IEEE Communications Standards Magazine, Volume 5, Issue 1, March 2021, pp. 40 - 46
DOI: 10.1109/MCOMSTD.011.2100004

Digital Twin Analysis to Promote Safety and Security in Autonomous Vehicles

Sadeq Almeaibed, Saba Al-Rubaye, Antonios Tsourdos, and Nico Avdelidis

***Abstract*—With the new industrial revolution of digital transformation, more intelligence and autonomous systems can be adopted in the manufacturing transportation processes. Safety and security of autonomous vehicles (AV) have obvious advantages of reducing accidents and maintaining a cautious environment to drivers and pedestrians. Therefore, the transformation to data-driven vehicles is associated with the concept of digital twin, especially within the context of autonomous vehicle design. This also raises the need to adopt new safety designs to increase the resiliency and security of the whole autonomous vehicle system. To enable secure autonomous systems for smart manufacturing transportation in an end-to-end fashion, this article presents the main challenges and solutions considering safety and security functions. This article aims to identify a standard framework for vehicular digital twins that facilitate data collection, data processing, and analytics phases. To demonstrate the effectiveness of the proposed approach, a case study for vehicle follower model is analyzed when radar sensor measurements are manipulated in an attempt to cause a collision. Perceptive findings of this article can pave the way for future research aspects related to employing digital twins in the autonomous vehicle industry.**

INTRODUCTION

CURRENTLY the automotive industry is undergoing dramatic changes with some major automotive companies finding themselves lagging behind relatively new software versions from software companies. The advancement and expanded usage of digitized technologies in the manufacturing sector is transforming every department in the automotive manufacturing chain, from design and product innovation to consumer and services. The industry is expected to continue massive growth in connected topology bypassing 50 billion machines in 2020 and beyond [1]. This causes a massive increase in data processing in autonomous vehicle (AV) platforms and supporting infrastructure within the category of Internet of Things (IoT). These segregated and distributed connectivity models pose a strong threat to vehicular manufacturing business and society due to vulnerability to hackers [2]. Therefore, automobile industry stakeholders including auto makers and information technology companies must fully understand the extent in which networks and data management systems are susceptible to cyber threats, secondly, what steps need to be taken to close the gaps in the data privacy aspect to secure car platforms. However, assessing the operational behavior and data breaches for smart cars in search for anomaly events could be very challenging when conducted by humans. Therefore, there is a big motivation by industry to study the impacts of cyber attacks in automotive manufacturing and develop new platform solutions for autonomous vehicles featuring safety, security, and data privacy [3]. This objective can be achieved by developing innovative data protection techniques when capturing data and during decision making procedures. IPC-2551 is considered to be the first 'International Standard for Digital Twins' that defines digital twin properties, types and complexities for digital twin product, architecture, and lifecycle framework [4]. Moreover, the concept of digital twin driven safety environment has been used by IoT in virtual representation of vehicle status transitions for platform health monitoring [5]. From this definition, it is evident that digital twins play a crucial role in promoting the visibility of operations and predictions of future machine safety. Similarly, the concept of digital twin is critical for data analytics to identify the situations when data irregularity starts to detach the virtual representations from physical reality. Digital twin in IoT also serves in connecting the autonomous vehicles [6] with the manufactures, thereby, helping business people to make crucial decisions in the supply chain and inventory management. The digital twin approach of autonomous vehicles is, therefore, a business tool and a credible technological asset.This approach helps to drive the autonomous vehicle industry as with each vehicle software update, a vehicle becomes slightly closer to the next level of autonomy.

The architecture of an autonomous vehicle can be divided into five categories: Perception, which is the process of sensing the surrounding environment using on-board sensors such as light detection and ranging (LIDAR), cameras and radio detection and ranging (RADAR). Localization, which finds the position of the vehicle using different techniques available. Planning, which determines the actions that will be carried by the self-driving platform based on perception and localization. Control is in charge of execute the actions determined by the planning,such as breaking, accelerating and steer the vehicle and finally, system management, which is in charge of supervise all the other categories, such as log recording, fault detection and provide a human-machine interface (HMI) in order to perform basic operations with the Advanced Driver Assistance Systems (ADAS) [7]. However, a complete profile for autonomous vehicle testing methodologies is still highly needed during the whole development process, including functions, system integration, verification, and validation. Thus, digital twins can be considered as a good virtual environment for testing ADAS and automated driving systems are good references for autonomous driving tests.

In the digital twin scenario, there are four different phases in the automotive industry where data are being exchanged, as shown in Fig. 1. In the initial phase, the autonomous car starts collecting different data such as manufacturing data, drivers perception data, and data that could connect the car to external

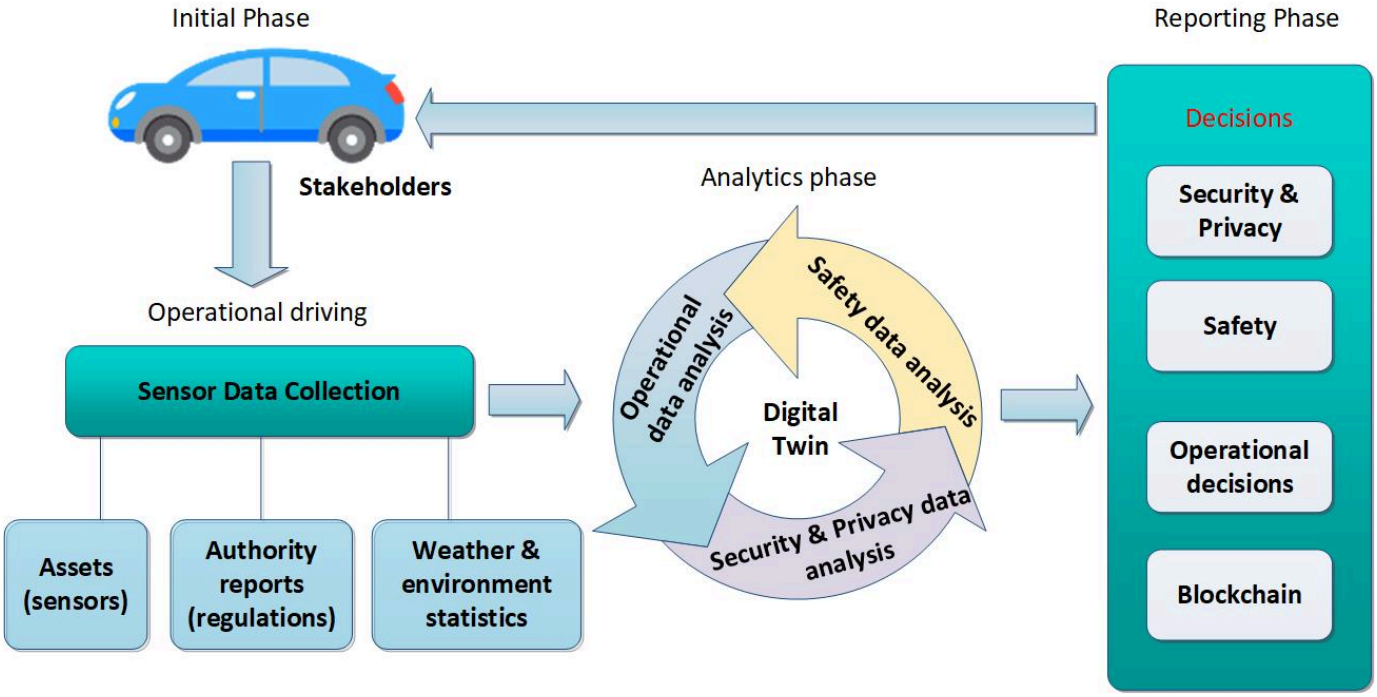


Fig. 1: Digital twin components supporting vehicle autonomy.

systems and services. In the operational driving phase, an autonomous car collects sensor data from different operational properties, environmental information, and official reports. In the analytics phase, the digital twin of an autonomous vehicle takes a decision automatically based on the collected and measured data. In the reporting phase, the decision taken should suggest how to improve the driving procedures that might affect the driver, which engineers should be able to control. The stakeholders then receive the reports that are manually created for further considerations. As we live in the fourth industrial revolution, more automation should be involved in the business processes. In this case, the digital twin may be able to generate automated decision-making reports that can be sent to the stakeholders. This article aims to study the impacts of safety and security concerns of digital twin scenarios for automotive manufacturing. The main objective is to investigate the current industry market and research about digital twin technology and data flow in such autonomous vehicles. Moreover, developing new framework solutions considering the stranded of safety and security. These objectives will be attained by introducing innovative data protection techniques including data gathering and operational decisions to handle any cyber threats and potential vulnerabilities.

The rest of this article is organized as follows. In the next section, we discuss the autonomous industrial vehicle approach. Then, we present a developed safety and security framework for digital twin information interaction. Following this, we present a case study using radar sensors for validating the feasibility of a safety approach for the proposed model in context of reliability. Finally, we conclude this article.

Levels of Autonomy and Operational Models

For an autonomous vehicle system, there are different levels of autonomy, as shown in Fig. 2:

- *Level 0*: This is the manual mode in which the car operates. The driver has the full control of the vehicle and there is no autonomous control.
- *Level 1*: Which is also referred to as the no automation category. This class is characterized by the driver having complete control of the main functions of the vehicle. These tasks include steering, braking, motive powering, and throttling. The driver is as well responsible for the vehicle safe operation.
- *Level 2*: Also known as the function-specific automation level. In this operational model, the manufacturer automates one or more control functions in the vehicle [8]. The person driving the vehicle assumes the overall control and safe operation of the automobile. However, the driver can opt to relinquish limited authority over some functions such as electronic stability and dynamic braking during emergencies.
- *Level 3*: Which is also known as combined-function automation. Computerization in this category entails at least two primary functions. These controls should work in harmony to relieve the driver and allow him or her to perform other tasks. Even though he or she is still liable for the safe operation of the vehicle and monitoring the roadway, autonomous vehicle systems with this level of automation allow the driver to leave control over some primary control functions [8]. However, the motorist should be ready to act without warning at all times.
- *Level 4*: automation, also referred to as the limited self-driving level, describes the capability that allows the

driver to surrender full control of all functions considered to be crucial for safety under particular environmental and traffic situations. In case of any changes, the automation infrastructure should allow for a safe and comfortable transition.

- *Level 5*: Refers to an automation infrastructure that gives the vehicle full self-driving capabilities. In this operational model, the manufacturer develops an automobile that carries out all the driving functions thought to be vital for the safe operation of the vehicle [9]. The infrastructure also enables the vehicle to monitor all roadway conditions during a full trip. In such circumstances, the designed vehicle assumes that the driver provides instructions for both the destination and navigation mechanism. Further, the autonomous car can move without any human intervention. The automated infrastructure is responsible for the safety of the vehicle operation.

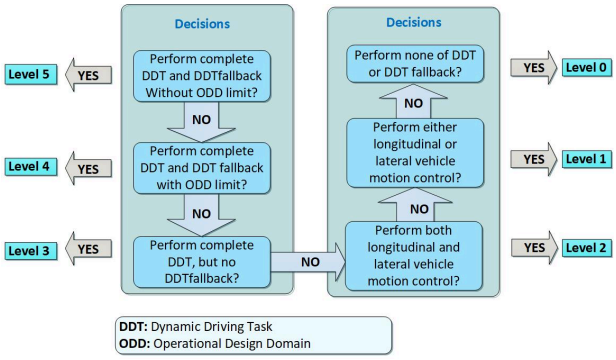


Fig. 2: Autonomy levels in vehicular systems.

DIGITAL TWIN APPROACH

The *Digital Twin* collects the real-time data from sensors and correlates the acquired information with historical data that was obtained earlier from the same car. Based on this processing, the digital twin can make a decision to alert for any unsafe environment [10]. The logical data flow in autonomous cars starts by collecting the data from platform sensors such as Light Detection and Ranging (LIDAR), radar, etc. The acquired data and events are proceeded within the digital twin analytics cluster to perform adjustments, suggestion, and alerts before sending them back to the automotive system. The Society of Automotive Engineers (SAE) developed a framework that highlights the industry market requirements for the development of connected and autonomous vehicles. A common theme in these requirements is the need for features that enable the components of the digital twins to interact directly with the physical autonomous system. The interaction is attainable through a framework that includes data, integration, analytics, and digital twin itself as part of driving system.

In the perspective of autonomous vehicles, a digital twin refers to the efforts placed in the design and implementation of processes needed to enhance the safety, security, and privacy of driverless cars [11]. The acquired data can be integrated to generate information which, when analyzed, leads to the generation of an automatic response. The conceptual architecture in the system is to support the flow of large amounts of data at high speeds. Any delayed speed of data reception, algorithmic analysis, and response may cause car crashes, which may result in fatalities. Therefore, automotive manufacturing should ensure that models and components used for digital twin deployments provide the anticipated safety and security features in optimal order. Since most of the data used by autonomous vehicles are frequently captured in the image format, it is necessary to have an instrument that captures a high level of image diversity including elements such as the sensor or radar. These details are obtainable through the integration of the data collected from global positioning systems (GPS), cameras, radar, and infrared sources such as LIDAR techniques [12]. The gadgets should have advanced environmental recognition capabilities as they are crucial for planning, decision making, and safe operations in autonomous vehicles. The other industry market requirement is a highly sensitive tool for capturing data. There are a number of challenges involved in autonomous driving which are still not solved. One of them is the sensor, which needs to detect and analyze the vast amount of environmental information for decision making. With more data, there is more unnecessary data that needs to be tuned out.

SYSTEM INTEGRITY OF AUTONOMOUS VEHICLES

As stakeholders continue to promote the development of AV, they must also take into consideration the immeasurable outcomes that may arise if there are miscalculations. One issue of concern for self-driving cars is safety and security. As the digital twin becomes an inseparable feature in driverless systems, the risks of becoming a top target for malicious hackers and cybercriminals are of considerable concern. Cybersecurity challenges should be considered during all development and deployment phases of any autonomous car, regardless the level of supported autonomy. The need for cybersecurity features arises from the fact that various types of sensors in vehicle platforms could be the entry points for any cyber-attack. The consequent impacts of a successful hacking would impact the autonomous vehicles safety involving mechanical, electrical and electronic systems. Such unexpected failures may cause catastrophic impacts that could be harmful to human life, vehicle, and environment.

Vulnerabilities of Autonomous Vehicles: In relations to security, autonomous vehicles are vulnerable to cyber-attacks in many ways. The first type of vulnerability relates to the fact that digital twins are hosted by cloud computing, which means that network components are virtualized on remote servers to process storage, retrieve, and store data. Those servers are stocked by 3rd party cloud service providers that offer scalable computational resources. Within the Internet of things context, autonomous vehicles possess a large amount of data that is exchanged with the network and normally stored in cloud. Most of the exchanged data include navigational information about the surrounding landscape and predicated routes for vehicles to follow in congested zones. Such information

is quite sensitive to the safety of vehicular platforms and communication systems. Therefore, any vulnerability in those systems could cause catastrophic sequences, especially when identified by hackers. The other form of vulnerability arises from the growing use of multiple programming languages from open source without enough validations and trails by supply chains. Therefore, automakers should consider validating software operational systems and align them with car parts for compatibility and tractability. This process will allow to identify vulnerability occurrence during production cycle and afterwards during upgrades and maintenance. Hackers may only take advantage of a component that has been programmed by an inferior coding language to penetrate the entire automated system. The third type of vulnerability experienced in autonomous cars concerns the blending of technologies and resources. Car manufacturers are competing among themselves to deliver the first autonomous vehicle. The heightened competition has discouraged them from sharing resources and technologies to develop a refined and secure model. These limitations may give hackers the chance to manipulate the vehicles in the future as firms are not willing to share ideas on safeguarding the cars.

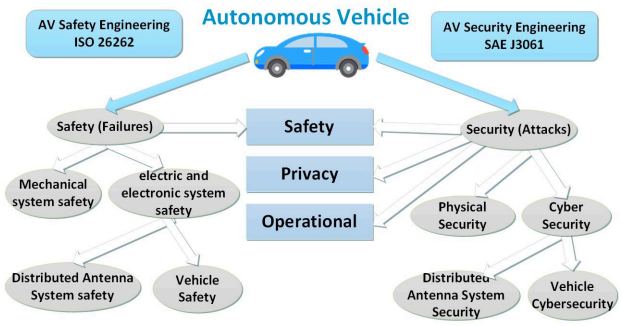


Fig. 3: Safety and security tree in autonomous vehicles.

Types of Attacks on Autonomous Vehicles: Self-driving vehicles are susceptible to attacks because they have to communicate with other cars and software and hardware infrastructure that are connected to external networks. There are several areas of attacks of autonomous vehicle systems: sensors, vehicular ad-hoc network (VANET) [6], and hardware.

1) *Sensors attacks*: These attacks may occur if hackers manipulate the sensors installed on the vehicles. The first instance of attack may take place on the global positioning system, which helps in locating and navigating the car.
2) *VANET attacks*:These attacks occur on the internal and external networks. An example of an attack on the internal network is the key or passcode attack. Users use passwords and keys to secure their vehicles. A hacker may use a method such as brute force to obtain these passwrodes and keys. A vehicle-to-everything (V2X) attack on the external network manipulates the smartphone or any other gadget that helps the car to communicate with the cloud through Bluetooth, Wi-Fi, or the global system for mobile (GSM) communications. Distributed denial of service (DDOS) attack occurs when a hacker manipulates a functioning system by using either a single or multiple attacking devices. A hacker can perform a DDOS attack by overpowering vehicle-to-vehicle (V2V) communication, the automated infrastructure, or a single network.
3) *GPS spoofing attacks*: A spoofing attack usually involves unauthorized terminals gaining access to a computer network and pretending to be a legitimate terminal in the compromised network by falsifying data. The approach enables the attacker to receive valid data illegitimately from the network and can be used to access other parts of the system or even cause significant damage to the compromised systems. In the context of GPS spoofing attacks, an attacker deceives a GPS receiver through broadcasting stronger as well as slightly different GPS signals. An autonomous vehicle using GPS for navigation then interprets the received signals as a set of normal location data. Spoofing enables the attacker to gain control of the autonomous vehicle because he or she has the ability to control the car by transmitting false information that the car uses for control.

Safety and Security Platform Model

The autonomous vehicles involve complex engineering and computing platforms with wireless access to the cloud. Therefore, manufacturers deploy embedded computing technologies in these vehicles to ensure that they operate effectively and efficiently in the physical environment. During manufacturing, operation, and maintenance phases, the AV stakeholders including manufacturers, users, regulators, fellow motorists, and technology companies should have predesigned solutions to issues of security and safety. The alignment process will use two sets of international standards: The Society of Automotive Engineers (SAE) SAE J3061 and the International Organization for Standardizations (ISO) ISO 26262 [13]. The former defines cybersecurity measures for conventional automobiles, whereas the latter defines the electrical and electronic (E/E) safety for car platforms. SAE J3061 addresses issues of security, while ISO 26262 deals with matters of safety. The SAE J3061 standard [14] recommends a mechanism for combining security and safety processes by creating communication links between cybersecurity and safety activities such as threat analysis and risk assessment, hazard analysis and risk assessment, safety requirements, and security requirements. The two concepts should be aligned in the design and development stage of self-driving cars to make sure that the autonomous vehicle attains the necessary level of protection. Since there are five to six possible levels of automation in self-driving cars, the security and safety of these autonomous vehicles are dependent on the environmental conditions and automation levels.

The developed framework is proposed to analyze safety and security concerns in autonomous vehicle systems, as shown in Fig. 4. The steps approach is appropriate for modeling and analyzing aspects of safety and security in digital twin systems. The new model comprises the six elements of the autonomous system: safety countermeasures, failures, functions, security countermeasures, cyberattacks, and digital twin.

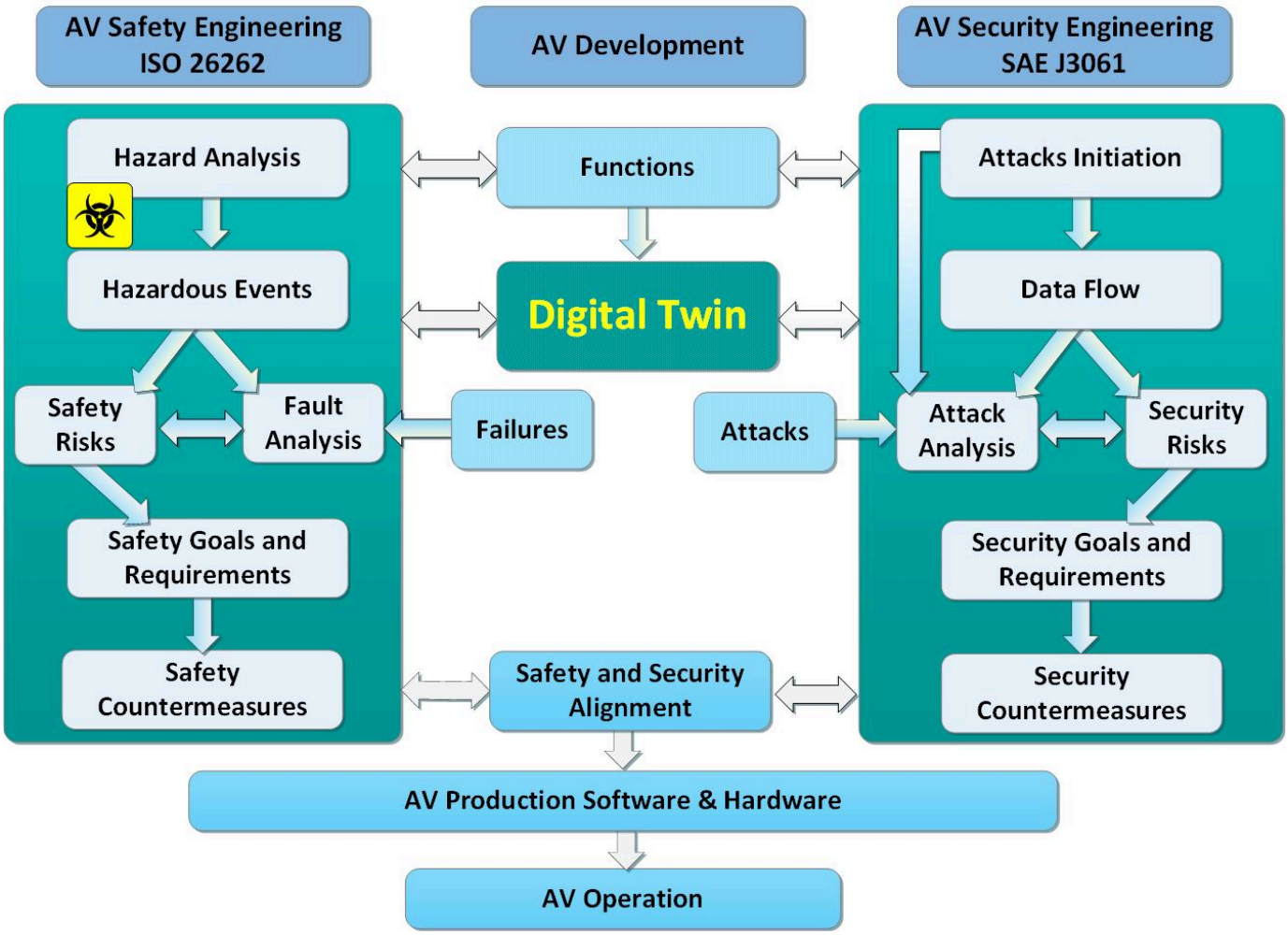


Fig. 4: Data twin proposed framework for vehicle safety and security.

It utilizes correlational matrices to demonstrate interdependencies between those elements. System analytics may be used to evaluate security and safety aspects by applying process functions and digital twins to better understand the impact of attacks and failures on the automated system. The first step of the framework is for checking safety and security, which is meant to model the functional hierarchy of the autonomous car. Functional objectives will be created and then specifying the functions and sub-functions required to realize the goal. The correlational matrix utilized to express the relationship between functions that can be low, moderate, or high. In the second stage, the digital twin explains the systems structure as a compendium of units and subsystems. A system analyst then assigns a particular relationship matrix to define the association between the functions and digital twin. In regard to the operations of AV, steps one and two entail the definition of the driving functions and systems or infrastructure of self-driving cars at the design and development stages. The functional and digital twin aspects of the autonomous vehicles are expressed and included in the model together with their relationships. Structural elements such as the installation of actuators and engine control units are included in this phase. Next phase is focused on performing analysis on safety hazards. The analyst determines any failures and includes them to the model. He or she will then identify the correlation among the functions, failures, and system structure and assign them a matrix. Then, analysis of security threats should be performed. The analyst or operator identifies all possible attacks and includes them on the model. Relationship matrices to express the interdependence among the attacks, structure, functions, and failures are then specified. This description, for instance, will designate an attack-failure matrix to establish the failures that may occur as a result of a successful attack. The last two stated steps are essential for addressing the vulnerabilities associated with autonomous cars. In terms of safety, a hazard analysis and risk assessment are performed to help with the identification and evaluation of possible hazardous and events. This assessment also assists with the expression of functional safety requirements in driverless vehicles.

Elements such as hazard, situation, and fault are utilized to ensure that all hazards relating to self-driving are catered for during development. After performing hazard analysis, the failures that have been taken into account in the security requirements are removed from the fault sequences and included on the developed framework. In terms of security, a threat analysis and risk assessment are performed to gauge the security

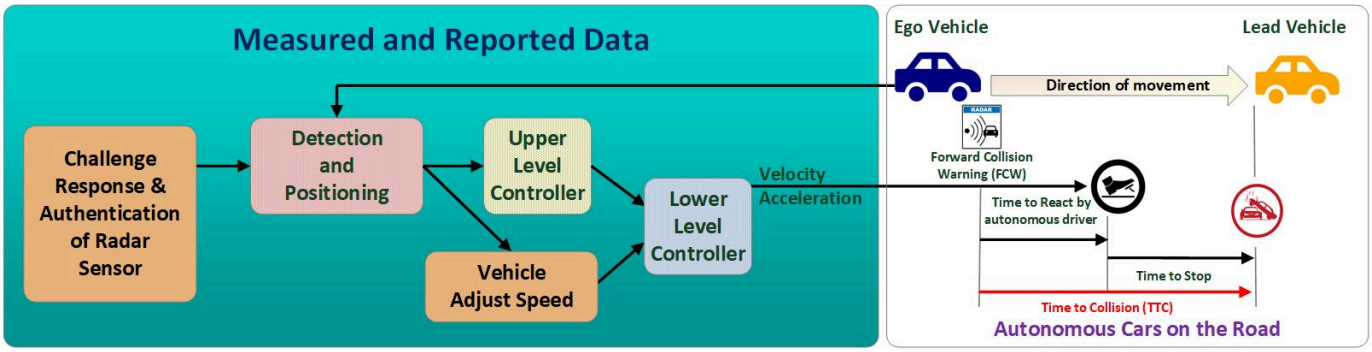


Fig. 5: Safety based detection radar sensor of vehicle follower model.

threats and deduce the functional security requirements of the autonomous vehicle. The dimensions expressed in the earlier stages can be utilized to define the attack initiation and create information-flow frameworks to assist in the identification of potential attacks. After that, the system analyst incorporates the safety countermeasures to the framework and defines the relationships. Finally, the analyst includes the security countermeasures on the model and determines their relationships. Particular matrices will be assigned to describe the relationship of attack and failures and their security countermeasures and the correlations between security and safety. In the last two steps performed, the security and safety countermeasures are specified and included to the model alongside their relationships. In terms of safety, the safety requirements are enhanced by designing and developing countermeasures to fulfill them. The same process is performed on the security aspect such that security countermeasures are developed to fulfill their respective requirements. This process is performed for safety and security alignment as well as for the next two phases which are AV production and AV operation.

Case Study: Vehicle Sensor Attack Detection

For validation purposes, a case study is developed to validate the scenario of using radar sensors in the vehicle follower model and how the collected data can be computed to identify an attack using digital twin. Data flow framework can help to highlight the originating sensors and various processes of system information including data collection, storage and execution. Typically, data flow frameworks show the whole path for data in end-to-end fashion starting sources to storage. However, it is necessary to define the detection process and prevention strategy to identify and prevent unauthorized access to autonomous vehicle systems. Although there are various strategies for eliminating the threat of attack or error in vehicular systems, the choice between those strategies is subject to regulations, standards, and technical features of software and hardware systems. Additionally, analytic modules are used to identify changes in the pipeline bandwidth and consumed power levels. Those monitoring sensors will trigger the appropriate alarm to alert the driver about a possible attack once there is irregularity in the columns of data exchanged or high-levels of computational power consumption. Tailoring to our test, the radar sensor can be programmed to trigger other additional actions such as driving in a predetermined pattern, activation of manual driving mode, positioning or even disabling auto-driving to ensure that a compromised car is unusable to the attacker. In a vehicle follower model, the car is equipped with an adaptive-cruise control (ACC) system that will always keep the vehicle on a reasonable path towards destination [15]. The ACC system built with a millimeter wave radar sensor to enable measurement of relative distance and velocity to a previous vehicle (attacker vehicle). The sensor measuring velocity of the following vehicle is considered as a trusted value for vehicle follower model and sensor detection scheme, as shown in Fig. 5. The forward-facing radar sensor is used for radar range measurements corresponding also to the longitudinal position of the target vehicle.

The cyber-attack impact is shown in Fig. 6-a, as the indicator reports an inclination in the vehicle direction as measured by the hacked radar sensor compared with the actual true direction on ground. This inclination shows that the sensor provides data that shows closer distance to destination compared with the real physical location on ground path. The impaired sensor in this case detects objects in low illumination within the radar cross-section (RCS) and shows them to be closer to the vehicle from the actual reality. Assuming accurate sensor measurements and once the data is transferred to the digital twin, it will mismatch the angle measured to the projected location of the target during azimuthal projection. Typically, the analytics scheme then refers to the actual measured data as the reference point for any calculations causing major disturbances in estimated data and potential accidents when using such data in automating the vehicle on the road.

Fig. 6-b shows the lateral position errors compared with the actual ground direction from surrounding objects (e.g. cars). This causes the digital twin to miss-calculate the availability of the surrounding lanes on the road and keep the car on a certain lane assuming no other options are available. Since the vehicle is not able to change lanes and combined with the effect of the forwarding collision center impact of Fig. 6-a. the digital twin will determine to reduce the car speed as it predicates arrival to destination. This shows that multi-sensor data need to be aligned in terms of provided measurements to be adopted by the digital twin, otherwise the analytics should neglect data from sensors that report incoherent data compared with other data sources. It also shows that digital twin could

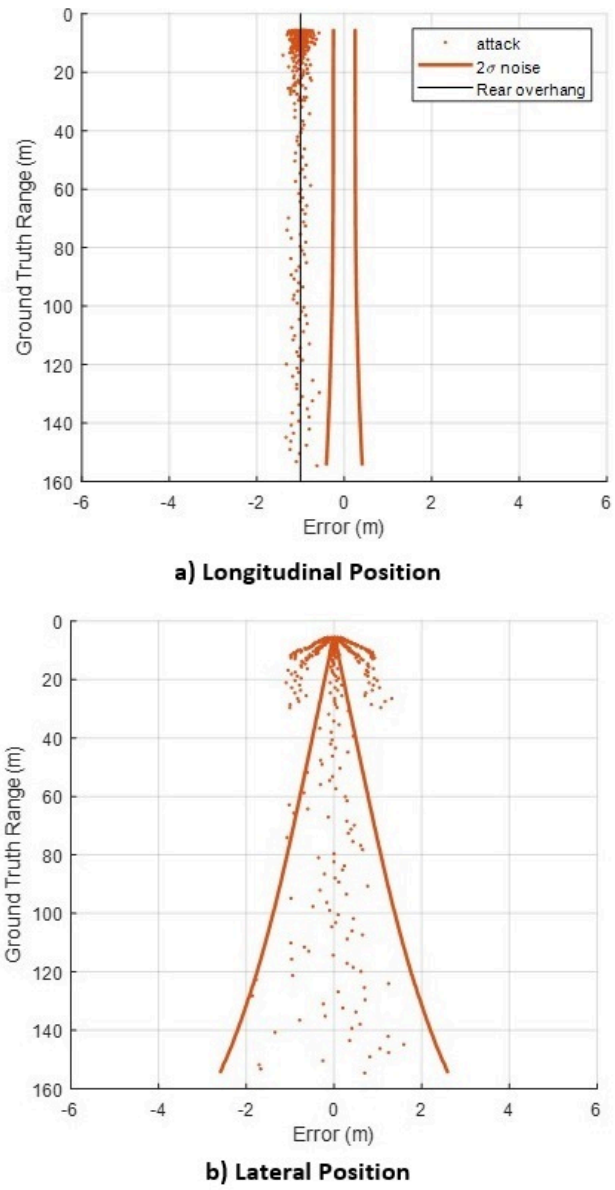


Fig. 6: Impaired detection data provided by vehicle sensors to digital twin.

carry the data verification process and classify a data source to be invalid or hacked considering data values even though the source of those data is genuine.

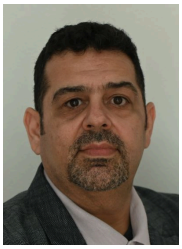
CONCLUSION

In this article, digital twin is explored to automate the decision making process inside an autonomous vehicle using radar sensor data collected from initial, analytics, and reporting phases, and generate reports to be sent to autonomous vehicles. Some of the advantages presented using the car-follower model bring the benefit of reducing the risk of cyber attack and accident. The vehicles must transmit, receive, and process data. Therefore, the stakeholders involved in the development of autonomous cars should, therefore, pay emphasis on privacy, safety, and security to enjoy the benefits of these vehicles. The proposed platform model in this article will help to achieve this goal by profiling the safety and security concerns and addressing them with their respective countermeasures. The recommended model aims at identifying, analyzing, and assessing the threats and providing the user with an opportunity to take appropriate countermeasures in ensuring safety and security using digital twins in driverless vehicles.

Sadeq Almeaibed obtained his M.Sc. degree in engineering and management of manufacturing systems from Cranfield University, United Kingdom in 2019, after obtaining B.Sc. from Colorado State University, USA in 2016. Currently, he is consultant engineer in manufacturing systems leading innovative projects from concept to completion. He has contributed to various development projects through direct engagement with clients and stockholders to meet the needs of emerging industries and technology developments.

Saba Al-Rubaye is a Senior Lecturer and leading connectivity research in the Digital Aviation Research and Technology Centre (DARTeC) at Cranfield University, United Kingdom. Dr Al-Rubaye is participating in developing industry standards by being an active voting member of IEEE P1920.2, Standard for Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems and of IEEE P1932.1 standard of License/unlicensed Interoperability. Her main research interests include, but not limited to UAV connectivity, digital twin, artificial intelligent, safety and security of autonomous vehicles. Dr Al-Rubaye is a Chartered Engineer (CEng), member of IET, Senior member of IEEE and certified Unmanned Aircraft System (UAS) Pilot.

Antonios Tsourdos is a Professor, head of the centre of Autonomous and Cyber-Physical Systems and Director of Research - Aerospace, Transport and Manufacturing, at Cranfield University, United Kingdom. He received his MEng on Electronic, Control and Systems Engineering from the University of Sheffield (1995), MSc on Systems Engineering from Cardiff University (1996) and PhD on Nonlinear Robust Autopilot Design and Analysis from Cranfield University (1999). Professor Tsourdos was a member of the Team Stellar, the winning team for the UK MoD Grand Challenge (2008) and the IET Innovation Award (Category Team, 2009).



Nico Avdelidis is a Professor and Head of the Integrated Vehicle Health Management (IVHM) Centre at Cranfield University, United Kingdom. He is also a Professeur Associe (Adjunct Professor) at Universite Laval, Quebec, Canada. He leads basic and applied research on various non-destructive diagnostics and monitoring approaches, as well as advanced research on IR and non-invasive imaging applications using autonomous systems. Professor Avdelidis is also an expert collaborator in the oN DuTy NSERC (Canada) Programme, leading research and training in the area of Diagnostics & Monitoring of Transport Systems.

REFERENCES

[1] S. Al-Rubaye, J. Rodriguez, L. Z. Fragonara, P. Theron, and A. Tsourdos, "Unleash Narrowband Technologies for Industrial Internet of Things Services," *IEEE Network*, vol. 33, no. 4, pp. 16–22, 2019.

[2] S. Al-Rubaye, E. Kadhum, Q. Ni, and A. Anpalagan, "Industrial Internet of Things Driven by SDN Platform for Smart Grid Resiliency," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–11, July 2017.

[3] A. Nanda, D. Puthal, J. J. P. C. Rodrigues, and S. A. Kozlov, "Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions," *IEEE Wireless Communications*, vol. 26, no. 4, pp. 60–65, 2019.

[4] IPC, "International Standard for Digital Twins," *IPC-2551*, pp. 1–70, 2020.

[5] P7001, "IEEE Draft Standard for Transparency of Autonomous Systems," *IEEE P7001/D1, June 2020*, pp. 1–36, 2020.

[6] E. Talavera, A. Díaz Álvarez, and J. E. Naranjo, "A Review of Security Aspects in Vehicular Ad-Hoc Networks," *IEEE Access*, vol. 7, pp. 41 981–41 988, 2019.

[7] C. Sippl, F. Bock, C. Lauer, A. Heinz, T. Neumayer, and R. German, "Scenario-Based Systems Engineering: An Approach Towards Automated Driving Function Development," in *2019 IEEE International Systems Conference (SysCon)*, 2019, pp. 1–8.

[8] J. M. Anderson, N. Kalra, K. D. Stanley, P. Sorensen, C. Samaras, and T. A. Oluwatola, *Autonomous Vehicle Technology: A Guide for Policymakers*. Santa Monica, CA: RAND Corporation, 2016.

[9] S. Hung, X. Zhang, A. Festag, K. Chen, and G. Fettweis, "Vehicle-Centric Network Association in Heterogeneous Vehicle-to-Vehicle Networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 5981–5996, 2019.

[10] I. Yaqoob, K. Salah, M. Uddin, R. Jayaraman, M. Omar, and M. Imran, "Blockchain for Digital Twins: Recent Advances and Future Research Challenges," *IEEE Network*, vol. 34, no. 5, pp. 290–298, 2020.

[11] C. B. S. T. Molina, J. R. d. Almeida, L. F. Vismari, R. I. R. González, J. K. Naufal, and J. Camargo, "Assuring Fully Autonomous Vehicles Safety by Design: The Autonomous Vehicle Control (AVC) Module Strategy," in *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, 2017, pp. 16–21.

[12] S. Mihai, P. Shah, G. Mapp, H. Nguyen, and R. Trestian, "Towards Autonomous Driving: A Machine Learning-based Pedestrian Detection System using 16-Layer LiDAR," in *2020 13th International Conference on Communications (COMM)*, 2020, pp. 271–276.

[13] J. Henriksson, M. Borg, and C. Englund, "Automotive Safety and Machine Learning: Initial Results from a Study on How to Adapt the ISO 26262 Safety Standard," in *2018 IEEE/ACM 1st International Workshop on Software Engineering for AI in Autonomous Systems (SEFAIAS)*, 2018, pp. 47–49.

[14] M. Steger, M. Karner, J. Hillebrand, W. Rom, and K. Römer, "A Security Metric for Structured Security Analysis of Cyber-physical Systems Supporting SAE j3061," in *2016 2nd International Workshop on Modelling, Analysis, and Control of Complex CPS (CPS Data)*, 2016, pp. 1–6.

[15] W. Jeon, Z. Xie, A. Zemouche, and R. Rajamani, "Simultaneous Cyber-Attack Detection and Radar Sensor Health Monitoring in Connected ACC Vehicles," *IEEE Sensors Journal*, pp. 1–1, 2020.

2021-03-31

Digital twin analysis to promote safety and security in autonomous vehicles

Almeaibed, Sadeq

IEEE

Almeaibed S, Al-Rubaye S, Tsourdos A , Avdelidis NP. (2021) Digital twin analysis to promote safety and security in autonomous vehicles. IEEE Communications Standards Magazine, Volume 5, Issue 1, March 2021, pp. 40-46

https://doi.org/10.1109/MCOMSTD.011.2100004