling in a car. Therefore, the IVI UI has to be able to dynamically adjust to the driver's and the passengers' device settings. The trend of car-sharing [10] strengthen the requirements on personalization. This aspect creates information security requirements too for the system, e.g. authentication, authorization, and accounting (AAA). [11]

Information security

Future autonomous cars will continuously monitor the environment and send information to the cloud where High Definition (HD) maps [12] will be created and maintained. The HD maps will be an integrated part of the traffic and logistics infrastructure, which is considered as critical infrastructure. In the same time, road vehicles will download HD map data to feed their navigation functions. Compromising the map providers IT system can have the potential to lead to hazardous driving situations for individual vehicles, as well as to traffic system level incidents. The in-car communication network can also be compromised via the IVI system, which can lead also to hazardous driving or traffic situations. The root cause of the security gap can be either a focused hacking or a malfunction of the UI integrating IVI system. Thus, developers have to analyze the IVI system's malfunction root causes from information security point of view. Vice-versa, the IVI system malfunctions have to be considered as root cause of security gaps.

Newcomers in business

With the integration of System on Chip (SoC), quality displays and high-performance Graphics Processing Units (GPU) global, originally non-automotive OS providers, e.g. Google and Apple, and several small software component developers appeared in the market. These companies have no traditional automotive background. This cultural gap is a big challenge to fill for each party. The software suppliers will have to adopt to the automotive quality standards. For software suppliers the Automotive Software Process Improvement and Capability dEtermination (ASPICE) [13] became the leading standard on the development processes. On the other hand, the OEMs tend to adopt agile software development methods, e.g. Scaled Agile Framework (SAFe) [14] at the different organizational levels. This is also an area, where the partners along the whole supply chain will have to come to a compromise.

FUNCTIONAL SAFETY STANDARDS

ISO26262 Road vehicles – Functional safety

The society and the authorities want to see a continuously decreasing trend in the number of car accidents. The inappropriately low level of safety can result in a recall with financial, legal as well as reputational consequences. In order to reduce such risks rooted in the malfunction of safety critical systems the International Organization for Standardization issued the functional safety standards for road vehicle ISO26262 in 2011. The standard purposes listed below:

- provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases;
- provides an automotive-specific risk-based approach to determine integrity levels Automotive Safety Integrity Levels (ASIL) [15]

Table 4 summarizes the ASILs. ASIL Quality Management (QM) refers to the lowest level of safety criticality and ASIL-D refers to the highest level of safety criticality. In the second column vehicle level functions listed as per their usually applied ASIL;

ASIL	Example
QM	Movie and game systems
A	Connectivity, GPS, navigation system
B	Instrument cluster, steering wheel sensor
C	Stability control, valve control
D	Braking, electronic power steering

Table 4: Automotive Safety Integrity Levels

- uses ASILs to specify applicable requirements of ISO 26262 so as to avoid unreasonable residual risk;
- provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved;
- provide requirements for relations with suppliers.

ISO/PAS 21448 Road vehicles — Safety of the intended functionality

The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons is referred to as the Safety Of The Intended Functionality (SOTIF). [16]

The standard provides guidance for the design, verification and validation activities necessary to achieve the safety of the intended function. It is important to note, that this standard does not cover the faults addressed by ISO26262 or hazards caused by the system. This standard is meant to be applied to intended functionality where situational awareness is critical for safety. Situational awareness is essential for emergency system functions (e.g. emergency brake) and Advanced Driver Assistance Systems (ADAS) at Levels 1 and Level 2. The standard can also be taken into account for higher levels, but further measures might need to be applied. Measures defined in the standard can be used for the development of innovative functions, where situational awareness is based on complex sensor data and processing algorithms. The standard considers intended use and foreseeable misuse combined with hazardous system behavior during hazardous event identification. Intentional misuse of the system is considered feature abuse. Such sort of abuse is not in the scope of the standard.

SAFETY INTEGRITY LEVEL

According to the automotive functional safety standards, the system safety topic has to be considered throughout the whole lifecycle of the vehicle. The interactions between the

vehicle and the environment has to be assessed and documented by certified safety specialists of OEMs during the concept phase in the Hazard Analysis and Risk Assessment (HARA) The outcome of the assessment will determine the ASIL for each considered hazardous event. The standard's guideline on severity classification considers damages caused to the vehicle, the passengers and pedestrians. In some situations, these damages can be significantly lighter than the resulting losses caused by a severe traffic jam, mainly in dense urban areas. The more automated driving features will be implemented in vehicles the driver more will be used to them. For example, sound effects and streamed video on the head unit assist drivers during reverse driving or emergency breaking. At this stage the controllability of the driving scenarios where such driving assisting systems or warning messages are unavailable are considered generally controllable. Due to the lack of driving experience with no driving assisting features the controllability specification guideline will need to be reviewed. The unavailability of warning messages at high speed, e.g. on motorway can have the potential to lead to hazardous situations classified with higher severity. Navigation solutions assist drivers in route planning, battery management of electric vehicles and charging station finding. Due to the loss of GPS signal or connection to a cloud-based navigation can lead to hazardous situations higher than ASIL QM. In case of fully autonomous cars (Level 5) the communication between the driver and the vehicle is essential. The driver must be able to instruct the vehicle under any condition. The combination of these changes will necessarily lead to the increase of ASIL of IVI functions.

CONCLUSION

The technical complexity and the performance of the In-Vehicle-Infotainment systems continuously increasing. Due to the safety and security requirements, developing reasonably reliable systems requires to follow standard processes throughout the whole vehicle lifecycle. The higher level of automation applied in a vehicle, the higher level of ASIL will be assigned to In-Vehicle-Infotainment systems. In order to meet reliability requirements SOTIF and information security also have to be applied from the concept phase of the vehicle lifecycle. Critical infrastructures including or interacting with autonomous road vehicles, e.g. road traffic, logistics, info communication systems, electric car charging stations, emergency services will have to be prepared for integrating autonomous road vehicles. The experts of the concerned infrastructures should be involved in the hazard analysis, the risk assessment and the safety concept's verification activities.

REFERENCES

[1] N. Krausz, A. Csepinszky, V. Potó, Á. Barsi, "Az autós térképtől az önvezetésig: a járműnavigáció története," Geodézia és kartográfia, ISSN 0016-7118 , 2019. (71. évf.), 1. sz., 14-18 p.

[2] G. Meixner, C. Häcker, B. Decker, "Retrospective and Future Automotive Infotainment Systems - 100 Years of User Interface Evolution" in Automotive User Interfaces, Springer International Publishing, 2017, ch 1, pp 3-53

[3]"*Passenger car In-Vehicle-Infotainment system*" NNG Lld, https://www.nng.com/nng-ux-atlas, 2020

[4] Levels of driving automation, SAE J3016, Society of Automotive Engineers International, USA, 2016.
[5] K. Panetta, „5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies,“ https://www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019, Gartner Inc, 2019.
[6] Albini, D. Tokody, Z. Rajnai, “The Categorization and Information Technology Security of Automated Vehicles Hybrid Navigation” Interdisciplinary Description of Complex Systems 16(3-A), 2018, 327-332.
[7] Development of products with embedded software, IATF16949:2016 8.4.2.3.1, Quality management system for organizations in the automotive industry, International Automotive Task Force, 2016.
[8] “How much code?” Cars, https://codeinstitute.net/blog/much-code-cars/, 2019.
[9] “Software Updates” Tesla Inc, https://www.tesla.com/support/software-updates, 2019.
[10] B. Schlag, L. Rößger, “Car sharing - Motive und Intentionen,” Reportpsychologie (45), 2, Germany, 2019, 10-19,
[11] Ueda, H, Kurachi, R, Takada, H, Mizutani, T, Inoue, M, Horihata, S, “Security authentication system for in-vehicle network,” SEI Technical Review, Number 81, 2015, 5-9
[12] Barsi, V. Poto, A. Somogyi, T. Lovas, V. Tihanyi, Zs. Szalay, “Supporting autonomous vehicles by creating HD maps,” Production Engineering Archives 16, Poland, 2017, 43-46.
[13] Automotive SPICE v3.1, Qualitäts Management Center im Verband der Automobilindustrie (VDA QMC) Working Group 13 / Automotive SIG, 2017.
[14] Scaled Agile Framework, Scaled Agile Inc, USA, https://www.scaledagileframework.com, 2019.
[15] “Concept phase”, ISO26262:2018 Part 3 Road vehicles — Functional safety, International Organization for Standardization, ISO/TC 22/SC 32, 2018.
[16] “Safety of the intended functionality,” ISO/PAS 21448 Road vehicles, International Organization for Standardization, ISO/TC 22/SC 32, 2019.