BÁNKI KÖZLEMÉNYEK
2. ÉVFOLYAM 1. SZÁM

Applying Information Security Risk Management Standards Process for Automated Vehicles

Malak M. Shatnawi,
Óbuda University, Budapest,
PhD student in Doctoral School on Safety And Security Science
malak.shatnawi@phd.uni-obuda.hu

***Abstract*—Development of the transportation system is the main concern for each country, it provides a continual flow of goods, services and information's essential for the economic, security, safety, welfare, and to the health of its citizens. Transportation generally framed as a key component for progress, the sustainability dimensions represented by the social, economic, and environmental pillars have direct impacts on the cities and regions growth and prosperity which become the main challenge for all researchers and engineers because of the expansion of transportation networks.**

The rapid modern technology brought changes in all fields including road transportation and infrastructure and one of the most contemporary research subjects in transportation is the Automated Vehicles AV or Self Driven Vehicles SDV. The main challenges in the field of autonomous vehicles rest in the fact of improving road safety, minimizing accidents and human errors. It is known that road safety is a difficult issue including several fields to study such as human, vehicles, roads and socio-economic and environment factors.

This paper will focus in transportation, infrastructure and mobility risk management which seeks to make transportation system more efficient in term of safety, security, traffic accidents, security of data and information technology as well as software systems against malfunctions and all kinds of attacks. The aim of the paper is to discuss the challenges and threats faced in the development of the autonomous vehicles AV by studding information security risk management standard process, and explaining how applying the process of International Organization for Standardization (ISO), the concept of applying ISO 27005, to AV will be discussed here through certain processes.

Keywords: autonomous vehicles, Information security risk management, transportation, safety and security.

1 INTRODUCTION

In the domain of Automated Vehicles AV there are many different studies and recently transport research generally focuses on the implementation of intelligent transport systems (ITS), for example; how to develop roads and traffic for transport automation system with partially or fully autonomous vehicles, nowadays there are strong social, environmental and economic impact of the automotive industry as well as the whole transportation systems.

Moreover, in the near future self-driving cars will fundamentally reformulate road transportation inducing technological and socio-economic developments and requiring adaptation of the applicable laws and social acceptance as well. The framework is continuously change over time, i.e. future transportation design has to take into consideration technical, economic, legal, and social aspects simultaneously [1].

Software in AV has various roles: engine control, external communications, car safety and security, and from the point of view of security the primary aim is to build a cyber-safe system with regard to the vehicles, vehicle systems and intelligent infrastructure within the intelligent transport system [2].

The fully automated vehicle drives by itself without human supervision. Should system performance degrade, the vehicle is autonomously "restored to the system state of minimal risk." From a technical point of view, the greatest challenge lies in the complete absence of a human supervisor who knows the system limits, recognizes system faults and, where needed, switches the vehicle into a safe state, but what does a safe state consist of; can the driver take control within the exact needed time especially on highways these questions and more need to be tested, analyse and assess to identify the impact [3].

The main challenges in the field of autonomous vehicles will be discussed since in the next few years automated vehicles are going to radically change road transport infrastructure , improving road safety by removing human error from the driving equation, through testing and validation processes for new autonomous systems and features and through develop cost and time efficient methodologies [14].

Special attention must paid to the discussion of safety challenges that a self-driving electrical car project can encounter and the main outcomes and future research possibilities development [4].

In literature review presented in this paper we will bring the concept of AV with risk assessment and management and explaining how bringing the process of Risk assessment with NIST SP 800-30[9] and International Organization for Standardization (ISO), ISO 27000 standard itself defines the terminology of the series, ISO 27001 states the general requirements for an Information Security Management System (ISMS) General guide lines specify parts of the ISMS e.g., ISO 27005 specifies risk management [5].

2 LITERATURE REVIEW

2.1 Automated Vehicles

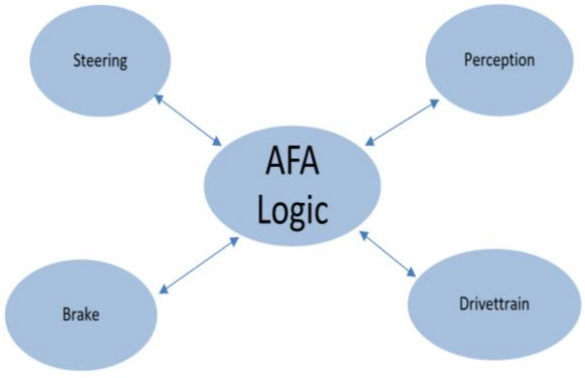
Society of Automotive Engineers (SAE) has described Automated Vehicles as "*autonomous vehicles or driverless, self-driving, or robotic cars or any vehicle operated without human supervision for motorway* " [14].

However, driverless cars definitions are varied from autonomous cars that are defined as versions of existing vehicles that are capable of taking over from the driver under certain circumstances, whereas driverless cars consider a more advanced next stage in development and usually lack steering wheel or pedals [1].

2.2 How Do Driverless Cars Work?

Lidar (light detection and ranging), radar, GPS, and computer are the backbone technology behind using driverless cars based on sensory data, with updated digital road maps processing that use the right path to follow with minimum risk of any obstacles that can face the car, processing information regarding the road signs and act accordingly, "*this allows the vehicle to adapt to changing situations, as well as travel through previously Unknown territories*" [6].

The National Highway Traffic Safety Administration (NHTSA) has helped to clarify policy and technical discussions around AVs by defining levels of automation as in the Figure below (NHTSA, 2013) [7].



1.Figure :Dependence of AFA Logic and connected elements

Source: Hazard Analysis and Risk Assessment for an Automated Unmanned Protective Vehicle (AFA is the German abbreviation), [8].

2.3 Classifying Automated Vehicles

Classification for automated cars as suggested by the National Highway Traffic Safety Administration:

"Level 1: Driver has complete control of vehicle at all times.

Level 2: Some vehicle controls are automated, e.g. automatic braking.

Level 3: Two or more controls can be automated at the same time, e.g. cruise control and lane keeping.

Level 4: The driver can cede control in certain circumstances.

Level 5: Full automation, Driver not expected to play any part in the driving process at all" [8], [13].

3 RISK MANAGEMENT

It is a fact that special attention in recent research is paid to the discussion of safety challenges that a self-driving electrical car project can encounter and the main outcomes and future research possibilities development [4]. Hence, risk management is brought to surface in this research as it aims to make the transportation system more secure in term of traffic accidents; protection against theft, security of software systems against malfunctions and external attacks.

Software in AV has various roles " engine control, external communications, car safety and security, and to build a cyber-safe system with regard to the vehicles, vehicle systems and intelligent infrastructure within the intelligent transport system [2].

The main challenges in the field of autonomous vehicles rest in the fact that " *Improving road safety by removing human error from the driving equation, through testing and validation processes for new autonomous systems and features and through develop a cost and time efficient methodologies*"[14].

There are continuously change in the fields of research over time, i.e. future transportation design has to take into consideration not only technical and economic aspects but also, legal, social and all kinds of necessary factors [1].

The concept of applying NIST SP 800-30 and International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27005 to AV will discussed [5].

4 METHODOLOGY

4.1 Applying ISO/ International Electrotechnical Commission (IEC) 27005 to AV

Because the process of reseasrch in transportation auotomated vehicles is combine the unlimited set of operational scenarios encountered in public traffic with the absence of human supervision this needs highest demands regarding functional safety throughout the development of these systems, to ensure safety, a risk assessment must be done, in this contribution analysis, risk assessment and evaluations acording to, Risk assessment with NIST, SP 800-30 [9] and ISO 27005 standard [5] will istablished (see Figure 2 below), the applicability of the ISO 26262 standard and all must be examined [11].

ISO/IEC 27005(3rd edition 2018-07) international standard, for automated vehicles risk assessment can be done coherently according to ISO/IEC 27005 (Information technology Security techniques — Information security risk management) standard, This document supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach, since these documents provides a guide line for information security risk management and it is applicable for all types of organizations (commercial, government, agencies, non-profit organizations) and it is up to the organization to define the approach to risk management [5].

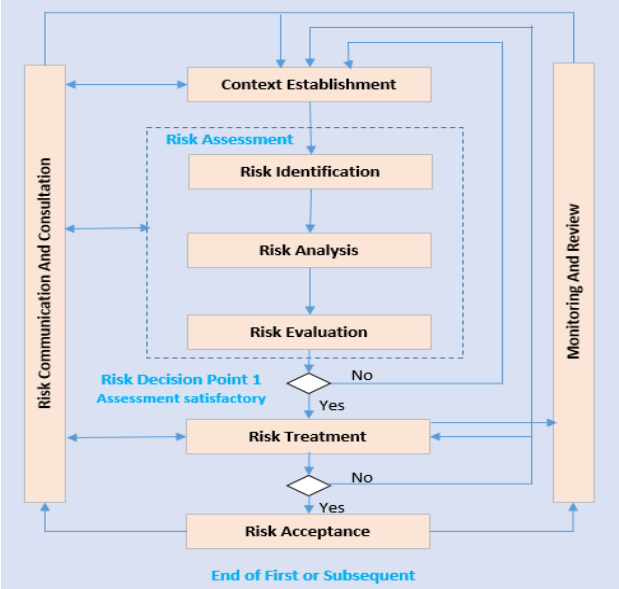
4.2 The applicability of the ISO 26262 Standard

The applicability of the ISO 26262 standard– the most recent standard for designing safety-relevant electronic systems in the automotive context – must be examined to ensure safety because the process combine the unlimited

set of operational scenarios encountered in public traffic with the absence of human supervision this needs highest demands regarding functional safety throughout the development of these systems [14].

4.3 Information Security Management System (ISMS)

By explaining Security Risk Management System SRMS for self-driving electric cars in general, and why self-driving electric cars must contain security aspects, however this issue is not yet clear or easy to imagine all of its future implications; having no idea what a future world of autonomous vehicles will look like, we know that they will reduce car accidents, time wasted in traffic, parking hassles, and probably road rage. But there are also big unknowns areas for example the insurance Instructions and regulations. And "*'if we look back 20 years, when the Internet was still in its dial-up infancy, and you had told someone that in 20 years we would use the Internet to post pictures and videos, observations and thoughts on the Web and online so that our family, friends could view and comment by sight and sound directly and at the same time* " maybe he will doubt it [4], this is the same case for self-driving vehicles technology, it could bring excited experience if it is safe which increase the chance for people who are interested in using them. However, SRMS should be a continual process, as seen in Figure2 below [5]:



2. Figure: Sources ISO/IEC 27005: 2018(E) [5], NIST SP 800-30,[9]

4.4 Information Security Risk Assessment

Risk assessment information data will be collected from, transportation planner studies, and formal institutions whom have a keen interest in how the market for such self-driving vehicles will develop, the risk assessment process will be identify, analyse and evaluate and each step in the assessment process will be estimated with Risk communication, consultation as well as Risk monitoring and review as in Figure 2, [5].

4.4.1 Risk Identifications

The expectations of using self-driving cars still not clear, usage number would increase or decrease, depending on how and when people use self-driving vehicles. Because self-driving vehicles are not yet completely present in the traffic streams, with the exception of a few test vehicles, it is difficult to reliably predict future consumer demand. Any outcomes are just theoretical at this point since the full self-driving technology is not available on the streets, [7]. 'This is why different risks studies associated with the self-driving vehicles technology and each must be carefully assessed and taken into account [4].

4.4.2 Risk Analysis

First of all why to analyse Security Risk for Self Driven Electric Vehicles SDEV, why we want to make SDEV Secure, the answer ofcaurse because the interruption of SDEV will lead to high economic, environment and social dmages and leave the whole system in risk [10]

Many literature reviews have discussed the advantages of AVs. handicapped or disabled consider such cars as blessings. It will bring the chance for minors to move on road without adults joining them. They will enrich the travel experience and bring excitement and release people who do not like to drive from this burden as the care intelligent system will choose the most optimal route, and will increase highway traffic jam. All of these needed to be analysed and that to inform decision makers and support risk responses by studying the following [5]: -

a. *Resource and Assets*

Through studies, workshops, interviews, observations as well as hard and soft copies of national and international papers, articles and from researchers, planners and engineers

b. *Threats*

- The automation vehicles should alert to its surrounding, since there is no separated automation infrastructure so we should take into consideration the threats from other objectives and cars as well as infrastructure combination, electric system security aspects against direct or indirect contacts.
- Threats related to operation and functional systems and its safety and it is mainly concerned with hardware failures and software bugs [4]

c. *Vulnerability and Impact*

- Deliberate corruption occurred and how it will lead to severe problems and direct and indirect interruption, economic, social and environmental damages that may leave the whole system in risk.
- charging and maintenance, operation and training [4].
- With the identification of priority areas according to risk degree, in order to rearrangement of risks acceptable and risk degree.

d. *Like hood of Failure*

sensors and sensitivity, for example the weather condition has a strong effect on the visual capability of the video based sensors. From another aspect, disturbances can also be simulated by region dependent road types or traffic signs tool [14].

4.4.3 Risk Evaluations

"by using certain electronic systems and sensors to observe the environment and for mapping, localisation and navigation such as Vehicle-to-Everything platform, a vehicular communication system that incorporates other more specific types of communication as (Vehicle-to-Infrastructure), (Vehicle-to-Vehicle), (Vehicle-to-

Pedestrian) or other users such as cyclists or Wi-Fi network by providing automatic warning to prevent an accident, (Vehicle-to-Device), (Vehicle-to-Grid), or any other entity that may affect the vehicle" [4].

Pedestrians or a person around the car behaviour is difficult to be anticipated in order to react properly by the care. "In case of a sudden reaction of a person, the system must be able to react and remain in a safe state. This holds also for people lying on the ground or small animals. After all, these are not imaginary but fully realistic situations; in case a collision occurs, the system has to be able to stop so that no injury occurs" [4].

4.4.4 Monitoring Risk and Risk Treatment

This is can be achieved by testing self-driving functions of the vehicles within a controlled area as a "Smart City". "Smart City" would be "a place, where connected car features and smart traffic control systems could be monitoring and testing among the conventional traffic stakeholders, testing the automated vehicles, using the controlled of the partially public road.

The modified regulation of the traffic could be time dependent and it would be dynamically changeable to always reach the safety objectives" [14].

4.4.5 Risk Acceptance

Any system can be acceptable by providing the following, comfort, safety, desirable velocity and traffic density, increase productivity (transport capacity), decreased traffic jams or even avoided with efficient and intelligent traffic control systems, reduce the number of accidents, reduce the emission of harmful materials and smart city transport with advanced ITS system [2].

4.4.6 Risk communication and consultation

If self-driving cars could approach people when ever needed, it will bring the blessing of less driving parks and less ownership of private cars. The safety and productivity are among the socio-economic benefits however, this is need public acceptance and usage before we release these benefits users create demand and

will determine the size market development. "*The advent of autonomous vehicles could be truly transformative*" [7].

Academic and non-academic, has discussed many virtues of Avs and how it will reduce the cost of travel,

allow minors to travel without adults present, enhancing travel experience, travel more safely, choose the route more optimally, questions come to the serface such as: How will other transportaion modes, such as travel by TV or no travel at all, be affected by such innovation? What are the effects on the labor force, when AVs emerge etc.[12]

In addition, what will happen if accident occur who will take the risk and carry the blame, is it the manufacture company or the software provider or another parties. How to be protected from hackers and severe attackers [13].

4.4.7 Risk monitoring and review

this will bring the following: -

Initiative studies for empty AVs from centre to external parking in the morning, and vice versa in the evening.

Increasing in travel rate with the exist of AV is something expected, but this will not necessarily cause a congestion increase in fact it will reduce traffic accidents and increase safety. Create smoother traffic flow and unlock existing capacity on roadways which mean less-road building [7].

5 CONCLUSIONS AND RECOMMENDATIONS

When Information Security Management System (ISMS) applied to Automated Vehicles AV with risk management in a systematic way the following social, economic and environmental dimensions will be achieved to maintain welfare for the whole society:

- It will change the life style of driving, as it motivates travelling for long distances, allow minors to travel without adults present. They will relieve busy people, elderly and people who fear driving from the burden of driving,
- Reduced costs of travel relative to traditional vehicles and that will make commuters accept longer travel distances in order to drive larger and comfortable residences and may increase the total amount and size of residential land.
- Enhance travel experience.
- People will travel more safely, choose the route more optimally, and will increase highway throughput.
- In addition to that, cities will change dramatically, downtowns, parking space will remove, and daytime parking will be unnecessary and it is possible that some locations of daytime and night-time parking will coincide, allowing to take advantage of natural complementarity of the two types of parking and to reduce the total amount of urban land dedicated to parking.
- Increase in the density of economic activity, causing increase in productivity.
- Although traffic is projected to increase, this will not necessarily cause a congestion increase, as AVs are expected to be operated more efficiently.

For further researches in the future; it is recommended to adopt initiative studies for empty AVs from centre to external parking in the morning, and vice versa in the evening, as long as Traditional Vehicles TV and AV travel together, the main traffic flow will be higher than the reverse traffic flow. This is because the main traffic will consist of both AVs and TVs, while the reverse traffic will be made of empty AVs only, this means that, if the government still adopt for traffic control, if control is done by means of congestion fees, the reverse (empty AV) traffic should optimally be allowed to travel for free.

6 REFERENCES

[1] Tamás Tettamanti1, István Varga1, Zsolt Szalay,: Impacts of Autonomous Cars from a Traffic Engineering Perspective, Technical Specification Methodology for an Automotive Proving Ground Dedicated to Connected and Automated Vehicles.2018

[2] Dániel Tokody, Attila Albini, László Ady, Zoltán Rajnai and Ferenc Pongrácz, : Safety and Security through the Design of Autonomous Intelligent Vehicle Systems and Intelligent Infrastructure in the Smart City. Available from: https://www.researchgate.net/publication/328134553_Safety_and_Security_through_the_Design_of_Autonomous_Intelligent_Vehicle_Systems_and_Intelligent_Infrastructure_in_the_Smart_City [accessed Nov 10 2018]..

[3] Markus Maurer • J. Christian Gerdes Barbara Lenz • Hermann Winner, : Autonomous Driving, Technical, Legal and Social Aspects, Springer Open, Sponsored by; Daimler and Benz Stiftung.

[4] Rassõlkin, A.; Sell, R.; Leier, M. (2018), : Development Case Study of the First Estonian Self-Driving Car, ISEAUTO,Tallinn, *Estonia*.

Volume/Issue: Volume 14: Issue 1. *First* Online: 28 Jul 2018. Page Count: 81–88. DOI: https://doi.org/10.2478/ecce-2018-0009

[5] ISO, INTERNATIONAL STANDARD ISO/IEC 27005 ,Third edition 2018/17, Information technology — Security techniques — Information security risk management Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information

[6] James Armestrong, How Do Driverless Cars Work? https://www.telegraph.co.uk/cars/features/how-do-driverless-cars-work/2018

[7] Johanna P. Zmuda, Ipek N. Sener, : Towards an Understanding of the Travel Behavior Impact of Autonomous Vehicles ,World Conference on Transport Research - WCTR 2016 Shanghai. 10-15 July

[8] Torben Stolte, Gerrit Bagschik, Andreas Reschka1, and Markus Maurer, Hazard, : Analysis and Risk Assessment for an Automated Unmanned Protective Vehicle, 2017

[9] NIST Special Publishing 800- 30 Revision1, : (National Institution Of Standard And Technology NIST , US Department of Commerce), : Guide for Conducting Risk Assessments,NIST SP 800-30 standard for technical risk assessment: Information Security, September 2012

[10] D. Pleskonjic1, F. Virtuani2, O. Zoggia2 , : Security Risk Management for Critical Infrastructures, 2011

[11] Paul Goodman,: Advantages and Disadvantages of Driverless Cars,Updated on November 22, 2016. https://axleaddict.com/safety/Advantages-and-Disadvantages-of-Driverless-Cars.

[12] Roman Zakharenko, : Self-driving cars will change cities, National Research University Higher S, Elsevier,2016 , vol. 61(C), pages 26-37.

[13] Lim, Hazel Si Min, Taeihagh, Araz`, : Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications, May2018, Vol. 11 Issue 5, pN.PAG-N.PAG. 1p.

[14] Zsolt Szalay, Adam Nyerges, Zoltan Hamar, Matyas Hesz, : Technical Specification Methodology For An Automotive Proving Ground Dedicated To Connected And Automated Vehicles, received 06 march 2017, accepted 18 march 2017.