https://doi.org/10.3311/PPtr.13848

Periodica Polytechnica Transportation Engineering, 48(3), pp. 253–259, 2020

Evaluation of Highway-pilot Function Based on FMEA Safety Analysis

Ádám Bényei[1], Gabor Vida[1*], Krisztián Pintér[1], Zsolt Szalay[1], György Ágoston[2]

[1] Department of Automotive Technologies, Faculty of Transportation Engineering and Vehicle Engineering,
Budapest University of Technology and Economics, H-1521 Budapest, P. O. B. 91, Hungary
[2] Department of Software Development and Application, Institute of Informatics, University of Dunaújváros,
H-2401 Dunaújváros, P. O. B. 152, Hungary
[*] Corresponding author, e-mail: gabor.vida@gjt.bme.hu

Received: 06 February 2019, Accepted: 18 March 2019, Published online: 11 September 2019

Abstract

Cybersecurity is becoming more and more relevant. Autonomous vehicles handle large amounts of data and can connect to more and more existing devices, smartphones, tablets, or even other cars and systems. This poses the risk of unauthorized access to data. Theoretically cars have separate computer units, operate in isolation, and are not connected, so there is less possibility to be attacked. However if the vehicles are interconnected, hackers can have easier access to personal data. They can get information about the location of the car owner, their typical trips, and, for example, allow an intruder to know when the tracked person is not at home. Furthermore it can also be happened that the vehicle operation is maliciously disturbed, which can result in a security risk for the passengers. In extreme cases, computer terrorist attacks can also be prepared - large-scale interventions on roads can lead to chaos across a region or country. In accordance with the introduced threats, it is a crucial objective of this research to indicate specific methods, which can help the industry to evaluate and prepare for these kinds of attacks in a proper way.

Keywords

failure mode and effect analysis, remote attack, vehicle safety, vehicle security

1 Introduction

With the increasing attention towards connected autonomous vehicles [CAV] in the current years from both the manufacturer and the customer side, it is more and more important to talk about safety and security (Tettamanti et al., 2016). Safety and security are both qualities that concern the overall system (Zöldy, 2019). But in general, these frameworks are handled separately in the vehicle industry. Improvement of traditional mechanical components with redundant inherent elements is in the focus of the functional safety standardization (ISO 26262) (Martin et al., 2017). In contrast to this, security topics are traditionally seen as attacks of a mechanical nature and as only affecting single vehicles (e.g. door lock and immobilizer related). Because of the spread of vehicular system networks (e.g. V2X), novel development objectives like automated vehicles, and on the air software updates, it is no more tolerable to expect that vehicles are not effected by cyber threats.

Since the introduction of Electronic Control Units [ECUs] in the automotive production process, the complexity of such inherent component frameworks has increased reasonably. According to professional estimation, 80 % of manufacturing related research activities was performed in the field of inherent vehicular systems in the previous years. Furthermore, nowadays the fast developments of information technology significantly contribute to the spread of V2X features. Bluetooth and internet interfaces are built in the newly produced vehicles and these lead the vehicle to new kind of risk arriving from the cyberspace. Summing up, the vehicle domain needs novel methods to improve cybersecurity (Szíjj et al., 2015) and safety focused development processes (Macher et al., 2016).

This paper aims to give some insight on the possible failures caused by cyberattacks by the application of a classical safety analysis for a specific automated function. This article specifically focuses on the highway-pilot function. The effect of cyber-attacks on safety will be in focus and not method and execution of cyber-attacks themselves. The research tries to indicate which failure

Cite this article as: Bényei, Á., Vida, G., Pintér, K., Szalay, Zs., Ágoston, Gy. (2020) "Evaluation of Highway-pilot Function Based on FMEA Safety Analysis", Periodica Polytechnica Transportation Engineering, 48(3), pp. 253–259. https://doi.org/10.3311/PPtr.13848

modes can be caused by cyber-attacks and try to define plans for their prevention. It needs to be expressed that this paper rather focuses on the possibility of sign and data spoofing than a direct vehicle attack scenario.

At first the most important references are introduced, which have been used during the research. This study is based on the following articles.

At first the current threat and risk assessment methodologies have been studied through Georg Macher's article. This paper attempts to indicate a similarities between available automotive safety and security related models. The outcomes present that the vehicle industry have not focused on security threats so far. Additionally, the article presents a model to cluster cyber-security risks and to contract safety and security evaluation. One good example for this approach is the Safety-Aware Hazard and Risk Assessment (SAHARA) method (Macher et al., 2016).

In the next step, existing safety analysis methodologies have been studied for a starting point. The chosen method is Failure Mode and Effect analysis because it is very common in the automotive industry. To do this the article of Struss and Fraracci (2012) has been evaluated. This paper is about a model-based automation of Failure Modes and Effect Analysis applied to a hydraulic part of a vehicle braking system. Although it focuses on the automation of the analysis, it provides good insight on the steps of an FMEA and how it is applied in an automotive environment. The FMEA's description from the SAE standard is as follows.

Failure mode and effects analysis (FMEA) is a rational and well-constructed system- and also component-scale evaluation. Potential failure modes are determined during the analysis, beside this the relevant causes and the expected effects related to the given the failure mode and the related severity scaling are also identified (SAE, 1993; Struss and Fraracci, 2012).

The rest of the sources focus on cyber-attacks or cyber-security related to CAVs. The first one focuses on cyber-attacks against connected automated vehicles (CAV). It presents the state-of-the-art methods to prevent these attacks and investigates another type of attack, the so-called slight-attacks. The paper concludes that when one CAV is under slight attacks, it is more risky if transmitted locations are influenced than velocities; if more connected vehicles are attacked, it may be more dangerous if many vehicles are influenced with low severity outcomes than if a small amount of vehicles are influenced with higher severity outcomes; furthermore, the result of slight-attacks can be more dangerous at deceleration than acceleration (Li et al., 2018).

The second article overviews different passive and active cyber-attacks on CAVs and presents solutions for each of these attacks based on the state-of-the-art methods and discusses possible improvement orientations in the field of CAV related cybersecurity (He et al., 2017).

Finally, the last article provides a brief overview of main cybersecurity threats on three relevant security fields of today – e-mobility, car sharing and automated valet parking. The article also discusses briefly the main protection concepts (Haas and Möller, 2017).

2 Method

Aiming to keep the methodology as simple as possible, a very specific case is examined. First, an FMEA of a highway-pilot CAV function has been performed. The analysis covers only the main failure modes and the aspect of security have been in the focus of the evaluation. Each failure mode and its effects are examined to decide whether they could be caused by cyber-attacks or not. Beside this objective prevention plans have been provided in each case. Beside the investigation of CAVs, it is also important to examine attacks targeting the infrastructure or other vehicles to some extent because falsified data can also cause critical impact related to the transportation process.

The FMEA is proved to be an effective method to start the investigation since it is applied widespread in the automotive industry, so most of the automated vehicle functions probably have already gone through a detailed evaluation or are going to be the subject of a related analysis in the near future. Because of its well applicability, many studies have already performed different FMEA related investigation. The main objective of the method is to substantially go through all potential component faults and estimate their effects on the analyzed functionality of the system in order to assess whether it can lead to a critical situation and violate safety requirements. Another important reason, why FMEA are so frequently used is its model based characteristic. Because of this, it can be used early in the design stage. On the other hand it also has to be mentioned that it is closer to qualitative methods than to numerical models, however it is completed with the identification of the risk priority number. The main design steps of FMEA process is presented in Fig. 1 (Struss and Fraracci, 2012).

3 Results

As mentioned earlier, the first step of the evaluation after the initial planning is the Failure Modes and Effect Analysis. The resulting FMEA can be seen in Table 1.

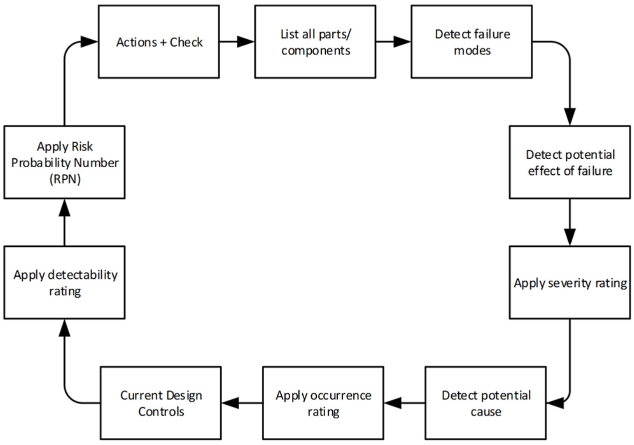

Fig. 1 FMEA phases

Severity, occurrence and detectability values are rated according to the main concept of the method and so the Risk Probability Number [RPN] is defined. These numbers are significantly relevant for our analysis since most of the failure modes are analyzed thoroughly. However, the Current Design Controls column is also left out, it is too specific, it differs for every OEM and in most cases, it is not necessary for our research.

The first step is to determine the items, functions or components we wish to examine. These should be chosen so that they cover the whole system. Based on the Highway Assist system by Bosch, we chose the following main components: (Bosch)

- Radar system
- Camera system
- ESP
- Speed sensor
- Brake sensor.

The radar and camera systems are responsible for the perception of the environment and for creating the situation analysis so that the main system can work with abstract data of the objects and the environment. The electronic stability control unit is the main coordinator of the function.

Table 1 The FMEA table of an ESP related cyberattack

Item / Function	Potential Failure Mode	Potential Effect of Failure	Potential Cause	S	O	D	RPN
Radar	False positive object detection	Unnecessary braking	Software error	7	3	1	21
		Lane-change cannot be executed	Sensor failure		4	1	28
		False lane model			5	4	140
	False negative object detection	Collision	Software error	9	2	2	36
		False lane model	Sensor failure		5	4	180
	Electronic component failure	System shutdown	Manufacturing error	4	3	1	12
		Electric fire			2	3	24
Camera	False object classification	Unnecessary braking	Software error	6	2	2	24
		Lane-change cannot be executed	Sensor failure		3	1	18
		Collision			2	2	24
	Electronic component failure	System shutdown	Manufacturing error	3	4	1	12
		Electric fire			2	3	18
ESP	False situation analysis	Unnecessary braking	Cyber-attack	8	2	7	112
		No braking when needed			2	7	112
		Braking on the wrong wheels			2	5	80
	Electronic component failure	System shutdown	Manufacturing error	3	4	1	12
		Electric fire			2	3	18
		Changed vehicle dynamics			4	4	48
Speed Sensor	False speed signal	False situation analysis of other systems	Sensor failure	5	2	1	10
		Not the desired amount of brake force	Cyber-attack		3	5	75
Brake Sensor	False positive brake signal	Not the desired amount of brake force	Sensor failure	6	3	1	18
		No braking when needed	Cyber-attack		2	5	60
	False negative brake signal	False situation analysis of other systems	Sensor failure	4	3	1	12
			Cyber-attack		2	5	40

Every demand related accelerating and braking has to be sent to the stability control first and it performs the demanded action considering the vehicle's dynamic parameters and the physical boundaries.

Speed and brake sensor have been analyzed additionally compared to the traditional system description due to cyber-security considerations. These sensors send their data on the CAN network that can potentially be vulnerable to cyber-attacks. A false signal from these sensors can cause serious malfunctions in the system but more of this later. In addition, a Highway Assist or Highway Pilot system uses data from other sensors but these two are the most important as they provide information about the state of the vehicle dynamics.

3.1 Radar system

The radar system is the most important component for situation analysis. It usually consists of a long-range and a medium-range or a short-range radar on the front and a medium-range radar at the rear of the vehicle. The radars are responsible for detecting and classifying the objects in the environment of the vehicle, so it is crucial that the objects are indeed detected and classified properly. On Fig. 2, the area that these radars can scan can be seen, including the range of the ultrasonic sensors around the vehicle.

From a logical point of view, the radar system can have three potential failure modes:

- False positive object detection
- False negative object detection
- Electronic component failure.

Of course, an FMEA (Ford) can be made for the radar system and its components also, thus further analysis regarding its possible failure modes and their effects and potential causes is possible (Martin et al., 2016) but in our case, the three failure modes are enough.

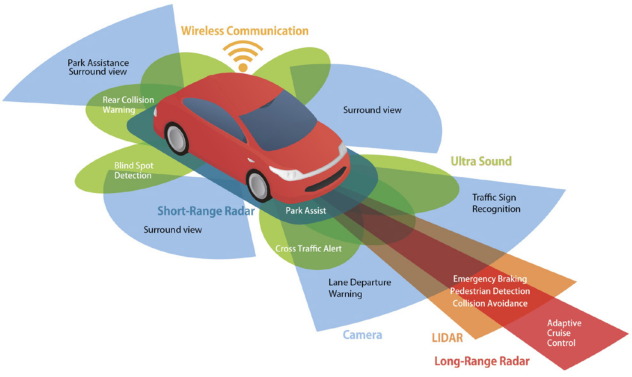

Fig. 2 Radars in highly automated vehicles (innovation-destination)

False positive object detection means that the system detected an object somewhere, when in reality there is no object. This is less dangerous but the manufacturers should still be prepared to handle these situations. The potential effects of this failure can be mainly unnecessary braking, false lane model and non-executable lane-change.

The unnecessary braking could be dangerous and of course inconvenient for the passengers and results in an unpredictable driving mode, that can confuse other drivers. A false lane model can also be dangerous, since if the system cannot determine the course of the lane properly, the vehicle can leave the lane. The implications of this on a multi-lane driving environment is quite clear, although the system considers other objects as well, so the braking of the whole lane-model is not that likely. Other effect can be a non-executable lane-change, because the system falsely detects an object in the way. These effects can be caused by errors or deficiency in the software or failure of the sensors. Cyber-attacks as a cause are not that likely. The radar system is usually not exposed to any outside network and even if an outside attack happened, it is hard to create a sudden, dangerous situation.

In case of false negative object detection, the system does not detect objects that are there in reality. This is more severe than the false positive case because objects not detected can lead to a collision, as it is one of the potential effects. For instance if the system does no detect a vehicle in front or in the next lane, that vehicle will not be calculated in the planned trajectory and a collision can happen without any brake-force applied. The other effect can be a false lane model, which is very similar to the false positive case, since the lane model is created with the detected and classified objects considered. Considering cyber-attacks, it is similar to the previous failure mode. Compromising one or few object's data will not cause serious malfunctions, especially if sensor-fusion is implemented, so cyber-attacks are not in focus in this case.

The third failure mode is electronic component failure. This contains many possible failures but analyzing these is not in the scope of this study. This failure can cause the whole system to shut down or cause electric fire if not handled correctly. Electronic component failures can be caused by manufacturing errors or wear. Obviously, cyber-attacks are not considered in this case.

3.2 Camera system

The camera system is used mainly to help the radar system with object classification and lane detection in a sensor-fusion. Its capabilities to determine distance to an object is very limited. For our study, two main failure modes have been chosen: false object classification and electronic component failure.

In our case, not much can be said about electronic component failure. Its effects and causes are the same as in the case of radar systems. Additionally, it does not come in to consideration in case of cyber-attacks.

Falsely classified objects can lead to serious effects like non-executable lane-change, unnecessary braking or even collision, if not compensated properly with other sensor data. In next step let's consider a case where the camera system cannot identify a vehicle and send data describing the environment without any indicated object in front of the ego vehicle. This could obviously lead to an accident if the other sensors also do not detect the object. Also problematic, if the lanes are detected falsely by the camera system and the vehicle leaves the real lanes because of a wrong lane-model.

As for the causes of these failure modes, the results are similar to the radar systems. A software error, for example, can easily cause failures like this. Other causes include sensor failures; this can produce a similar effect. Considering cyber-attacks, the situation is the same as in the case of radar systems. These sensors usually work in fusion, so an attack against the camera system alone should not cause serious issues in most cases. Additionally, this system should also be isolated, thus making the attacker's job harder to cause any malfunctions.

3.3 ESP

The Electronic Stability Program is a safety-critical function and it can be found in every commercial vehicle since 2014. Every request from other functions to change vehicle dynamics have to go through the ESP first. It decides if the requested action can be executed and to what extent. Without request, it continuously monitors the vehicle's movement parameters and encroaches if necessary. This means that it is crucial for the ESP not to be compromised.

Two main failure modes have been evaluated for our case: false situation analysis and electronic component failure. First, the second case is presented as it is more straightforward. Electronic component failure is similar as in the previous cases. It can be caused by manufacturing errors or wear and it can result in system shutdown, electrical fire or if the failed component is not that critical, it can cause malfunctions in the system. It means that the ESP can modify vehicle dynamics the wrong way, causing the car to behave differently, it could become hard to control.

The other possible failure mode is more interesting according to our concept as false situation analysis can be a result of a cyber-attack. Since the ESP gets most of the information it requires from the CAN network, a potential attack and falsification of the information transmitted here can result in a malfunction. Attacking the CAN network can cause other functions to fail as well, but in a Highway pilot function's case, the ESP is critical. False CAN messages can cause the system to build its model completely wrong, resulting in unpredictable behavior and stability loss. This includes the following effects: unnecessary braking, no braking when needed and braking on the wrong wheels. This last one makes the situation worse than in the previous cases because it makes the vehicle unstable and it can cause an accident. For the other two, the same applies as in the previous cases; both can be dangerous, especially when no braking is applied.

3.4 Speed sensor

Another important component is the speed sensor. This is a simpler case since its only failure mode is transmitting a false speed signal. Transmitting no signal at all could be a different case but the system in the vehicle should be prepared for this, so for our study, these two can be examined together as one. In the FMEA, the two potential effects of failure are false situation analysis and not the desired amount of brake force. A false speed signal can cause serious problems in the vehicle's systems, since this is the main input variable for most. The situation analysis can be false, and the wrong functions can be activated. For example, parking assistant functions can move the steering wheel at high angles but should only do so, when under certain speed. Receiving false speed signals can cause them to become active. This can cause a huge risk if there is no protection against this on the lower levels of system components.

However, it is relatively easy to protect the system from a false speed signal, let it be a simple sensor failure or a cyber-attack that caused it. First of all, every subsystem that has speed as one of its main input, has limits to it. For instance, a parking assist has to check the vehicle speed and it cannot be activated if it is over a specified value. This is true for other assistant systems as well, that take the control from the driver. Furthermore, the speed signal can be corrected with the wheel speed signals. This happens in the

ESP, so that the system can drop the speed value if it seemed invalid after the comparison. This also makes the job of a potential attacker harder because it is not enough to falsify the speed signal, the attacker also has to adjust the wheel speed signals accordingly. Overall, this makes attacks on the speed signals unlikely and easy to defend against.

3.5 Brake sensor

The brake sensor is similar to the speed sensor in a sense that it provides a quantitative signal of the vehicles' dynamics. However, the brake signal also has another aspect to it, its existence. In the case of the speed sensor, it is not enough to know that the vehicle is moving or not, we need to know the actual value. In this case, however, often it is enough to know that the vehicle is braking; the exact value of the brake-force or the deceleration is secondary.

So in this case, as potential failure modes, we can talk about false positive and false negative brake signals. A false positive signal means that there is an active brake signal that does not reflect the actual state of braking. This can cause the following effects: the braking is executed with less than the desired brake-force; no actual braking is done when necessary. Both scenario can lead to an accident and both can be caused by either a sensor failure or a cyber-attack.

A false negative brake signal means that there is no brake signal even though the brake force is not zero. This is the safer failure mode since the vehicle will eventually slow down but even this can create dangerous situations, for instance if the system gets no feedback of the actual force of the braking and it tries to add more. On the other hand, as in the case of the speed sensor, falsifying one signal will not fool most systems in a vehicle. The speed sensor, the wheel speed sensors and accelerometer signals can rule out a false brake signal, so a potential attack would have to change these signals as well; this makes the attacking of the brake signal harder.

4 Summary

This study's goal was not to determine all possible vulnerabilities but rather to raise some questions about the possible failure modes induced by cyber-attacks in case of automated vehicles. The aspects covered by the FMEA are not that broad but it gives good insight on possible vulnerabilities starting from a method that is well known and practiced in the vehicle industry. From the study, it can be concluded that nowadays it is hard to find any parts of a commercial vehicle that cannot be compromised by cyber-attacks. In addition, as the level of automation slowly increases, more and more subsystems of a vehicle are vulnerable against cyber-attacks.

It is crucial that the communication systems are well protected or prepared because this can be a good starting point of every cyber-attack. From this segment the ESP is the most vulnerable part since in some systems it is responsible for executing all vehicle dynamics and if its information is compromised, it can lead to dramatic results. Two main aspect of this were studied: what happens if the speed or brake sensor's signal is falsified. It was concluded that in most cases, it is not a serious problem because of other sensor's data but if the attacker can compromise those too, the situation is far worse.

Also important are the camera and radar systems. These are more and more widespread and absolutely necessary for any kind of automation. It can be very dangerous if an attacker manages to create or hide objects from the camera or radar system, or in the worst case both, by overwriting the communication between the ECUs or accessing the controllers themselves.

Acknowledgement

The research reported in this paper was supported by the Higher Education Excellence Program of the Ministry of Human Capacities in the frame of Artificial Intelligence research area of Budapest University of Technology and Economics (BME FIKP-MI/FM).

References

Bosch GmBh "Highway Assist", [online] Available at: https://www.bosch-mobility-solutions.com/en/products-and-services/passenger-cars-and-light-commercial-vehicles/automated-driving/highway-assist/ [Accessed: 14 November 2018]

Ford Motor Company (2011) "FMEA Handbook Version 4.2", Ford Motor Company, Dearborn, MI, USA.

Haas, R. E., Möller, D. P. F. (2017) "Automotive Connectivity, Cyber Attack Scenarios and Automotive Cyber Security", In: IEEE International Conference on Electro Information Technology (EIT), Lincoln, NE, USA, pp. 635–639. https://doi.org/10.1109/EIT.2017.8053441

He, Q., Meng, X., Qu, R. (2017) "Survey on Cyber Security of CAV", In: Forum on Cooperative Positioning and Service (CPGPS), Harbin, China, pp. 351–354. https://doi.org/10.1109/CPGPS.2017.8075153

Innovation-destination "Autonomous Car", [online] Available at: https://innovation-destination.com/2018/02/16/7-factors-critical-success-self-driving-cars/sensor-and-camera-systems-of-vehicle-autonomous-car-driverless-vehicle [Accessed: 20 December 2018]

Li, Y., Tu, Y., Fan, Q., Dong, C., Wang, W. (2018) "Influence of cyber-attacks on longitudinal safety of connected and automated vehicles", Accident Analisys & Prevention, 121, pp. 148–156. https://doi.org/10.1016/j.aap.2018.09.016

Macher, G., Armengaud, E., Brenner, E., Kreiner, C. (2016) "Threat and Risk Assessment Methodologies in the Automotive Domain", Procedia Computer Science, 83, pp. 1288–1294. https://doi.org/10.1016/j.procs.2016.04.268

Martin, H., Tschabuschnig, K., Bridal, O., Watzenig, D. (2017) "Functional Safety of Automated Driving Systems: Does ISO 26262 Meet the Challenges?", In: Watzenig, D., Horn, M. (eds.) Automated Driving, Springer International Publishing, Cham, Switzerland, pp. 387–416. https://doi.org/10.1007/978-3-319-31895-0_16

SAE (1993) "SAE AIR4845 The FMECA Process in the Concurrent Engineering (CE) Environment", SAE International, Warrendale, PA, USA. https://doi.org/10.4271/AIR4845

Struss, P., Fraracci, A. (2012) "Automated Model-based FMEA of a Braking System", IFAC Proceedings Volumes, 45(20), pp. 373–378. https://doi.org/10.3182/20120829-3-MX-2028.00230

Szíjj, A., Buttyán, L., Szalay, Zs. "Hacking cars in the style of Stuxnet", [pdf] Laboratory of Cryptography and System Security, Budapest, Hungary, Available at: http://www.hit.bme.hu/~buttyan/publications/carhacking-Hacktivity-2015.pdf [Accessed: 20 November 2018]

Tettamanti, T., Varga, I., Szalay, Z. (2016) "Impacts of Autonomous Cars from a Traffic Engineering Perspective", Periodica Polytechnica Transportation Engineering, 44(4), pp. 244–250. https://doi.org/10.3311/PPtr.9464

Zöldy, M. (2019) "Legal Barriers of Utilization of Autonomous Vehicles as Part of Green Mobility", In: Burnete, N., Varga, B. (eds.) Proceedings of the 4th International Congress of Automotive and Transport Engineering (AMMA 2018), Proceedings in Automotive Engineering, Springer International Publishing, Cham, Switzerland, pp. 243–248. https://doi.org/10.1007/978-3-319-94409-8_29