Politecnico di Torino

Master of Science in Computer Engineering

Tesi di Laurea Magistrale

Rethinking Automotive Software Development: Exploring Software Defined Vehicle and its potential

Supervisors
prof. Danilo Bazzanella
dott.sa Piera Limonet

Candidate
Lorenzo Sciara

Anno Accademico 2023-2024

Summary

This thesis project delves into the analysis of contemporary connected vehicle platforms, focusing on the benefits and challenges associated with these advanced solutions and emphasising aspects of safety and flexibility. A key trend in the current automotive sector is the prospect of transforming the car from a hardware-focused product to a software-driven device. The technology of choice for leading software development and production companies driving this change is the Software Defined Vehicle (SDV).

The primary objective of the thesis is to apply this paradigm to the development of a simulator for a vehicle control unit responsible for collecting telemetric data from the vehicle. The implementation of the simulator involves an in-depth analysis of the drawbacks of the automotive software production industry and the advantages of the Software Defined Vehicle solution. The simulator implementation also includes the creation of a scaled-down version of a connected vehicle platform, storage infrastructure and example application.

Using the Amazon Web Services (AWS), an environment in the cloud is established for the development of the necessary software for the operation of the vehicle control unit. Development of the vehicle control unit simulator is carried out, including client connectivity to interact with the cloud platform, telemetry generation, logic for remote operations, and optional applications. The final phase involves testing the simulator on compatible hardware to validate its functionality and performance.

The successful completion of this project in collaboration with Storm Reply, not only highlights the potential of the software-defined vehicle paradigm as a leading force in the future of the automotive sector, but also explores the economic, safety and security benefits associated with its adoption, paving the way for significant progress in the field and ensuring an advanced and safe end-user experience.

Acknowledgements

Acknowledgement (optional)

Contents

List of Figures

List of Tables

Listings

Chapter 1

Introduction

1.1 Context

The automotive industry stands out as one of the fastest-growing sectors, playing a significant role as both an employer and an investor in research and development; at the same time, it represents one of the most crucial domains for the European Union's economy. As reported in the article [1], in 2015, 21 million motor vehicles of all types were produced in Europe, representing a 23% share in the global production of more than 90 million units.

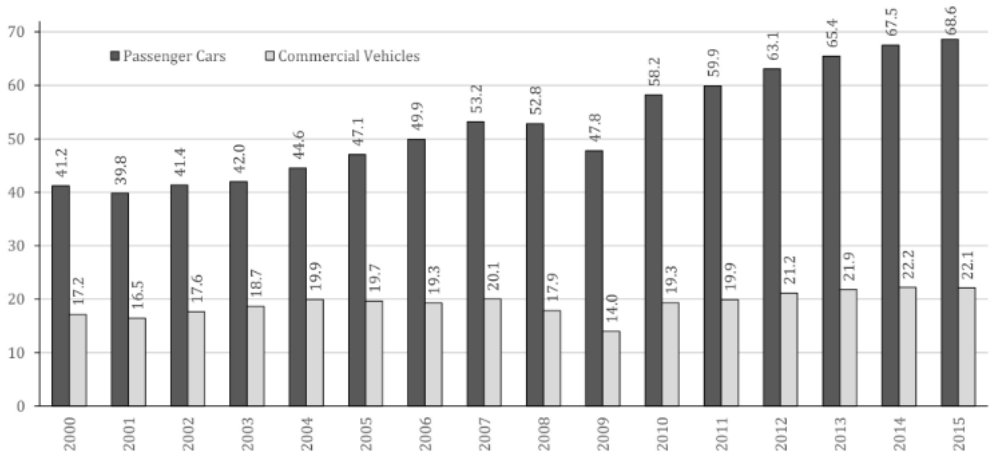

Figure 1.1. World automobile production in million vehicles [1]

In the evolving landscape of automotive technology, the imperative for automotive companies extends beyond the traditional realms of mechanical engineering to encompass a crucial reliance on both software and hardware components for vehicle construction. A glimpse into the intricate web of modern cars, as illustrated in Figure 1.2, reveals a mosaic of hundreds of distinct processors interfacing at various levels, earning contemporary vehicles the moniker of "Computers on wheels."

However, the proliferation of processors within vehicles, orchestrating communication to manage diverse components, presents a formidable challenge; each component often integrates a processor with unique logics, diverging from the logics

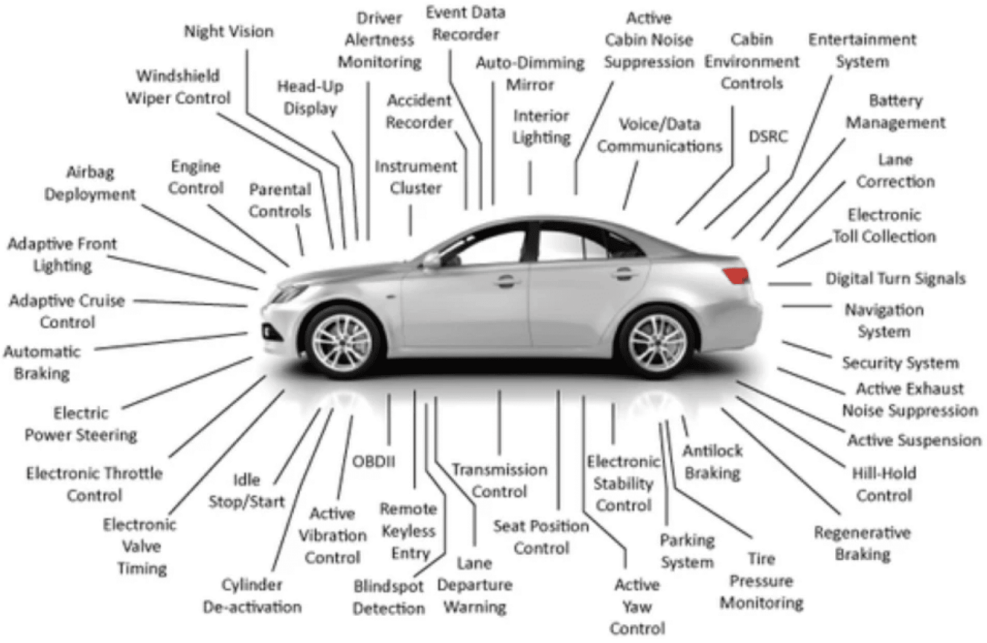

Figure 1.2. An incomplete overview of computers in a modern car [2]

embedded in processors of other components. Complicating matters further, these components are frequently supplied by companies with proprietary management logics, not readily accessible to the automotive companies themselves.

In addressing this intricate scenario, the transformative concept of a Software Defined Vehicle (SDV) comes to the forefront. Defined as "any vehicle that manages its operations, adds functionality, and enables new features primarily or entirely through software" [6], the notion of SDV offers a comprehensive solution to the challenges posed by the intricate interplay of software and hardware in modern vehicles.

Effectively navigating the development of SDV technology necessitates a collaborative approach across diverse companies, particularly in the realms of hardware and cloud computing. This collaborative synergy is exemplified in the realization of our project, made possible through the partnership with Storm Reply.

1.2 Company

Leveraging extensive experience in the cloud industry and fostering deep-rooted relationships within the automotive sector, Storm Reply stands out as the ideal choice to lead the project discussed in this thesis. A key player in the Reply group, Storm Reply specializes in designing and implementing innovative Cloud-based solutions and services [7].

With a diverse clientele spanning various sectors, notably the automotive industry, the company's expertise played a pivotal role in comprehensively understanding the project's context and internal dynamics. This profound knowledge served as the cornerstone for developing a tangible exemplification of the infrastructure.

Figure 1.3. Logo of the partenr company of the project

A point of pride for Storm Reply is its recognition as an Amazon Web Services (AWS) Premier Consulting Partner since 2014, ranking among the top Amazon Partners globally. This distinctive characteristic underscores the decision to develop the infrastructure using Amazon Web Services.

According to the official AWS description page [8] the AWS Cloud spans 102 Availability Zones within 32 geographic Regions around the world and servs 245 countries and territories. With millions of active customers and tens of thousands of partners globally, AWS has the largest and most dynamic ecosystem. AWS is evaluated as a Leader in the 2022 Gartner Magic Quadrant for Cloud Infrastructure and Platform Services, placed highest in Ability to Execute axis of measurement among the top 8 vendors named in the report.

Figure 1.4. Here are a series of market research reports published by IT consulting firm Gartner that rely on proprietary qualitative data analysis methods to demonstrate market trends, such as direction, maturity and participants. [3]

The infrastructure exhibits several key attributes contributing to its robustness and efficiency:

- **Security:** The infrastructure undergoes 24/7 monitoring to ensure the confidentiality, integrity, and availability of data. All data flowing across the AWS global network is automatically encrypted at the physical layer before leaving secured facilities.
- **Availability:** To ensure high availability and isolate potential issues, applications can be partitioned across multiple AZs (Availability Zones) within the same region, creating fully isolated infrastructure partitions.
- **Performance:** AWS Regions offer low latency, low packet loss, and high overall network quality. This is achieved through a fully redundant 100 GbE fiber network backbone, often providing terabits of capacity between Regions.

- **Scalability:** The AWS Global Infrastructure allows companies to take advantage of the virtually infinite scalability of the cloud. This enables customers to provision resources based on actual needs, with the ability to instantly scale up or down according to business requirements.
- **Flexibility:** The AWS Global Infrastructure provides flexibility in choosing where and how workloads are run, whether globally, with single-digit millisecond latencies, or on-premises.
- **Global Footprint:** AWS boasts the largest global infrastructure footprint, continually expanding at a significant rate.

1.3 Thesis Goal

In the automotive context, the use of Software Defined Vehicle (SDV) plays a crucial role in terms of costs, innovation, and safety. The goal of the thesis intertwine with the opportunities provided by Software Defined Vehicle technology, addressing the primary challenge of managing the current difficulties associated with the presence of various specialized hardware platforms on the same vehicle.

The central objective of this thesis is to propose a Software Defined Vehicle solution capable of eliminating various phases of the software production pipeline. This would result in significant time and cost savings, enabling the investment of these resources in other sectors. Since, by definition, a Software Defined Vehicle is characterized by the ability to undergo software updates dynamically and flexibly, this solution offers significant security advantages in various aspects:

1. Human Safety Critical Security: From the moment that a vehicle can be classified as safety critical (as it is reported in the standard ISO 26262-1:2018 of the ISO society where is said that "safety is one of the key issues in the development of road vehicles" [9]), the elimination of software vulnerabilities related to the vehicle's systems is crucial for the overall safety of the vehicle itself.
2. Intrinsic Software Security: This approach allows for the prevention and resolution of vulnerabilities unknown at the time of software design, contributing to ensuring a high standard of security.

Consequently, the use of Software Defined Vehicle aims to completely separate software and hardware, allowing the production of high-level software on entirely generalized hardware systems. This results in significant savings in terms of time and money for hardware production, along with providing an advantage in terms of security due to the simplification of software.

For example, as demonstrated by NIST in the research on the Analysis Of The Impact Of Software Complexity [10], the increase in software complexity in different cases results in less analyzable programs. In some instances, the same vulnerability analysis tool may detect vulnerabilities, while in others, analyzing the same code, it may not.

From a practical standpoint, the project's goal is to provide, through the use of AWS services, a cloud infrastructure capable of managing the Software Defined Vehicle both in terms of software production and data analysis.

Chapter 2

State-of-the-Art Analysis

The following chapter constitutes an in-depth exploration of current technologies and methodologies within the automotive industry, with a specific focus on the complexity of vehicular software development. Firstly, the current automotive landscape will be examined, providing a detailed insight into challenges associated with software development in vehicles.

Subsequently, through meticulous analysis of scientific publications, technical reports, and practical implementations, the chapter delves into the radical transformation of the automotive sector facilitated by the concept of Software Defined Vehicle (SDV). This technology, crucial for technological progress and vehicular safety, will be explored from various perspectives. Particularly, the synergy between Cloud, software, and hardware will be investigated, highlighting solutions proposed by major industry players and analyzing their applications, benefits, and limitations.

The objective is to offer a comprehensive overview of current dynamics, emphasizing the pivotal role of SDV in the evolution of the automotive industry.

2.1 Current Automotive Software Development

In the past, the automotive industry advanced primarily through the development of technologies in mechanical engineering, focusing on perfecting combustion engines. Nowadays, the paradigm has radically changed due to multiple factors, including electrification, automation, shared mobility, and connected mobility.

Software technology development in the automotive field can be metaphorically compared to what has happened in smartphone development, as highlighted in the manifesto document regarding Bosch's Software Defined Vehicle (SDV) [11].

The ultimate goal is to achieve simple and user-friendly devices that fully meet the user's needs. Currently, many customers express dissatisfaction because their cars do not offer the same functionality and ease of use common in smartphones. Many ask: Why can't my $50,000 car perform the same tasks as my $300 smartphone?

A key difference between the automotive and smartphone industries is the level of complexity, which brings with it a number of issues.

2.1.1 difficulties

We can analyse in depth the problems of the current automotive software that is being developed via 4 main difficulties:

- **Specialized Hardware:** Today's vehicles are still complex systems of systems. Each subsystem in a car, from brakes to transmission, is a complex entity, supplied by a different manufacturer and integrated with a unique software architecture. The level of complexity and the need for seamless interoperability between systems far exceeds that of today's smartphones.
- **Time:** The software production pipeline involves many development and testing steps with a not inconsiderable amount of time spent on each one. This is greatly increased by the presence of different components, so development time must be considered for each different unit of the system.
- **Cost:** The complexity of the software systems in vehicles entails very high costs, aggravated by the fact that the test phase is often carried out directly on the boards (for hardware requirements), which means a much longer production process, especially in the event of errors.

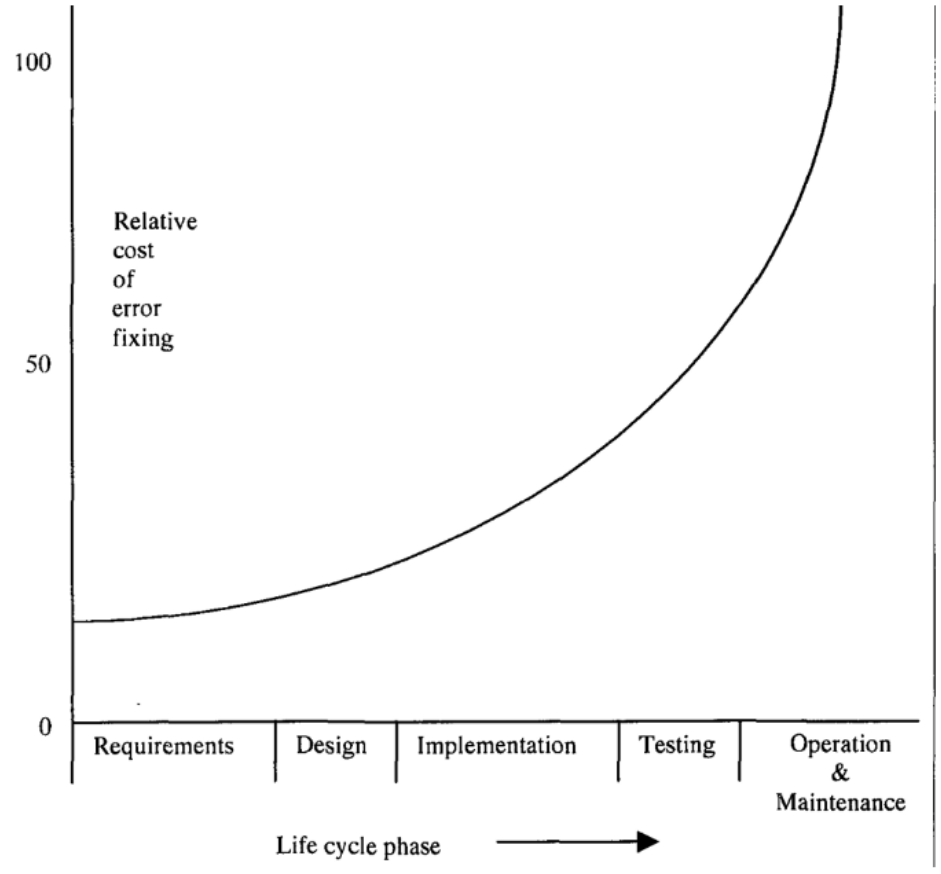

Figure 2.1. Cost of fixing errors increases in later phases of the life cycle [4]

- **Human Safety Security:** Automotive embedded software must meet stringent reliability and security requirements, while delivering performance and a reasonable memory footprint. To develop automotive embedded software, you need the right tools that meet safety and security standards to evaluate, prototype and test your software.

What lessons can be drawn from the study of barriers that can be applied to the vehicle lifecycle? Historically, the vehicle lifecycle has been characterised by the simultaneous production and deployment of tightly integrated hardware and software. Once the vehicle was in the hands of the consumer, its characteristics remained largely unchanged until the end of its life. However, the SDV paradigm introduces the possibility of decoupling hardware and software release dates, a prerequisite for adopting a digital-first approach. This approach brings the design and virtual validation of the digital vehicle experience to the forefront of the lifecycle. It also requires the application of the digital-first concept, which means that new ideas for the vehicle experience are first explored in virtual environments to ensure early user feedback, long before any custom hardware needs to be developed or a physical test vehicle is available. Digital first is the application of design thinking and lean startup principles, originally rooted in internet culture, to the tangible realm of automotive development.

2.2 Introduction to Software Defined Vehicle

The Software Defined Vehicle represents the new frontier of automotive manufacturing and is poised to completely change the paradigm of automotive production.

If we imagine bringing a feature update to one of today's vehicles, it will most likely take anywhere from one to seven years from the idea to when that feature is actually perceptible in the production vehicle; this takes so long because the vehicles produced up to this point have not been designed with frequent updates in mind [12]. Traditionally focused on physical functionality, the automotive industry has evolved from early electronic features such as airbags, vehicle stabilisation and braking systems to modern driver assistance and even automated driving. The current shift towards a digital experience is possible thanks to vehicle design that includes software integration as a fundamental part. Software should no longer be seen as an accessory to the vehicle, but as an integral part of the vehicle itself.

The simultaneous efforts of major automotive companies such as Bosch, Renault and Stellantis, in collaboration with leading computer developers such as Arm, BlackBerry and AWS, have given rise to the Software Defined Vehicle concept, which they define as "any vehicle that manages its own operations, adds functionality and enables new features primarily or entirely through software" [6].

The Software Defined Vehicle solution is nowadays being considered by several companies as the manifesto of a new era of vehicle development. An example is given by the Renault Group, which in an overview of its products describes: "Today, it is already possible to make remote updates of some vehicles via the Firmware Over The Air (FOTA) system. This keeps the vehicle safe by making it

easier and faster to improve the on-board system and apply patches. Tomorrow, the Software Defined Vehicle's flexible and scalable architecture will enable the faster development and integration of new features throughout the vehicle lifecycle, directly into the cloud, that is, in secure online servers accessible from anywhere and anytime" [13].

It is evident that Software Defined Vehicles represent the future of the automotive industry, promising an enriched and sustainable user experience as vehicle technologies evolve. This section further clarifies the current state of the industry, highlighting the key enablers that are allowing the development of the SDV paradigm and the benefits of this innovation.

2.2.1 Enablers

There are mainly three fundamental technologies that contribute to the realisation of the Software Defined Vehicle: standardized hardware, cloud and over-the-air (OTA) updates via OTA servers, all developed by leading companies in the computing industry. In this section, each technology will be analysed with reference to concrete examples from the current market.

- **Standardized hardware**

  One of the most important aspects of Software Defined Vehicle is the separation of software from hardware. To achieve this, it is essential to move away from the approach of using dedicated hardware for each vehicle component system, and instead favour an approach based on general purpose processors that are as centralised as possible. This transition not only promotes ease of software development and scalability, but also offers the opportunity to create parity between the virtual development and test environment and the real execution environment.

  Several players in the semiconductor industry have stepped up to the challenge of realising this vision, including Arm. Through the development of energy-efficient processors, Arm is present in every part of the vehicle, from high-performance systems in advanced driver assistance systems (ADAS), automated driving (AD), in-vehicle infotainment (IVI) and digital cockpits, to gateway, body and microcontroller endpoints [14]. The aim is to create Arm-based MCUs that enable implementation of a common architecture, scalability between applications to meet processing requirements, software reuse and reduced development costs.

  Another major player is Qualcomm, which is being adopted by the Renault Group through its Snapdragon Digital Chassis vehicle architecture, a set of cloud-connected platforms for telematics and connectivity, digital cockpits, assistance and driver autonomy.

- **Cloud**

  Using a cloud platform that offers scalable and secure solutions for real-time application updates, increased connectivity and efficient data management is essential for SDV.

Well-known companies such as Amazon Web Services (AWS) and Google Cloud are already present in the automotive industry as partners of partner of many automotive companies. The AWS services and technologies will be in depth described in the futher chapters.

- **Over-The-Air updates**

  An Over-The-Air (OTA) update is the remote and wireless transfer of applications, services, firmware and configurations from a server to a target device. This process takes place over an available network, preferably the Internet. The main purposes of OTA are to remotely update software or firmware, provide power-safe procedures to ensure that the device will boot even if power is lost during the update process, maintain a robust implementation, ensure data protection and reduce overall maintenance costs [15].

  In the context of the thesis, it is crucial to acknowledge that the implementation of OTA updates may increase the vulnerability of automotive systems to hacking and other cyber attacks. These vulnerabilities could potentially be exploited by hackers to gain unauthorised access to private information, take remote control of the vehicle or even cause it to malfunction. Another significant issue is the leakage of information about updates and their sources. This can enable malicious actors to introduce viruses and malware, further exacerbating the security risks associated with OTA updates [16].

  To perform an OTA update, both a client on the vehicle, responsible for waiting and checking for incoming updates, and a server, facilitating the availability of the update broadcast to all connected devices, are essential. In this context, Autosar can be considered, as it represents a standard and open source architecture for intelligent mobility [17], which includes a dedicated platform for client and server management of OTA updates. Another notable example is Hawkbit, which serves as a backend framework for deploying software updates to edge devices and is being developed by the Eclipse Foundation; this tool will be discussed in more detail in later chapters as it will be used to create a proof of concept. The final tool of note is AWS Greengrass, an edge agent manager for managing software updates in edge IoT devices, provided by AWS; this tool will also be discussed in later chapters as an alternative solution to the client manager.

- **MQTT communication**

  The Message Queuing Telemetry Transport (MQTT) is a standardized protocol, specified by ISO/IEC 20922:2016 and developed by the Oaesis organization. It enables the exchange of Application Messages over a network connection, providing an ordered, lossless stream of bytes from the Client to Server and Server to Client without the need to support of a specific transport protocol.

  In an MQTT transport, an Application Message carries payload data, a Quality of Service (QoS), a collection of Properties, and a Topic Name. Clients, which can be programs or devices, perform various actions such as opening and closing network connections, publishing Application Messages, subscribing to requested Application Messages, and managing subscriptions [18].

On the Server side, it acts as an intermediary between publishing and subscribing Clients. The Server accepts network connections, processes Subscribe and Unsubscribe requests, and forwards Application Messages matching Client Subscriptions. The Server, also known as the Broker, essentially coordinates messages among various Clients. Its responsibilities extend to authorizing and authenticating MQTT Clients, transmitting messages to other systems for further analysis, and managing tasks such as handling missed messages and Client sessions [19].

Sessions, representing stateful interactions between Clients and Servers, can last for the duration of a Network Connection or span multiple consecutive connections.

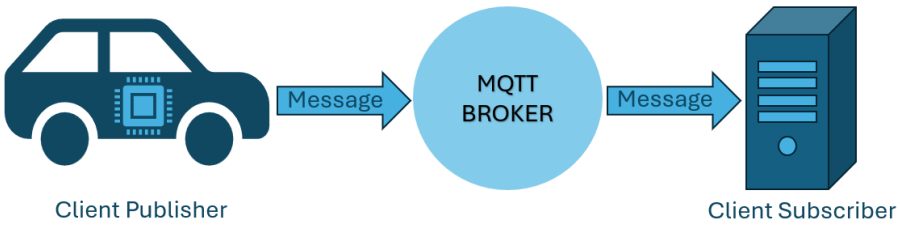

Figure 2.2. A simple representation of communication using the MQTT protocol

The MQTT protocol can be used in SDV, both for sending data produced by the vehicle to the cloud servers and for sending updates from the servers to the vehicle. This is because the MQTT protocol allows asynchronous and misaligned communication even in the presence of poor connectivity, a situation that cannot be underestimated in the automotive field.

The collaborative efforts of this technologies contribute to advancement of SDV for makeing vehicles not only defined by their physical attributes but also as dynamic entities that can be continuously updated through software.

2.2.2 Benefits

The Software Defined Vehicle, as introduced in the previous chapters, brings several benefits to both automotive companies and the end-user experience. These innovations are made possible by the fact that the vehicle becomes a device that can be constantly monitored and updated in real time via the cloud throughout its entire lifecycle. Let us now look at the key benefits.

From the point of view of this project, the main innovation brought by this technology is the security of the device software. Since, as mentioned above [9],

vehicles are considered as safety elements critical to human life, the safety benefits can be analysed from two perspectives:

- **Human Safety Critical Security:** The ability of SDV to receive real-time data from the vehicle allows in-depth monitoring of all its components. Taking the influence of tyres as an example, it has been found that most road accidents are caused by tyre wear and lack of regular maintenance. It is therefore necessary to assess the health of tyres through continuous monitoring of physical parameters such as tyre thickness, temperature and pressure, as well as regular maintenance. This helps to eliminate or minimise the possibility of tyre bursts and subsequent accidents. It also improves the safety of people and vehicles [20]. These factors can be monitored either manually or automatically: manual predictive maintenance requires human intervention and can lead to some errors; automatic predictive maintenance using artificial intelligence can be more efficient [21]. Renault defines this work as "predictive maintenance" [13], stressing the importance of collecting and analysing data in a centralised system to anticipate and prevent potential failures, ensure the safety of people, reduce maintenance costs and improve the performance of the vehicle.

- **Intrinsic Software Security:** In the presence of bugs and vulnerabilities in the vehicle's software, SDV makes it possible to intervene promptly to resolve each problem and reduce the window of exposure.

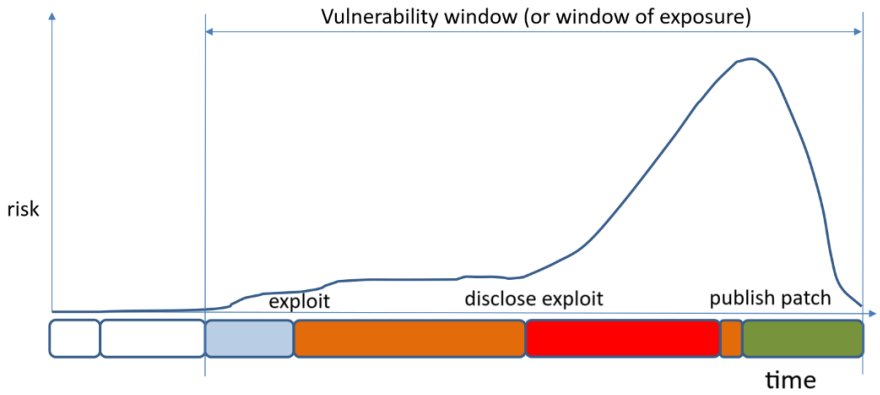

Figure 2.3. Risks and time relationship in the various phases of a vulnerability lifecycle

A crucial aspect of vehicle software security is the robustness of the algorithms, especially in the context of autonomous driving. In this context, a predictive algorithm responsible for vehicle safety decisions can be continuously improved and optimised. The SDV also introduces the concept of the 'digital twin', a platform that virtually replicates the functionality and behaviour of the vehicle. Thanks to this technology, predictive algorithms used in autonomous driving can be effectively tested on the cloud platform and, when ready, integrated directly into the vehicle.

From a user experience point of view, two other significant benefits can be identified: an increase in the value of the vehicle, which can be continuously upgraded over time, and the ability to enable additional vehicle functions via software. For example, the user can decide to activate a feature for a certain period of time and then deactivate it (paying only for the time it is used), or activate a new feature that was not available at the time of purchase. In essence, the vehicle becomes a dynamic platform that is constantly evolving and fully customisable through the software.

For automotive companies, the benefits mentioned so far can bring direct benefits to the industry. In support of this, Stellantis reports that: "the team in Poland will contribute to the global software creation network that is key to Stellantis' work in creating software-defined vehicles (SDVs) that offer customer-focused features throughout the vehicle's life span, including updates and features that will be added years after the vehicle is manufactured. "Creating an infrastructure inside our vehicles that easily and seamlessly adapts to meet driver expectations is a key element of Stellantis' global drive to deliver cutting edge mobility. Stellantis' software-driven strategy deploys next-generation tech platforms, building on existing connected vehicle capabilities to transform how customers interact with their vehicles and to generate €20 billion in incremental annual revenues by 2030".

In addition, the SDV paradigm brings an advantage from a software production pipeline perspective. In today's software production scenario, there can be two development mechanisms:

- A more traditional mode in which software is created directly on the system, hence on the processor itself. This is undoubtedly the most inconvenient solution, as it would require unnecessary overuse of processors, wasting resources, money and time.
- Alternatively, developers rely on cumbersome operating system emulation tools on the host machine and the cross-compilation process, which uses a dedicated compiler to produce executable code for the target system. Once the code is on the development system, a final integration and validation test can be performed, but scalability is limited to the number of physical hardware platforms.

Typical workflows for the development, integration and validation of embedded systems are as follows [22]:

As explained in the following chapters, by using the software defined vehicle, i.e. operating systems that rely on general purpose porpouse architectures to provide parity between cloud and edge systems, it is possible to reduce the embedded developer's workflow to remove many of the steps that are now no longer required, as shown in the diagram below [22]:

2.2.3 initiatives: SOAFEE

In 2021 Arm, AWS, and other founding members announced the Scalable Open Architecture for Embedded Edge (SOAFEE) Special Interest Group, which brings

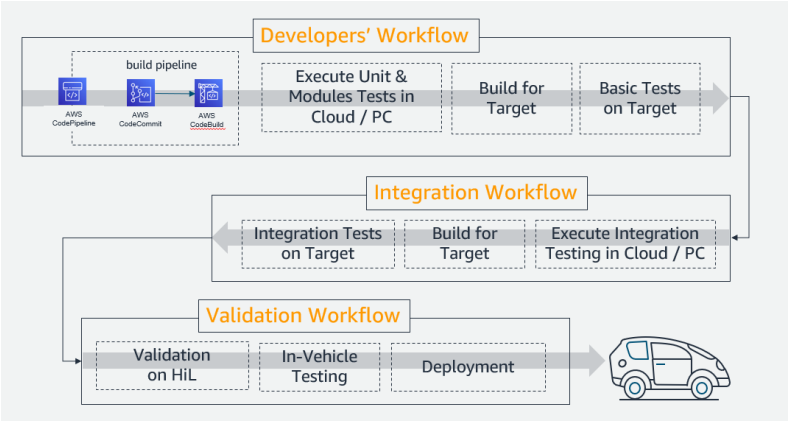

Figure 2.4. today development, integration, and validation workflows for embedded systems

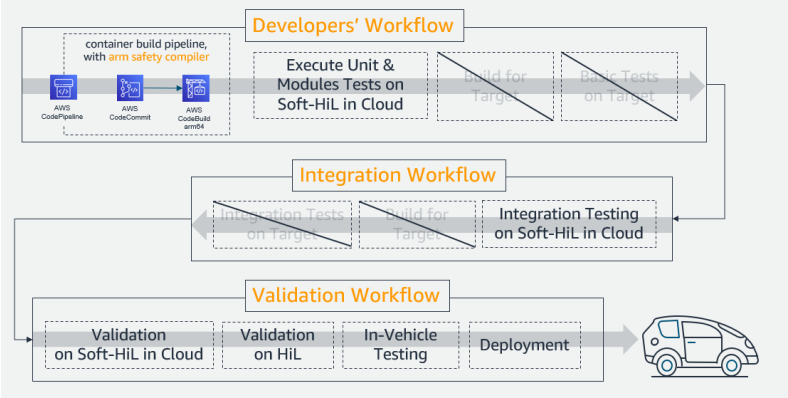

Figure 2.5. future development, integration, and validation workflows for embedded systems

together automakers, semiconductor, and cloud technology leaders to define a new open-standards based architecture to implement the lowest levels of a software-defined vehicle stack. [22]

SOAFE is created to achive Software Defined Vehicle, and for doing that four-pillar principle are used [23]:

1. Standards: standardization ensures interoperability and compatibility among various software components, fostering a cohesive ecosystem for Software Defined Vehicles.

2. New software architecture and methodologies: this involves transitioning from traditional monolithic architectures to more modular and scalable designs; the incorporation of agile development practices and DevOps methodologies ensures efficient and continuous software evolution.

3. Industry collaboration: Fostering partnerships, knowledge sharing and collaboration among key stakeholders, including automakers, technology companies and regulators, is essential.

4. Vehicle simulation: simulated environments allow in-depth testing and refinement of software functionality to ensure optimal performance and security under a variety of conditions.

SOAFEE aims to adopt and enhance current standards used in today's cloud-native world to help manage the software and hardware complexity of the automotive Software Defined Vehicle architecture.

The core principles of safety, security, and real time are inherent in each pillar. It is fully expected that the SOAFEE architecture will support use-cases that execute safety-critical services alongside non-safety-critical ones. It is fully expected that the SOAFEE architecture will support use cases that execute safety-critical services alongside non-safety-critical services. As it is not reasonable to develop the whole platform according to one safety standard, the strategy is to develop only safety-critical elements according to ISO 26262 and to isolate them from the non-safety-critical elements in order to ensure spatial, temporal and communication isolation. All implementations pass security checks and follow a set of best practices /citeSoafeeArchitectureOverview.

The SOAFEE paradigm is based on a very sophisticated architecture becouse it should work in the same way in the vehicle and in the cloud and follow cloud native technologies while considering the automotive specific needs for safety and limited resource footprints [5].

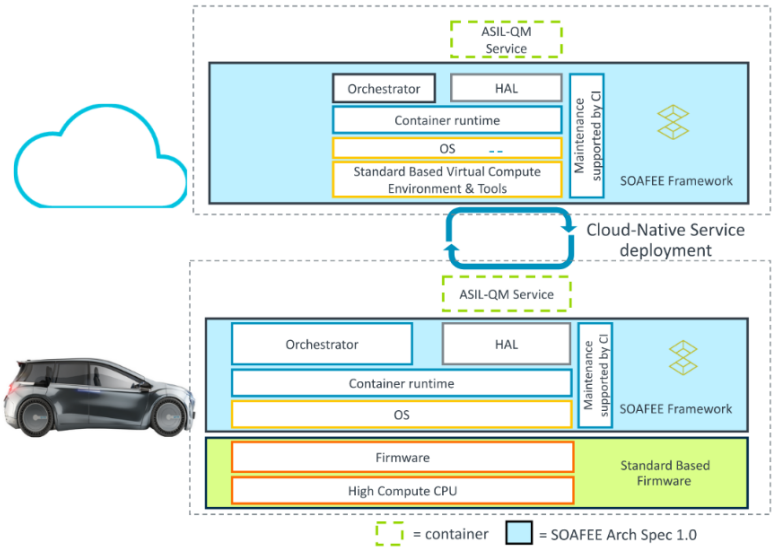

Figure 2.6. SOAFEE Architecture v1.0 [5]

Chapter 3

Proof Of Concept

As the analysis in previous chapters has shown, the Software Defined Vehicle is a pivotal advancement in the evolution of the entire automotive industry toward a safer, more efficient, and more sustainable future. This chapter explores the Proof of Concept (PoC) phase within the context of the thesis, aiming to validate the feasibility and efficacy of implementing SDV technologies. The main objective of this chapter is to translate theoretical concepts into concrete results, demonstrating the practical application of SDV in real-world situations. Through the PoC, we aim to confirm the fundamental principles and features of SDV, including its potential impact on vehicle performance, user experience, and overall safety. The multifaceted nature of SDV requires a structured approach to its implementation, taking into account factors such as standardized hardware, cloud integration, and over-the-air (OTA) updates. To achieve this, a PoC was designed to address these components individually and holistically, ensuring a seamless integration that aligns with the envisioned paradigm shift in automotive manufacturing. Furthermore, this chapter aims to demonstrate the collaborative efforts with industry-leading technologies and platforms, highlighting the strategic partnerships forged with key players in the automotive and software development sectors. By aligning with renowned entities, the PoC aims to leverage their expertise, technologies, and frameworks, thereby enhancing the robustness and scalability of the SDV ecosystem. Test and Validation are the concluding phases of this chapter, where the Proof of Concept is subjected to real-world scenarios. A demonstration involving a Raspberry Pi (RPi) serves as a tangible validation of the implemented SDV functionalities. This section serves as the litmus test, affirming the seamless orchestration of SDV within the envisioned architecture. The exploration of the POC begins by detailing the services and technologies offered by Amazon Web Services (AWS) in the IoT and automotive fields that are essential for project implementation.

3.1 Amazon Web Services

Amazon Web Services (AWS) is a widely adopted cloud solution with over 200 fully featured services available globally across multiple data centers. It is used by millions of customers, from emerging startups to industry giants and government agencies, as the cloud platform of choice to reduce costs, increase agility, and

accelerate innovation [24].

AWS stands out by providing a broad set of services, including infrastructure technologies as well as cutting-edge capabilities such as machine learning, artificial intelligence, data lakes, analytics, and the Internet of Things. This extensive service portfolio facilitates the fast, easy and cost-effective migration of existing applications to the cloud and the creation of diverse digital solutions. AWS provides purpose-built databases for various application types, allowing users to choose the most suitable tool for optimal cost and performance. The depth of AWS services is unmatched, providing customers with a comprehensive toolkit for diverse computing needs.

Beyond its vast offerings, AWS has a large and dynamic global community with millions of active customers and tens of thousands of partners. This inclusive ecosystem spans industries and business sizes, with startups, enterprises, and public sector entities leveraging AWS for a myriad of use cases. The AWS Partner Network (APN) solidifies this network with thousands of system integrators and independent software vendors who adapt their technology to work on AWS.

AWS demonstrates its commitment to innovation through continuous technological advancements. In 2014, AWS launched AWS Lambda, which pioneered serverless computing. This allows developers to run their code without the need to provision or manage servers. Another example is Amazon SageMaker, a fully managed machine learning service that empowers developers to use machine learning without any previous experience.

Rooted in more than 17 years of operational experience, AWS offers unmatched reliability, security, and performance [25]. Since its establishment in 2006, AWS has become a globally trusted platform, revolutionizing IT infrastructure services by providing a highly reliable, scalable, and cost-effective cloud solution for businesses worldwide in the form of web services with pay-as-you-go pricing [26]. As analyzed below, one of the key benefits of cloud computing is the ability to replace a company's initial capital expenditures required for infrastructure with low costs that vary as needed and can scale with the business.

3.1.1 Cloud Computing

What is cloud computing? Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, you can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider like Amazon Web Services (AWS). Organizations of every type, size, and industry are using the cloud for a wide variety of use cases, such as data backup, disaster recovery, email, virtual desktops, software development and testing, big data analytics, and customer-facing web applications. For example, healthcare companies are using the cloud to develop more personalized treatments for patients. Financial services companies are using the cloud to power real-time fraud detection and prevention. And video game makers are using the cloud to deliver online games to millions of players around the world. The cloud gives you easy access to a broad range of technologies so that you can innovate faster and build

nearly anything that you can imagine. You can quickly spin up resources as you need them-from infrastructure services, such as compute, storage, and databases, to Internet of Things, machine learning, data lakes and analytics, and much more. You can deploy technology services in a matter of minutes, and get from idea to implementation several orders of magnitude faster than before. This gives you the freedom to experiment, test new ideas to differentiate customer experiences, and transform your business. With cloud computing, you don't have to over-provision resources up front to handle peak levels of business activity in the future. Instead, you provision the amount of resources that you actually need. You can scale these resources up or down to instantly grow and shrink capacity as your business needs change. The cloud allows you to trade fixed expenses (such as data centers and physical servers) for variable expenses, and only pay for IT as you consume it. Plus, the variable expenses are much lower than what you would pay to do it yourself because of the economies of scale. With the cloud, you can expand to new geographic regions and deploy globally in minutes. For example, AWS has infrastructure all over the world, so you can deploy your application in multiple physical locations with just a few clicks. Putting applications in closer proximity to end users reduces latency and improves their experience. The three main types of cloud computing include Infrastructure as a Service, Platform as a Service, and Software as a Service. Each type of cloud computing provides different levels of control, flexibility, and management so that you can select the right set of services for your needs [27]:

- Infrastructure as a Service (IaaS): IaaS contains the basic building blocks for cloud IT. It typically provides access to networking features, computers (virtual or on dedicated hardware), and data storage space. IaaS gives you the highest level of flexibility and management control over your IT resources. It is most similar to the existing IT resources with which many IT departments and developers are familiar.

- Platform as a Service (PaaS): PaaS removes the need for you to manage underlying infrastructure (usually hardware and operating systems), and allows you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application.

- Software as a Service (SaaS): SaaS provides you with a complete product that is run and managed by the service provider. In most cases, people referring to SaaS are referring to end-user applications (such as web-based email). With a SaaS offering, you don't have to think about how the service is maintained or how the underlying infrastructure is managed. You only need to think about how you will use that particular software.

3.1.2 Security

AWS is architected to be the most flexible and secure cloud computing environment available today. Our core infrastructure is built to satisfy the security requirements for the military, global banks, and other high-sensitivity organizations. This is

backed by a deep set of cloud security tools, with over 300 security, compliance, and governance services and features, as well as support for 143 security standards and compliance certifications.

AWS infrastructure has been architected to be one of the most flexible and secure cloud computing environments available today. It is designed to provide an extremely scalable, highly reliable platform that enables customers to deploy applications and data quickly and securely. This infrastructure is built and managed not only according to security best practices and standards, but also with the unique needs of the cloud in mind. AWS uses redundant and layered controls, continuous validation and testing, and a substantial amount of automation to ensure that the underlying infrastructure is monitored and protected 24x7. IT Security is often not the core business of our customers. IT departments operate on limited budgets and do a good job of securing their data centers and software given limited resources. In the case of AWS, security is foundational to our core business and so significant resources are applied to ensuring the security of the cloud and helping our customers ensure security in the cloud, as described further below [28].

Strong security at the core of an organization enables digital transformation and innovation. AWS helps organizations to develop and evolve security, identity, and compliance into key business enablers. At AWS, security is our top priority. AWS is architected to be the most secure global cloud infrastructure on which to build, migrate, and manage applications and workloads. This is backed by our deep set of 300+ cloud security tools and the trust of our millions of customers, including the most security sensitive organizations like government, healthcare, and financial services.

We innovate on behalf of our customers so they can move quickly, securely, and with confidence to enable their business. With AWS cloud infrastructure, and our broad set of security services, and partners, our customers integrate powerful security technology and control to enable their business to innovate securely. Build, run, and scale your applications on infrastructure architected to be the most secure cloud computing environment available today. As organizations migrate and build on cloud, they need assurance that they have a secure foundation. AWS has the most proven operational experience of any cloud provider. Our cloud infrastructure is highly trusted and secure-by-design, giving customers the confidence to accelerate innovation. Move fast and stay secure by confidently integrating and automating security into every part of your organization. Building securely should be the path of least resistance - with no tradeoff between security with speed. With security automation, teams spend their limited time on the highest value tasks, reduce human error, and scale security best practices across the organization. Innovate with a wide portfolio of security services and partner solutions to help achieve end-to-end security for your organization. Organizations require powerful capabilities, designed and built by experts, which encode years of experience, knowledge and best practices, all available at their fingertips. They don't want to navigate this changing threat and compliance landscape alone [29].

The AWS global infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards. With AWS, you can be assured that you are building web architectures on top of some of the

most secure computing infrastructure in the world. The IT infrastructure that AWS provides to you is designed and managed in alignment with security best practices and a variety of IT security standards including the following that life science customers may find most relevant [30]:

- SOC 1, 2, 3: AWS System and Organization Controls (SOC) Reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help you and your auditors understand the AWS controls established to support operations and compliance. The SOC 1 reports are designed to focus on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements. The AWS SOC 1 report is designed to cover specific key controls likely to be required during a financial audit, as well as covering a broad range of IT general controls to accommodate a wide range of usage and audit scenarios. The AWS SOC1 control objectives include security organization, employee user access, logical security, secure data handling, physical security and environmental protection, change management, data integrity, availability and redundancy and incident handling. The SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. These principles define leading practice controls relevant to security, availability, processing integrity, confidentiality, and privacy applicable to service organizations such as AWS. The AWS SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the criteria for the security and availability principles set forth in the AICPA's Trust Services Principles criteria. This report provides additional transparency into AWS security and availability based on a pre-defined industry standard of leading practices and further demonstrates the commitment of AWS to protecting customer data. The SOC2 report information includes outlining AWS controls, a description of AWS Services relevant to security, availability and confidentiality as well as test results against controls. You will likely find the SOC 2 report to be the most detailed and relevant SOC report as it relates to GxP compliance. AWS publishes a Service Organization Controls 3 (SOC 3) report. The SOC 3 report is a publicly-available summary of the AWS SOC 2 report. The report includes the external auditor's assessment of the operation of controls (based on the AICPA's Security Trust Principles included in the SOC 2 report), the assertion from AWS management regarding the effectiveness of controls, and an overview of AWS Infrastructure and Services.

- FedRAMP: The Federal Risk and Authorization Management Program (FedRAMP) is a US government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP uses the NIST Special Publication 800 series and requires cloud service providers to receive an independent security assessment conducted by a third-party assessment organization (3PAO) to ensure that authorizations are compliant with the Federal Information Security Management Act (FISMA).

- ISO 9001: ISO 9001:2015 outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures required to achieve effective quality management within an organization. Specific sections of the standard contain information on topics such as: Requirements for a quality management system (QMS), including documentation of a quality manual, document control, and determining process interactions; Responsibilities of management; Management of resources, including human resources and an organization's work environment; Service development, including the steps from design to delivery; Customer satisfaction; Measurement, analysis, and improvement of the QMS through activities like internal audits and corrective and preventive actions. The AWS ISO 9001:2015 certification directly supports customers who develop, migrate and operate their quality-controlled IT systems in the AWS cloud. You can leverage AWS compliance reports as evidence for your own ISO 9001:2015 programs and industry-specific quality programs, such as GxP in life sciences and ISO 131485 in medical devices.

- ISO/IEC 27001: ISO/IEC 27001:2013 is a widely-adopted global security standard that sets out requirements and best practices for a systematic approach to managing company and customer information that's based on periodic risk assessments appropriate to ever-changing threat scenarios. In order to achieve the certification, a company must show it has a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information. This widely-recognized international security standard specifies that AWS do the following: We systematically evaluate AWS information security risks, taking into account the impact of threats and vulnerabilities; We design and implement a comprehensive suite of information security controls and other forms of risk management to address customer and architecture security risks; We have an overarching management process to ensure that the information security controls meet our needs on an ongoing basis. AWS has achieved ISO 27001 certification of the Information Security Management System (ISMS) covering AWS infrastructure, data centers, and services.

- ISO/IEC 27017: ISO/IEC 27017:2015 provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO/IEC 27002 and ISO/IEC 27001 standards. This code of practice provides additional information security controls implementation guidance specific to cloud service providers. The AWS attestation to the ISO/IEC 27017:2015 standard not only demonstrates an ongoing commitment to align with globally-recognized best practices, but also verifies that AWS has a system of highly precise controls in place that are specific to cloud services.

- ISO/IEC 27018: ISO 27018 is the first International code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed

by the existing ISO 27002 control set. AWS has achieved ISO 27018 certification, an internationally recognized code of practice, which demonstrates the commitment of AWS to the privacy and protection of your content.

- HITRUST: The Health Information Trust Alliance Common Security Framework (HITRUST CSF) leverages nationally and internationally accepted standards and regulations such as GDPR, ISO, NIST, PCI, and HIPAA to create a comprehensive set of baseline security and privacy controls. HITRUST has developed the HITRUST CSF Assurance Program, which incorporates the common requirements, methodology, and tools that enable an organization and its business partners to take a consistent and incremental approach to managing compliance. Further, it allows business partners and vendors to assess and report against multiple sets of requirements. Certain AWS services have been assessed under the HITRUST CSF Assurance Program by an approved HITRUST CSF Assessor as meeting the HITRUST CSF Certification Criteria. The certification is valid for two years, describes the AWS services that have been validated, and can be publiccaly accessed. You may look to leverage the AWS HITRUST CSF certification of AWS services to support your own HITRUST CSF certification, in complement to your GxP compliance programs.

- CSA Security, Trust and Assurance Registry (STAR): In 2011, the Cloud Security Alliance (CSA) launched STAR, an initiative to encourage transparency of security practices within cloud providers. The CSA Security, Trust and Assurance Registry (STAR) is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or are considering. AWS participates in the voluntary CSA Security, Trust and Assurance Registry (STAR) Self-Assessment to document AWS compliance with CSA-published best practices. AWS publishes the completed CSA Consensus Assessments Initiative Questionnaire (CAIQ) on the AWS website.

GxP is an acronym that refers to the regulations and guidelines applicable to life sciences organizations that make food and medical products such as drugs, medical devices, and medical software applications. The overall intent of GxP requirements is to ensure that food and medical products are safe for consumers and to ensure the integrity of data used to make product-related safety decisions. The term GxP encompasses a broad range of compliance-related activities such as Good Laboratory Practices (GLP), Good Clinical Practices (GCP), Good Manufacturing Practices (GMP), and others, each of which has product-specific requirements that life sciences organizations must implement based on the 1) type of products they make and 2) country in which their products are sold. When life sciences organizations use computerized systems to perform certain GxP activities, they must ensure that the computerized GxP system is developed, validated, and operated appropriately for the intended use of the system. [31]

3.1.3 Used services

3.2 Design

3.2.1 Architecture

3.3 Implementation

3.3.1 Code

3.3.2 Tools

3.4 Test and Validation

3.4.1 RPi demo

Chapter 4

Conclding Remarks

4.1 Contribution Recaps

4.1.1 Have we meet the PoC goals?

4.2 Future Works

4.2.1 Transform the poc in a product

4.2.2 Virtual workbenches

4.2.3 Manage additional Use Cases (ML, Cockpit Apps, remote ECU etc..)

Chapter 5

Conclusions

Bibliography

[1] Vošta and Kocourek, "Competitiveness of the european automobile industry in the global context." *Politics in Central Europe*, vol. 13, no. 1, pp. 69–89, 2017. [Online]. Available: https://www.politicsincentraleurope.eu/documents/file/PCE_2017_1_13.pdf#page=71

[2] R. Saracco, "Sdv: Software defined vehicles," 2021. [Online]. Available: https://cmte.ieee.org/futuredirections/2022/11/01/sdv-software-defined-vehicles/

[3] J. Scheibmeir, S. Sicular, A. Batchu, M. Fang, V. Baker, and F. O'Connor, "Magic quadrant for cloud ai developer services," *Gartner*, 2023. [Online]. Available: https://pages.awscloud.com/Gartner-Magic-Quadrant-for-Cloud-AI-Developer-Services.html?trk=d59e704f-4f30-4d43-8902-eb63c3692af4&sc_channel=el

[4] M. KARLSSON and L. SCHÖNBECK, "Department of technology management and economics," *CHALMERS UNIVERSITY OF TECHNOLOGY*, p. 11, 2018. [Online]. Available: https://odr.chalmers.se/server/api/core/bitstreams/077c3440-c033-418e-92ed-eda5dd638c5f/content

[5] S. project and M. Spencer, "Architecture," 2023. [Online]. Available: https://architecture.docs.soafee.io/en/latest/contents/architecture.html

[6] B. QNX, "What is a software-defined vehicle?" *Software-Defined Vehicles*, 2024. [Online]. Available: https://blackberry.qnx.com/en/ultimate-guides/software-defined-vehicle

[7] S. Reply, "Who we are," 2024. [Online]. Available: https://www.reply.com/storm-reply/en/

[8] AWS, "Aws global infrastructure," *About-aws*, 2024. [Online]. Available: https://aws.amazon.com/about-aws/global-infrastructure/

[9] I. Society, "Functional safety," *ISO 26262-1:2018 Road vehicles*, no. 2, 2018. [Online]. Available: https://www.iso.org/obp/ui/en/#iso:std:68383:en

[10] C. D. D. O. E. N. Fong and P. E. Black, "Impact of code complexity on software analysis," *NIST IR*, vol. 8165, no. upd1, pp. 1–12, 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8165.pdf

[11] D. Slama, A. Nonnenmacher, and T. Irawan, "The software-defined vehicle," *A Digital-First Approach to Creating Next-Generation Experiences*, pp. 1–6, 2023. [Online]. Available: https://www.bosch-mobility.com/media/global/mobility-topics/mobility-topics/software-defined-vehicle/

[12] A. Nonnenmacher and L. Product, "What is a software-defined vehicle in your opinion?" 2024. [Online]. Available: https://www.bosch-mobility.com/en/mobility-topics/software-defined-vehicle/?gad_source=1

[13] R. Group, "What is software defined vehicle?" 2024. [Online]. Available: https://www.renaultgroup.com/en/news-on-air/news/

all-about-software-defined-vehicle/
[14] Arm, "Do you have the right tools?" 2024. [Online]. Available: https://www.arm.com/developer-hub/embedded-systems/automotive-tools
[15] A. K. Srivastava, K. CS, D. Lilaramani, R. R, and K. Sree, "An open-source swupdate and hawkbit framework for ota updates of risc-v based resource constrained devices," *2nd International Conference on Communication, Computing and Industry 4.0*, p. 1, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9689433
[16] M. Helmy and M. Mahmoud, "Enhanced multi-level secure over-the-air update system using adaptive autosar," *International Conference on Computer and Applications*, p. 1, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10401797
[17] Autosar, "Vision," 2024. [Online]. Available: https://www.autosar.org/about
[18] A. Banks, E. Briggs, K. Borgendale, and R. Gupta, "Mqtt version 5.0," *OASIS Standard*, pp. 10 – 13, 2020. [Online]. Available: https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.pdf
[19] AWS, "What are mqtt components?" 2024. [Online]. Available: https://aws.amazon.com/it/what-is/mqtt/
[20] B. J. R. G and R. P, "Iot based system to predict the defects of tires in heavy vehicle," *International Conference on Sustainable Communication Networks and Application (ICSCNA)*, p. 1, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10370342
[21] K. T. Selvi, N. Praveena, K. Pratheksha, S. Ragunanthan, and R. Thamilselvan, "Air pressure system failure prediction and classification in scania trucks using machine learning," *Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, p. 1, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9742716
[22] L. H. M. da Ros Gomes and S. Goscik, "Building an automotive embedded linux image for edge and cloud using arm-based graviton instances, yocto project, and soafee," 2022. [Online]. Available: https://aws.amazon.com/blogs/industries/
[23] S. project, "Achieving software-defined vehicles," 2023. [Online]. Available: https://www.soafee.io/
[24] AWS, "Amazon web services," 2024. [Online]. Available: https://www.aboutamazon.eu/what-we-do/amazon-web-services
[25] ——, "Cloud computing with aws," 2024. [Online]. Available: https://aws.amazon.com/what-is-aws/
[26] ——, "About aws," 2024. [Online]. Available: https://docs.aws.amazon.com/whitepapers/latest/gxp-systems-on-aws/about-aws.html
[27] ——, "What is cloud computing?" 2024. [Online]. Available: https://aws.amazon.com/what-is-cloud-computing/
[28] ——, "Aws cloud security," 2024. [Online]. Available: https://docs.aws.amazon.com/whitepapers/latest/gxp-systems-on-aws/aws-cloud-security.html
[29] ——, "Aws cloud security," 2024. [Online]. Available: https://aws.amazon.com/security/
[30] ——, "Gxp," 2024. [Online]. Available: https://docs.aws.amazon.com/whitepapers/latest/gxp-systems-on-aws/aws-certifications-and-attestations.

html

[31] ——, "Aws certifications and attestations," 2024. [Online]. Available: https://aws.amazon.com/compliance/gxp-part-11-annex-11/?nc1=h_ls