TTTP

DOI: 10.7251/JTTTP2402117K
UDC: 656.1.022:338.486.1.02

PROFESSIONAL PAPER

ISO 26262 Functional Safety Systems for Road Vehicles

Mehmed Konaković, dipl. ing. saob.
JU "Centar za napredne tehnologije u Sarajevu", Internacionalni Univerzitet Travnik u Travniku, Saobraćajni fakultet Travnik u Travniku, konakovicmesa@hotmail.com

Abidin Deljanin, dipl. ing. saob.
Internacionalni Univerzitet Travnik u Travniku, Saobraćajni fakultet Travnik u Travniku, adeljanin@hotmail.com

Received: May 31, 2024
Accepted: September 23, 2024

Abstrakt: The dynamics in the global automotive industry are constantly evolving, opening pathways to new markets and technological paradigms. Advancements such as H2 and e-vehicles present clear opportunities but also entail challenges of uncontrolled development, particularly with the growing influence of China in the EU.

Traffic accidents involving vehicles with electric propulsion pose specific challenges for investigators and analysts. Analyses reveal increased complexity and harmfulness of these accidents, emphasizing the need for new methods of investigation and damage assessment, as well as for tightening regulations.

The production of e-vehicles faces financial challenges and technological demands. Production efficiency, including the use of one-piece chassis panels, is crucial for competitiveness in the market. The future of the automotive industry in the EU requires complex strategies focused on the development of e-vehicles for urban needs, H2 technology for freight trucks, and alternative fuels to ensure energy independence. Traffic safety is gaining importance, recognizing energy as a key factor in global security. Attitudes of countries like the Netherlands towards e-vehicles vary, with the issue of electric energy availability highlighted as significant. In this complex landscape of the automotive industry, contemplating the future requires a balance between technological innovation, safety, and sustainability.

Keywords: e-traffic, technological curve, energy, renewable sources, independence

JEL: Q2, Q3, Q4 and Q5 - stručni članak.

ISO 26262

ISO 26262 is an international standard titled "Road vehicles – Functional safety," representing a norm for the functional safety of electrical and/or electronic systems implemented in road vehicles. This standard was adopted by the International Organization for Standardization (ISO) in 2011 and revised in 2018. Functional safety characteristics are integral to every phase of vehicle development, from specification to design, implementation, integration, verification, validation, and production release. ISO 26262 defines functional safety for vehicle equipment applicable throughout the lifecycle of electronic and electrical safety systems. The primary goal of the standard is to address potential hazards caused by faulty behaviors of electronic and electrical systems as a whole, their components, or mechanical subsystems. This is a risk-based safety standard, involving continuous qualitative risk assessment of failure occurrence and determination of safety measures to avoid and control systematic failures, as well as to treat random hardware failures or ultimately mitigate the harmful consequences of failures.

The standard regulates the safety lifecycle of automobiles in phases of management, development, production, operation, service, and decommissioning. It standardizes the development process from requirement specifications, design solutions, implementation, integration, verification, validation, and configuration. In line with the specificities of the automotive industry, it standardizes the determination of risk classes (Automotive Safety Integrity Level - ASIL). The analysis of the automotive safety integrity level indirectly determines the necessary safety requirements, ensuring the acceptability of residual risk. It ensures an adequate level of safety by creating conditions for the required validation and confirmation measures.

The content of ISO 26262:2018 is structured into 12 chapters as follows: Vocabulary, Functional Safety Management, Concept Phase, Product Development at the System Level, Product Development at the Hardware Level, Product Development at the Software Level, Production, Operation, Service, and Decommissioning, Supporting Processes, Automotive Safety Integrity Level (ASIL) Oriented and Safety Oriented Analysis, Guidelines for ISO 26262, Guidelines for the Application of ISO 26262 to Semiconductors, and Adaptation of ISO 26262 for Motorcycles.

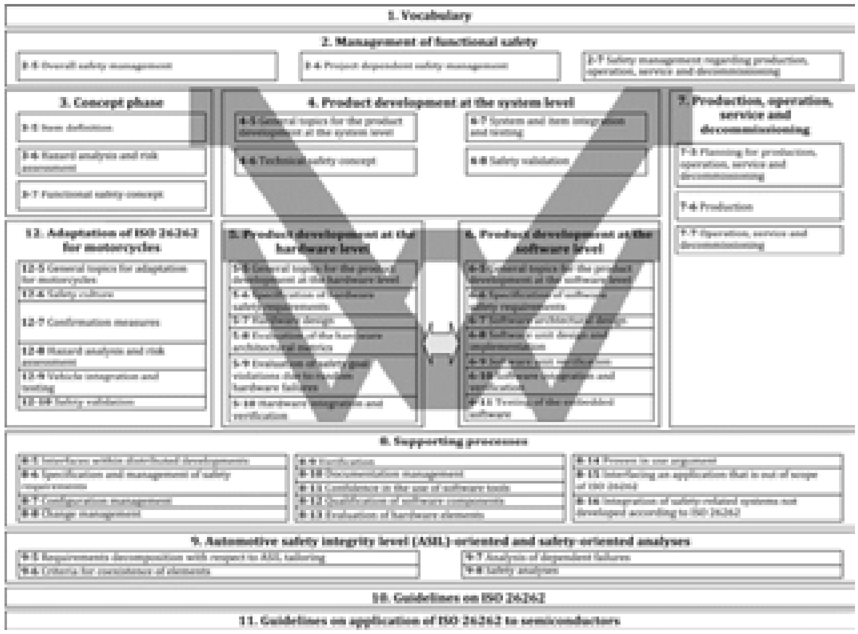

Figure 1. Overview of the ISO 26262 Structure (Source: ISO online platform)

Glossary - ISO 26262 provides a project glossary of terms, definitions, and abbreviations such as:

- item - an individual part or detail referred to by the term,
- element or system - a part or assembly with one or more hardware/software units,
- fault - identified condition that deviates and may cause a failure,
- error - deviation from the calculated or measured correct value or state,
- failure - cessation of proper behavior of an element due to an error,
- fault tolerance - capability to perform despite the presence of error(s),
- malfunction - is a failure,
- hazard - defines a state of real possibility of harm occurrence,
- functional safety - identifies the absence of unreasonable risk due to hazards caused by malfunctioning of electrical and electronic systems.

Functional safety management for vehicle applications is defined as organizational safety management, and standards for safety lifecycle in vehicle development and production.

The safety lifecycle according to ISO 26262 identifies and assesses hazards (safety risks), establishes safety requirements to reduce risks to an acceptable level, and manages and monitors safety requirements, ensuring their fulfillment in the product. These processes are treated as integrated or parallel to the quality management system, and they include:

- Identification of item (specific automotive system product),
- Definition of top-level system functional requirements for each item/position,
- Identification of a broad set of hazardous events for each item/position,
- Determination of the appropriate ASIL for each hazardous event,
- Establishment of safety goal and ASIL for each hazardous event,
- Functional safety defines the system architecture to achieve safety goals,
- Filtering of safety goals and renaming into lower-level safety requirements,
- Each safety requirement inherits the ASIL of the higher requirement/goal, but reduction is possible,
- Assignment of safety requirements to subsys-

Table 1: Safety lifecycle according to ISO 26262

Concept	Meaning
Unsafe event	The hazard at the vehicle level and the vehicle's operational situation that may lead to an accident if not timely controlled by the driver.
Safety goal	Highest safety requirement - reduces the risk of hazardous events to an acceptable level
Automotive safety integrity level (ASIL)	The classification of safety goals, as well as validation and confirmation measures in accordance with the standard, ensuring the achievement of that safety goal
Safety requirements	All safety goals from the highest to the lowest, including the levels of functional and technical safety requirements assigned to hardware and software components

(Source: Author)

tems, hardware, and software components in accordance with standards and processes for the highest ASIL, and
- All components of the developed architecture are developed in accordance with assigned safety (and functional) requirements.

Support processes are established to provide support for the safety lifecycle processes. They are active in all phases and include:
- Control and collective analysis aimed at achieving goals, requirements (dispersed development and production),
- Precise specification of safety requirements and their management,
- Product control, their repeatability in series with the possibility of identifying changes,
- Change management including impact on safety requirements,
- Planning, control, reporting, analysis, and testing,
- Planned identification and management of all documentation,
- Software reliability and software tool suitability,
- Qualification of developed software and hardware components for integration into the developed ASIL item/position, and
- Service history analysis aimed at proving quality.

The Automotive Safety Integrity Level (ASIL) analysis is an assessment of risk reduction to the level necessary to prevent hazardous events or hazards. In the automotive industry, a set of risk reduction assessments has been developed, classified into a safety risk classification in the automotive system or its elements, ranging in size from the smallest (D) to the highest (A). By assigning an appropriate goal for addressing a specific hazard to each risk, a safety requirement arises.

Quality management is achieved when all assessed risks are tolerable. For example, in the case of a requirement for a vehicle to start, no safety processes are needed, only a standard quality management procedure, etc

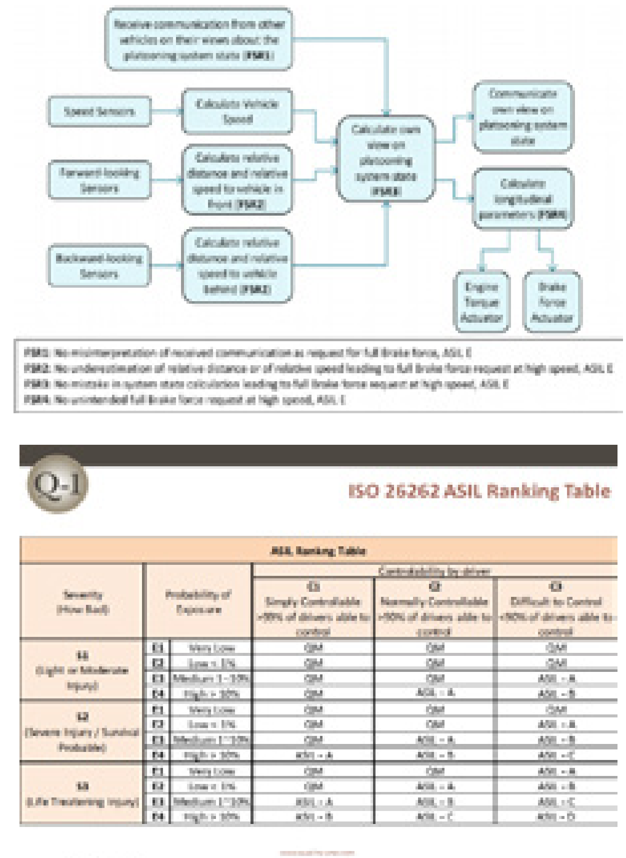

Figure 2: ASIL Functioning Scheme (Source: ISO online platform) / Overview of ASIL Ranking and Guidelines (Source: Q-1 Portal, January 20, 2024)

Table 2: Overview of assessments for determination ADSL

Severity of hazard (S)	Exposure (E)	Controllability (C)
S0 – no injury	E0 –minimal probability	C0 –general control
S1 –minor and moderate injuries	E1 - very low probability	C1 - easily controlled
S2 –with severe and life-threatening injuries	E2 - low probability	C2 –normally controlled
S3 –life-threatening to fatal injurie	E3 - medium probability	C3 –difficult to control/not contr.
	E4 - high probability	

Table 3: Hazard Classification

CLASS	EXPLANATION	NOTE
D	Lowest level of life-threatening risk	Loss of braking on all wheels
C	Level of life-threatening risk	Loss of braking on rear wheels and the like
B	Difference between C and B with the largest step and possible injuries	Loss of lights, brake signals …
A	Lowest risk of injury/hazard	Example: malfunction of brake lights

(Source: Author)

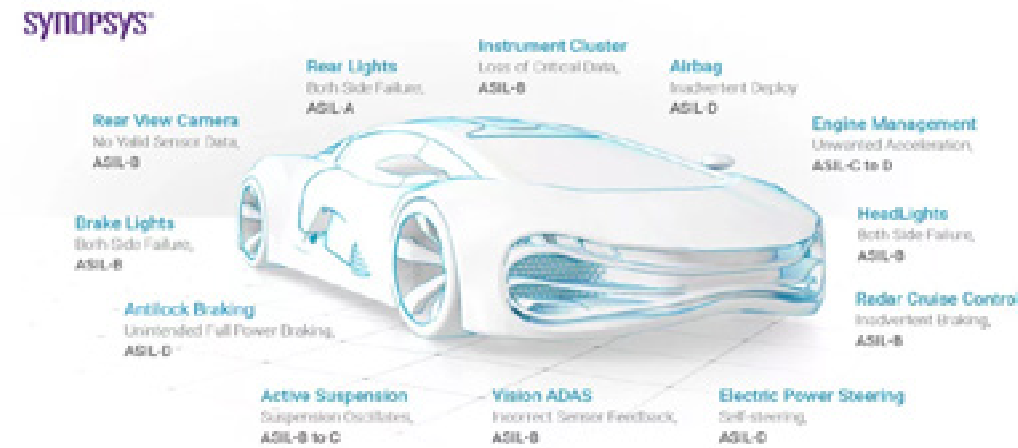

Figure 3: ASIL/Sensor Scheme (Source: Synopsys website, October 10, 2023)

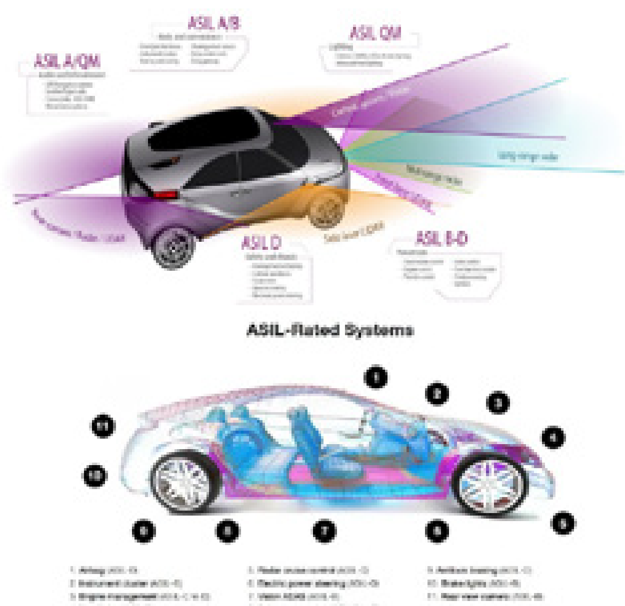

Figure 4: ASIL/Sensor Scheme (Source: Gary Hilson, EET Asia, 'ford', October 10, 2023)

For electric vehicles, ASIL is implemented after the highest safety criticality is assigned to the electric motor drive and battery management system. Alongside the drive train, airbags, anti-lock brakes, and power steering require an ASIL-D rating. This represents the highest level of stringency applied to safety because the risks associated with their failure are the greatest. Conversely, components such as rear lights require an ASIL-A rating. Headlights and brake lights would generally be ASIL-B, while cruise control would typically be ASIL-C.

It's significant that ASIL differs between electric and conventional vehicles, and it raises the question of the magnitude of hazards present in different types of vehicles. It's important to understand which vehicle and which subsystem in the vehicle pose or, under certain circumstances, cause greater destruction, damage, and endangerment. ASIL is a younger standard, so there is ongoing debate about its qualities or significance compared to other standards that have been in use for a longer period. It should be concluded that all standards must be applied, and there are always situations where

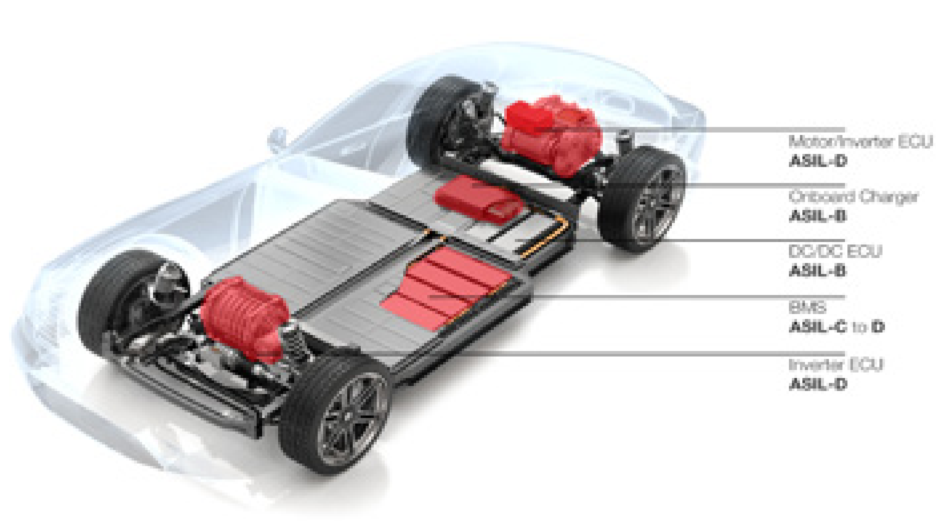

Figure 5: Schematic Overview of ASIL Ratings for Electric Vehicles (Source: https://info.typhoon-hil.com, February 20, 2024)

Table 4: Comparative Standard Overview

Approximate Mapping of ASIL Across Domains							
Domain	**Safety Levels Specific to the Domain**						
Cars (ISO 26262) (ASIL)	QM		A	B	C	D	-
General (IEC 61508)	-		SIL-1	SIL-2		SIL-3	SIL-4
Railway CENELEC 50126/128/129)	-		SIL-1	SIL-2		SIL-3	SIL-4
Space (ECSS-Q-ST-80)	Kasa E		Klasa D	Klasa C		Klasa B	Klasa A
Aviation: air (ED-12/ DO-178 / DO-254)	DAL-E		DAL-D	DAL-C		DAL-B	DAL-A
Aviation: land (ED-109/DO-278)	AL6		AL5	AL4	AL3	AL2	AL1
Medicine (IEC 62304)	Klasa A			Klasa B		Klasa C	-
Household (IEC 60730)	Klasa A			Klasa B		Klasa C	-
Machines (ISO 13849)	PL a	PL b	PL c	PL d		PL e	-

(Source: https://en.wikipedia.org/wiki-ASIL, 20.10.2023.)

the response to certain risks is at least controlled or tested in relation to one of the earlier established norms.

ISO 26262 is an international standard that pertains to functional safety in the automotive industry. It plays a crucial role in enhancing traffic safety in Europe by providing a framework and guidelines for the development of secure electronic systems in automobiles.

ANALYSIS OF FACTORS INFLUENCING TRAFFIC SAFETY SYSTEM

Although there is an apparent correlation between the implementation of standards such as ISO 26262 and the state of traffic safety, precisely quantifying the impact of these standards on the number of traffic accidents in Europe can be challenging. This is because the factors influencing traffic safety are diverse, including infrastructure, regulations, driver behavior, and others. However, there are several ways to analyze the impact of implementing standards like ISO 26262 on traffic safety:

- Vehicle performance analysis: A detailed analysis of the performance of vehicles developed in accordance with standards like ISO 26262 can be conducted. This would involve investigating accident cases involving vehicles that were or were not compliant with the standard.
- Statistical data analysis: Trends in reducing the number of traffic accidents after standards such as ISO 26262 are introduced or applied on a broader scale can be explored.
- Comparative study with other regions: Comparing the safety performance of vehicles and the number of traffic accidents in Europe with other regions that may not be as focused on the implementation of these standards can provide some insight.
- Surveys and opinion research: Conducting surveys among drivers and other traffic participants can provide information on the perception of vehicle safety.

Intelligent safety systems in vehicles, whether equipped with new or conventional technologies, play a crucial role in improving the safety of drivers, passengers, and other traffic participants. Key intelligent safety systems in modern and conventional vehicles include:

a. Collision avoidance system - using sensors such as radar, cameras, and lidar to detect vehicles, pedestrians, or obstacles in front of the vehicle,
b. Lane departure warning system - using cameras or sensors,
c. Distance maintenance system - using radar or cameras to assess the distance between vehicles and automatically adjust speed or activate brakes to maintain a safe distance from the vehicle in front,
d. Driver fatigue recognition system - using sensors to monitor the driver's behavior, such as steering wheel position or eye movements, to detect signs of fatigue or lack of attention,
e. Blind-spot detection system - using sensors mounted on side mirrors to detect vehicles in the driver's blind spot,
f. Automatic pedestrian braking system - using sensors to recognize pedestrians in front of the vehicle and can automatically activate brakes to avoid a collision or reduce severity.

These are just some of the intelligent safety systems in modern and conventional vehicles. Their combination provides additional protection and contributes to reducing the number of traffic accidents and injuries.

CLASSIC AND NEW TECHNOLOGIES

The global strength and power of the automotive industry in Western Europe and America have been in the development and production of internal combustion engines. In this economic capacity, giants like BMW, Mercedes-Benz, Ford, Honda, etc., have emerged. Civilization and cooperation enable advanced technologies to become practically a "household activity." The possibility of exchanging information and collaborating on a free basis has laid the foundation for the development of new forces from India, China, Thailand, etc. The European Union, as a global player in environmental protection and standardization, has had clearly defined policies to cease the production and sale of vehicles emitting CO2 by the year 2035. However, in today's world, due to the aforementioned facts, it is clear that electric vehicles can be made by anyone. Production from a garage to mass production is possible. The best example is Mr. Rimac in Croatia. In such a situation, it has happened that the markets of EU and America are flooded with Chinese vehicles that are technologically advanced and cheap.

As a measure of protection, the European Parliament has approved the Commission's proposal that Chinese electric vehicles should not be considered climate neutral. In the transport business, this regulation leaves a mark because all companies in Europe must report the CO2 footprint for their services by rail, road, or air. This is a complex issue due to the obligation to calculate the actual parameters of CO2 emissions in the use of electric energy. According to these protocols, it turns out that gasoline and diesel are more favorable for use than electric energy, and this is due to the way electric energy is produced. In terms of environmental protection, there is actually a relocation of pollution sites. Namely, the greatest pollution occurs at the location of electric energy production.

Electric vehicles (EVs) are becoming increasingly popular as an alternative to vehicles with internal combustion engines (ICE) due to their potential cleanliness and efficiency. In this work, we conduct a comparative analysis between these two types of vehicles to understand their advantages and disadvantages.

Comparative analysis shows that both E-vehicles and SUS vehicles have their advantages and disadvantages. The final choice depends on individual needs, preferences and local conditions. The new e and H2 vehicle technologies represent innovative approaches that are increasingly being used to reduce emissions and improve energy efficiency in the automotive industry.

These options represent an alternative to traditional internal combustion engine vehicles and aim to reduce greenhouse gas emissions and other harmful emissions in transportation. Key requirements in the development of these technologies include efficiency, reliability, safety, and cost-effectiveness to become widely accepted and competitive in the market.

Intelligent safety systems for electric (e) and hydrogen (H2) propulsion vehicles bring a range of challenges that differ from traditional internal combustion engine vehicles. Specific safety challenges of new e and H2 technologies include:

1. High voltage and electrical safety: Electric vehicles use high-voltage systems to power electric motors. There is a risk of electric shock to passengers and personnel in the event of an accident or damage to the high-voltage system. Therefore, passenger and personnel safety is necessary through adequate insulation, safety switches, and first aid training.
2. Battery fires and explosions: Lithium-ion batteries used in electric vehicles can be susceptible to overheating and fires in the event of a malfunction or damage. This challenge requires the development of overheating detection systems, fire suppression, and procedures for safe handling of damaged vehicles.

Table 5: Analysis of Techno-Economic and Environmental Characteristics

Element	EVs	ICE Vehicles
Propulsion	Electric motor powered by battery	ICE - gasoline or diesel engine
Performance	Higher acceleration and torque at lower speeds	Longer range on a single fueling and can refuel quickly
Emission	Do not produce direct emissions at local level	Produce exhaust gases that can be harmful to the environment
Price	More expensive to purchase and lower operating costs due to cheaper charging	Usually cheaper to purchase but higher fuel and maintenance costs
Accessibility	Subsidies and incentives - facilitations	Greater availability in most markets
CO2 Emission	Depending on the method of electricity production, lower carbon footprint	Have a higher carbon footprint due to burning fossil fuels
Sustainability	With renewable energy sources for charging - more environmentally friendly	Dependence on fossil fuels makes them less sustainable in the long run

Table 6: Characteristics and Requirements of Electric and H2 Technologies

System Elements	Electric Vehicles	Hydrogen Vehicles
Propulsion	Instead of traditional ICE engines, EVs use electric motors powered by electricity from batteries	Hydrogen vehicles use hydrogen, which, in reaction with oxygen in fuel cells, produces electricity to power the vehicle
Energy/Power Source	Efficient, long-lasting batteries are key to the performance of electric vehicles	In order to provide vehicles with adequate power and performance, fuel cells must be efficient, reliable, and cost-effective
Charging Infrastructure	Development of fast chargers and expansion of charging networks that must be accessible, reliable, and efficient	Hydrogen vehicles require hydrogen refueling infrastructure (production, storage, distribution)

(Source: Author)

3. Hydrogen safety: Hydrogen is a flammable gas, so there is a risk of fire or explosion in the event of a hydrogen leak or vehicle collision. It is necessary to ensure safe hydrogen storage, transportation, and handling systems, as well as leak detection systems and procedures for rapid evacuation in case of danger.
4. Charging infrastructure: Lack of charging infrastructure can present a safety challenge as drivers may be forced to use alternative, possibly less safe, charging methods. Inadequate maintenance or poorly designed charging stations can also pose risks of electrical or chemical accidents.
5. Crash safety: Since e and H2 vehicles use different propulsion systems and construction from traditional vehicles, there is a need to adapt safety systems in the event of a crash. This includes adaptive active and passive safety systems to ensure optimal protection for passengers and vehicles in various crash scenarios.

ISO 26262 contributes to addressing the challenges of manufacturing and using vehicles through functional safety in the automotive industry, i.e., through risk analysis, detection and diagnostic system, and error resilience. It provides a framework and guidelines for identifying, analyzing, and managing functional safety risks in vehicles, which can help address some safety challenges associated with e and H2 technologies. The fundamental contributions to addressing these challenges may include:

1. Risk analysis: This ISO requires risk analysis for all electrical and electronic systems in the vehicle, which can help identify hazards related to high voltage, battery fires or explosions in electric vehicles, as well as safety risks associated with hydrogen storage and handling.
2. Detection and diagnostic system: The standard requires the implementation of fault detection and diagnostic systems in electrical and electronic systems, which can help detect problems with batteries or hydrogen systems, etc.
3. Error resilience: ISO 26262 promotes the design of systems that are resilient to errors and can safely respond to faults or failures. This can help minimize the risk of electric shocks, fires, or explosions in electric vehicles, as well as manage the risks of hydrogen leaks or vehicle collisions.

CONCLUSION

Ecology, given its importance, is definitely a factor in traffic safety with a significantly dangerous impact on a broad scale. All measures taken since 2011, with the first publication of ISO 26262 and others, have yielded results. In the EU, there is a trend of continuous decrease in the number of fatalities by around 4.5% annually. Similar statistics are observed in Bosnia and Herzegovina. The number of electric vehicles is significantly increasing at a rate of about 12%.

ISO 26262 is not specifically tailored to all aspects of safety related to e and H2 technologies, so it may be necessary to combine ISO 26262 with other standards, regulations, and best practices relevant to these technologies, which is crucial for the successful proliferation of e and H2 technologies in the automotive industry and their acceptance by consumers.

Due to the growing economy and competition, Europe must focus on new technologies that offer various forms of powertrains or propulsion concepts, towards hydrogen technologies that have unparalleled advantages. Strategies must be flexibly set by defining goals and without imposing technological guidelines, ensuring the achievement of goals with optimal technological solutions and without delving into the details of specific technologies and industries.

Attention and resources need to be directed towards the development of other e-fuels, synthetic fuels that could provide an additional alternative, especially from the perspective of the vehicle lifecycle from production to use and recycling. This approach enables stability in the automotive industry, provides an opportunity for simpler solutions in traffic safety, and allows the introduction of new standards that will provide an opportunity for a safer environment and the continued development of civilization.

BIBLIOGRAFIJA

[1] A. Deljanin, F.Kiso: University textbook, “Evaluation Methods in Planning and Designing Transportation Infrastructure” Publisher: Faculty of Traffic and Communications, University of Sarajevo, 2017.
[2] Zavada J., „Vehicles“, Faculty of Transport and Traffic Sciences, Zagreb, 2000
[3] ISO 26262
[4] Pikula B., Justification of Electric and Hybrid Vehicle Use in Urban Areas, Sarajevo Green Design Conference, Sarajevo, 2012.
[5] Initiative ‘Resource-Efficient Europe’, European Parliament, Brussels, 2011.
[6] Initiative ‘Industrial Policy for the Era of Globalization’, European Parliament, Brussels, 2011.
[7] Initiative ‘Digital Agenda for Europe’, European Parliament, Brussels, 2011.
[8] Science and Technology, International University of Travnik, 2020-2022.
[9] https://hydrogeneurope.eu/
[10] http://eurokodovi.ba/
[11] https://www.bing.com/images , 29.05.2023.
[12] https://ec.europa.eu/eurostat
[13] https://en.wikipedia.org/wiki-ASIL, 20.10.2023.,
[14] https://info.typhoon-hil.com, 20.02.2024. g
[15] https://www.eetasia.com/, Zahtjevi ASIL D Pokretanje evaluacije memorije, Gary Hilson
[16] Portals: Sinopsys, Q-1, Ford, 20.01.2024.