UNECE R155/R156 Compliance through a Novel Cybersecurity Lifecycle Approach

Executive Summary

The advent of Software-Defined Vehicles (SDVs) has revolutionized the automotive industry by triggering a transition from traditional hardware-centric architectures to software-centric systems. SDVs leverage advanced software and connectivity to enable over-the-air (OTA) updates, remote diagnostics, and new feature deployments, unlocking unprecedented flexibility and innovation. However, this increased reliance on software and connectivity also introduces new security challenges that must be addressed in compliance with emerging cybersecurity regulations and standards.

These regulations and standards mandate that manufacturers implement robust cybersecurity measures, including risk assessment processes, secure software development practices, and incident response plans throughout the vehicle's lifecycle.

Remote teleoperation driving, where vehicles can be controlled remotely by human operators, is a prime example of the capabilities enabled by SDVs. This use case is expected to evolve rapidly over the next 3-4 years, enabling advanced scenarios such as remote delivery services, autonomous valet parking, and remote assistance for self-driving vehicles in challenging situations. However, this evolution also introduces additional complexities in terms of secure communication, access control, and threat detection, necessitating robust security measures to safeguard the system against potential cyberattacks and unauthorized access.

This whitepaper is the first of several updates expected from project **SecureTCU**, a UK South Korea collaborative research and development project (CR&D), funded by UK's Innovate UK and South Korea's KIAT. The project is developing a next-generation TCU with an integrated Intrusion Detection System (IDS) and aims to enhance the security posture of SDVs. This product addresses a critical need in the automotive industry, as manufacturers strive to meet stringent cybersecurity requirements while unlocking the full potential of connected and automated driving systems.

Further, the Secure Telematics Control Unit will offer insights into the development challenges of a next-generation Telematics Control Unit (TCU) with an integrated Intrusion Detection System (IDS) for detecting threats in a

remote teleoperation driving use case. The development of the SecureTCU follows a comprehensive Systems, Safety and Cybersecurity engineering process using an Integrated safety and security application, CRISKLE™, which evaluates safety hazards that could arise as a result of a security threats on asset/s in the teleoperated driving scenario. Additionally, this whitepaper introduces an industry first concept of integrated safety and security analysis and examines the interactions between safety and security, providing recommendations for addressing potential risks.

Table of Contents

1 Introduction

Software-Defined Vehicles (SDVs) represent the next generation of automotive technology, where the vehicle's functionality is primarily controlled and managed through software rather than traditional hardware-centric architectures. SDVs are designed to be highly connected, enabling features such as Over-the-Air (OTA) software updates, remote diagnostics, and advanced telematics services.

The shift towards SDVs is driven by the need for increased flexibility, scalability, and the ability to continuously enhance and customize vehicle features throughout the product lifecycle. However, this increased connectivity and reliance on software also introduces new cybersecurity risks that must be addressed.

1. Connected and OTA-enabled: SDVs are designed to be wirelessly connected to enable features like Over-the-Air (OTA) software updates, remote diagnostics, and telematics services. This connectivity opens potential attack vectors for cyber threats if not properly secured.
2. Increased Attack Surface: With more software components and interconnected systems, SDVs have a larger attack surface compared to traditional vehicles, making them more vulnerable to cyber threats if proper security measures are not implemented.
3. Safety and Operational Risks: Cyber-attacks on SDVs can potentially compromise vehicle safety systems, leading to operational disruptions, safety hazards, or even physical harm to occupants and bystanders.
4. Data Privacy Concerns: SDVs collect and transmit vast amounts of data, including potentially sensitive information about vehicle operations, location, and user behaviour. Inadequate cybersecurity measures can lead to data breaches and privacy violations.
5. Regulatory Compliance: Emerging regulations and standards, such as UN R155 and ISO/SAE 21434, mandate robust cybersecurity measures for connected and automated vehicles, including SDVs.
6. Brand Reputation and Trust: Successful cyber-attacks on SDVs can severely damage the reputation and consumer trust of automotive brands, leading to significant financial and legal consequences.

The automotive industry recognizes the urgent need for comprehensive cybersecurity solutions to protect SDVs from emerging cyber threats. This demand created an opportunity for project partners with specialized expertise in engineering, deep tech technology, cybersecurity, test, and validation to develop and innovate on *Secure Telematics Control Unit* or **SecureTCU**.

As SDVs continue to evolve, with features like remote teleoperation becoming more prevalent, the cybersecurity challenges will become even more complex. Proactive measures, such as implementing robust intrusion detection and prevention systems, secure communication protocols, and adhering to industry best practices, are crucial to ensuring the safe and secure operation of these highly connected and software-defined vehicles.

2 Introduction to Project Partners

Project consortium comprise expertise to deliver the **SecureTCU**, by leveraging a range of diverse and extensive automotive development skills. Integrating *Beam Connectivity's* TCU with *Autocrypt's* IDS security software, assessed by *Secure Element's* Integrated Product Security Lifecycle Platform CRISKLE™ for performing safety, security risk analysis, vulnerability management and validated at *KATECH's* test facilities. This project demonstrates collaboration of four partners who are on the mission to deliver a next generation **SecureTCU** developed to handle requirements for a remote Teleoperations Application with a technology readiness level (TRL) 7.

2.1 Secure Elements

Secure Elements is an automotive cybersecurity software company dedicated to ensuring the security of modern-day mobility systems. The company specialises in building cybersecurity tooling solutions for safety and cybersecurity engineering risk assessments, vulnerability management and vehicle cybersecurity monitoring using security operations centre (SOC), ensuring that automotive products are built secure by design, meeting ISO/SAE 21434 and UNECE R155 requirements.

Our product/s include CRISKLE™, offered as a software as a service (SaaS) application, which is the Integrated Safety and Security Platform and CRISKLE™ MSOC , a mobility security operations centre. This project will extensively use CRISKLE™ for safety and security risk assessments, management of vulnerabilities while following the full secure software development lifecycle. CRISKLE™ MSOC will be used towards the later part of the project to view security threats and alerts originating from the on-board intrusion detection system (IDS) on the TCU.

2.2 Beam Connectivity

Beam Connectivity are pioneers in better connected vehicles. Our ambition is to build best-in-class connected vehicle systems by supporting our customers to focus on the value of their connected vehicle data while us taking care of the underlying connection.

Our core offering is Connected Vehicle as a Service (CvaaS), a high performance and versatile platform with all the components required to stand-up a connected vehicle system. CVaaS includes our own design of high-performance Telematics Control Unit, cloud platform for storing and managing vehicle data, web portal for visualising connected vehicle data, mobile application which can be easily customised to our customers branding and feature requirements and management of the mobile cellular network. CVaaS Supports all connected vehicle use cases including telemetry, OTA software updates, remote control. Beam have already developed a TCU and deployed these to vehicles from Honda, WAE Technologies and Aidea scooters.

2.3 Autocrypt Co Ltd

AUTOCRYPT is an automotive cybersecurity and mobility solutions provider, dedicated to software-defined, connected, and autonomous mobility. AUTOCRYPT is committed to ensuring that connected and software-defined vehicles experience can be trusted by drivers and passengers on and off the road, keeping everyone involved safe from harm.

AUTOCRYPT secures the rapidly evolving architecture of software-defined vehicles and smart mobility, using custom solutions built for ISO/SAE 21434 and UN R155/156. Backed by decades of industry experience, our solutions can be customized and adapted to any vehicular and infrastructure environment.

AUTOCRYPT's In-Vehicle System Security solution provides complete protection for the embedded systems of a vehicle through a three-step process from 1) TARA, 2) Security Testing, and 3) Mitigation and Monitoring. AutoCrypt® IDS monitors communications within the vehicle, responding to any abnormal or malicious activities using its proprietary Security Sensor.

2.4 KATECH (Korea Automotive Technology Institute)

KATECH, the Korea Automotive Technology Institute, is the leading automotive test facility in South Korea for wireless connectivity and cyber security. KATECH's team at Future Connected Mobility Centre has an international reputation, state-of-the-art test chambers, simulators, and equipment for vehicle testing. They have close relationships with Hyundai, Korean OEMs and major OEMs selling vehicles into Korea including GM and Renault.

3 Software Defined Vehicle (SDV) Cybersecurity and Remote Teleoperations

3.1 Barriers to SDV Cybersecurity

While the benefits of Software-Defined Vehicles (SDVs) are significant, ensuring their cybersecurity poses several challenges. Barriers to key to adoption include complexity of SDV architectures as shown in Figure 1, with numerous (zonal consolidation) interconnected systems, components and software. This increases the attack surface and makes it challenging to implement end-to-end security measures.

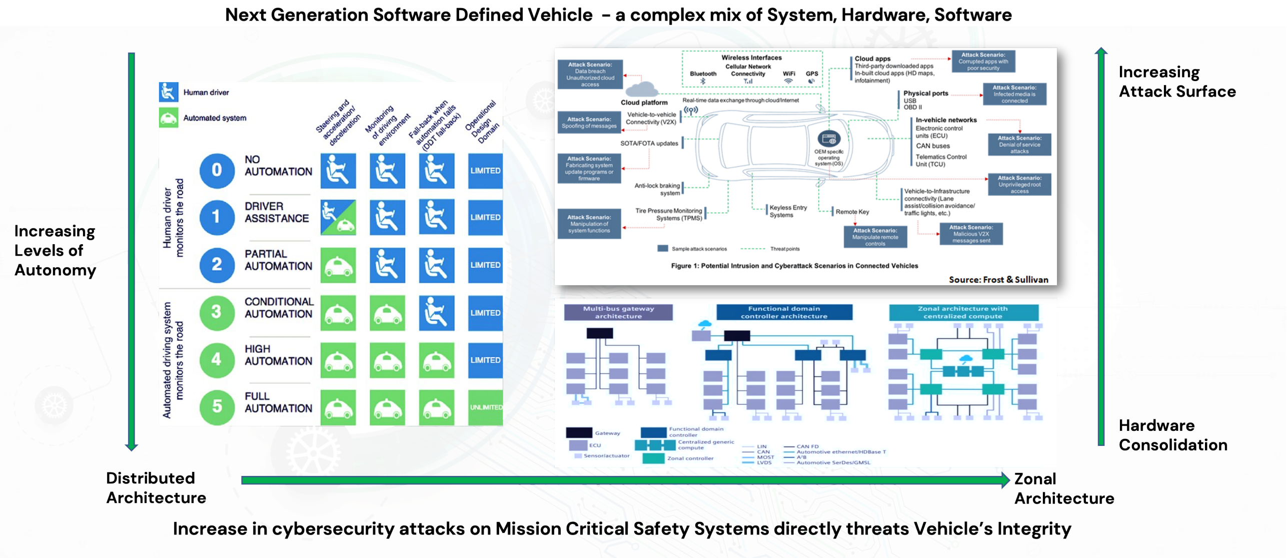
Next Generation Software Defined Vehicle – a complex mix of System, Hardware, Software
Increasing Levels of Autonomy
Human driver
Automated system
Steering and acceleration/ deceleration
Monitoring of driving environment
Fall-back when automation fails (DDT fall-back)
Operational Design Domain
Human driver monitors the road
Automated driving system monitors the road
0 NO AUTOMATION
1 DRIVER ASSISTANCE
2 PARTIAL AUTOMATION
3 CONDITIONAL AUTOMATION
4 HIGH AUTOMATION
5 FULL AUTOMATION
LIMITED
UNLIMITED
Wireless Interfaces
Bluetooth
Cellular Network Connectivity
WiFi
GPS
Cloud platform
Real-time data exchange through cloud/Internet
Attack Scenario: Data breach Unauthorized cloud access
Vehicle-to-vehicle Connectivity (V2X)
Attack Scenario: Spoofing of messages
SOTA/FOTA updates
Attack Scenario: Fabricating system update programs or firmware
Anti-lock braking system
Tire Pressure Monitoring Systems (TPMS)
Attack Scenario: Manipulation of system functions
Keyless Entry Systems
Remote Key
Attack Scenario: Manipulate remote controls
OEM specific operating system (OS)
Cloud apps
Third-party downloaded apps
In-built cloud apps (HD maps, infotainment)
Attack Scenario: Corrupted apps with poor security
Physical ports
USB
OBD II
Attack Scenario: Infected media is connected
In-vehicle networks
Electronic control units (ECU)
CAN buses
Telematics Control Unit (TCU)
Attack Scenario: Denial of service attacks
Attack Scenario: Unprivileged root access
Vehicle-to-Infrastructure connectivity (Lane assist/collision avoidance/ traffic lights, etc.)
Attack Scenario: Malicious V2X messages sent
Sample attack scenarios
Threat points
Figure 1: Potential Intrusion and Cyberattack Scenarios in Connected Vehicles
Source: Frost & Sullivan
Multi-bus gateway architecture
Functional domain controller architecture
Zonal architecture with centralized compute
Gateway
ECU
Sensor/actuator
Functional domain controller
Centralized generic compute
Zonal controller
LIN
CAN
MOST
LVDS
CAN FD
Automotive ethernet/HDBase T
A²B
Automotive SerDes/GMSL
Increasing Attack Surface
Hardware Consolidation
Distributed Architecture
Zonal Architecture
Increase in cybersecurity attacks on Mission Critical Safety Systems directly threats Vehicle's Integrity

Figure 1: Next Generation Architecture

Additionally, the adoption rate of standardized cybersecurity practices and guidelines across the automotive supply chain can lead to inconsistencies and introduction of severe weaknesses in the SDV architecture. Limited cybersecurity expertise within the automotive industry, coupled with the rapid pace of technological advancements, can result in skill gaps and difficulties in keeping up with emerging threats.

Furthermore, the need for highly automated driving (HAD) features, remote teleoperations, continuous software over-the-air (SOTA) updates, introduces a wide array of attack surfaces that can be exploited. It is imperative on mobility providers to ensure continual cybersecurity risk assessment, management, and manage vulnerabilities, increase overall quality and enhancing customer experience. Overcoming these barriers requires industry-wide collaboration, adoption of secure development lifecycles, and investment in cybersecurity talent and training.

The **SecureTCU** project evaluates systemic monitoring, detection, and analysis of threats on a Remote Teleoperation Driving system which is highly dependent on the vehicle's TCU connectivity with the internet / offboard server. Designing a system to meet unpredictable network latency is a challenging task, which is compounded by need to have a secure connection. In Remote Teleoperation Driving System, it is quite possible that incoming packets might have to be rejected/dropped due to perceived security threat, for example an attacker could launch an attack and disrupt the communication or an attacker performing a man-in-the-middle attack (MiTM). To counter this threat, the on-board system shall always be ready to repel such attacks by detecting intrusions at the point of entry, allowing it to filter critical data packets and ensure entry of only legitimate packets in the system.

Further, the on-board IDS rule-sets and the off-board IDS policy manager of the Intrusion Detection System must always be in sync to be able to detect, respond, recover, identify and protect against anomalies. The IDS rule-sets themselves are subject to cyber-attacks, which necessitates the requirement for secure storage on the TCU, to protect the integrity and freshness of the rule-sets in the TCU. There exists an opportunity for an attacker to exploit poor connectivity as a means to introduce such delays in updating the rule-set, allowing modification with an extended window of opportunity for the attacker.

Teleoperated vehicles will therefore need a secure on-board and off-board infrastructure with a quick turnaround time to fix the vulnerabilities detected while the system is live and a mechanism to distribute the patch to all such affected system. Such a system does not exist in the automotive market today.

4 Remote Teleoperations System Analysis

While Remote Teleoperated Driving Scenario as an end to end capability may have several cybersecurity relevant use-cases, it also enables advanced use cases such as remote delivery services, autonomous valet parking, and remote assistance for self-driving vehicles in challenging situations. While offering significant convenience and efficiency benefits, remote teleoperation introduces unique safety and security challenges.

One such application area under investigation in the **SecureTCU** project is the monitoring, detection and reporting of on-board intrusions/anomalies using an IDS on the TCU. All this, in a remote teleoperated driving involving a human operator remotely controlling a vehicle's steering, acceleration, and braking systems over a wireless network.

4.1 Proposed System Architecture

The proposed system architecture as shown in Figure 2, shows the end to end deployment of the remote teleoperation application. The architecture was developed using MBSE modelling tools after taking into consideration stakeholder requirements. Further, the system elements are processed for safety and security risk analysis in CRISKLE™.

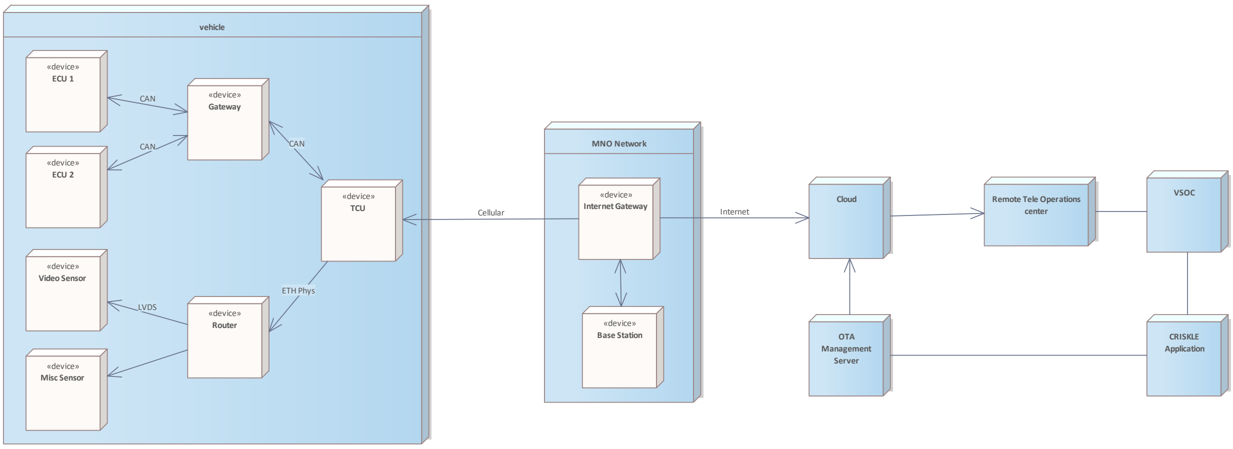

Figure 2: System Architecture

4.2 Safety Situation Analysis

Ensuring the safety of vehicles in a remote teleoperation systems is paramount, as any safety failures could potentially lead to catastrophic consequences. The ISO 26262 – Road Vehicles - Functional Safety standard provides a comprehensive framework for addressing functional safety in the automotive industry, including guidelines and requirements for risk assessment, system design, and validation processes.

When conducting a safety analysis for remote teleoperation systems using the ISO 26262 standard, several key areas and situations need to be thoroughly examined. One critical aspect is the communication link between the remote operator and the vehicle. Potential hazards could arise from communication disruptions, latency issues, or interference, which could result in delayed or corrupted control commands. The safety analysis should assess the risk levels associated with various communication failure modes and define appropriate mitigation strategies, such as failsafe mechanisms or redundant communication channels.

Another area of focus is the human-machine interface (HMI) and the potential for operator errors. The safety analysis should consider scenarios where the remote operator may misinterpret sensor data, make incorrect control inputs, or experience cognitive overload due to information overload or distractions. Factors such as ergonomics, user interface design, and operator training should be evaluated to minimize the risk of operator-induced hazards.

The integration of multiple systems and components from various suppliers is another critical aspect to analyse. Potential safety issues could arise from incompatibilities, software bugs, or hardware failures in any of the interconnected systems, such as sensors, actuators, or control modules. The safety analysis should identify potential failure modes, evaluate their impact, and define appropriate diagnostic and redundancy measures to ensure system robustness.

Environmental factors and external influences should also be considered in the safety analysis. For instance, situations where the remote operator has limited visibility or situational awareness due to adverse weather conditions, obstructions, or sensor degradation could pose significant risks. The analysis should examine the potential impact of these scenarios and define appropriate mitigation strategies, such as transferring control to an on-board system or implementing enhanced sensor fusion techniques.

Furthermore, the safety analysis should address key cybersecurity risks, as any security breaches or unauthorized access to the remote teleoperation system could potentially compromise safety. Vulnerabilities in communication channels, software components, or system interfaces should be identified, and appropriate security measures should be integrated into the overall safety concept.

By thoroughly analysing these situations and applying the principles and processes outlined in the ISO 26262 standard, this project will be analysing safety measures for remote teleoperation systems. This includes conducting hazard analysis and risk assessment (HARA) using CRISKLE™ for deriving safety goals and requirements, implementing hardware and software safeguards where required and conducting rigorous testing and validation.

4.3 Security Situation Analysis

Ensuring the cybersecurity of remote teleoperation systems is critical to mitigating safety risks and maintaining consumer trust. The automotive industry has developed several standards and regulations to address this challenge, including the ISO/SAE 21434 standard for automotive cybersecurity engineering and the UNECE Regulation No. 155 (R155) on cybersecurity and cyber security management systems.

A key aspect of these standards is the requirement to conduct a comprehensive Threat Analysis and Risk Assessment (TARA) throughout the vehicle's lifecycle. The TARA process involves identifying potential cybersecurity threats, vulnerabilities, and attack vectors specific to the remote teleoperation use case. The TARA analysis will be conducted in CRISKLE™ which will include systemic evaluation of risks associated with communication channels, system interfaces, software components, and potential for unauthorized access or manipulation of control commands.

Common vulnerabilities that must be addressed include weak authentication mechanisms, insecure communication protocols, software vulnerabilities (e.g., buffer overflows, code injection), and supply chain risks introduced by third-party components or software dependencies. The TARA should also consider the impact of successful attacks, such as safety hazards resulting from compromised vehicle control systems or data breaches involving sensitive user information.

Based on the TARA findings, ISO/SAE 21434 and R155 mandate the implementation of robust cybersecurity requirements and controls. These include secure communication protocols with end-to-end encryption and message authentication, secure software development practices (e.g., code reviews, penetration testing), secure over-the-air (OTA) update mechanisms, and comprehensive access control and identity management systems.

To detect and respond to potential cybersecurity threats in real-time, integrating an Intrusion Detection System (IDS) into the Telematics Control Unit (TCU) is a crucial component. The TCU acts as the central communication gateway in connected vehicles, making it an ideal location for an IDS to monitor network traffic, system logs, and other data sources for suspicious activities or anomalies.

The IDS can leverage various techniques, such as signature-based detection (matching known attack patterns), anomaly-based detection (identifying deviations from normal behaviour), and machine learning models to identify potential threats. Upon detecting a potential intrusion, the IDS can generate alerts, initiate incident response processes, and potentially trigger failsafe measures to mitigate the impact of the attack.

Some of the threats under consideration in this project and those that can arise in situations involving remote teleoperations are

- Unauthorized access to the remote-control interface
- Man-in-the-middle attacks intercepting and manipulating control commands

- Distributed Denial of Service (DDoS) attacks disrupting communication links
- Injection of malicious code or firmware into vehicle systems
- Replay attack to deceive the recipient into believing that the replayed data is genuine
- Brute force attack based on the principle of trial and error (does not rely on any specific vulnerabilities in the target system).

Adhering to ISO/SAE 21434, R155, and implementing defence-in-depth security measures, including an IDS on the TCU, is essential for ensuring the cybersecurity and safety of remote teleoperation systems. Continuous monitoring, threat intelligence updates will be performed in CRISKLE™, to stay ahead of evolving cyber threats in this rapidly advancing domain.

4.4 The importance of Integrated Safety and Security Analysis

The integration of safety and security analysis is crucial for developing robust and resilient systems. These two aspects are intrinsically linked, and a siloed approach to their evaluation can lead to gaps and oversights that may have severe consequences.

So, why is an integrated evaluation needed?

1. Safety and security risks are interconnected: Security breaches can directly impact safety, and safety hazards can potentially create security vulnerabilities. For example, if an attacker gains unauthorized access to the vehicle control systems, they could send malicious commands that cause unintended acceleration, hard braking, or steering inputs, resulting in collisions, injuries, or loss of life. Conversely, a safety-critical system failure could potentially expose vulnerabilities that an attacker could exploit.
2. Conflicting requirements: In some cases, safety and security requirements may seem to conflict with one another. For instance, a safety requirement might mandate redundant systems for fault tolerance, while a security requirement may discourage redundancy to minimize the attack surface. An integrated analysis can help identify and resolve such conflicts early on, ensuring that both safety and security objectives are met without compromising either aspect.
3. Holistic risk assessment: By considering safety and security together, a more comprehensive risk assessment can be conducted, taking into account the interdependencies and cascading effects of potential threats and hazards. This holistic approach enables the identification of risks that might be overlooked in siloed analyses, leading to more effective mitigation strategies.

So, how is an integrated analysis different from siloed safety and security analyses?

Traditional siloed analyses often treat safety and security as separate domains, with different teams working in isolation. This approach can lead to inconsistencies, redundancies, and gaps in the overall system design and risk management processes. An integrated analysis, on the other hand, promotes collaboration between safety and security experts, fostering a shared understanding of the system's vulnerabilities and hazards as shown in Figure 3.

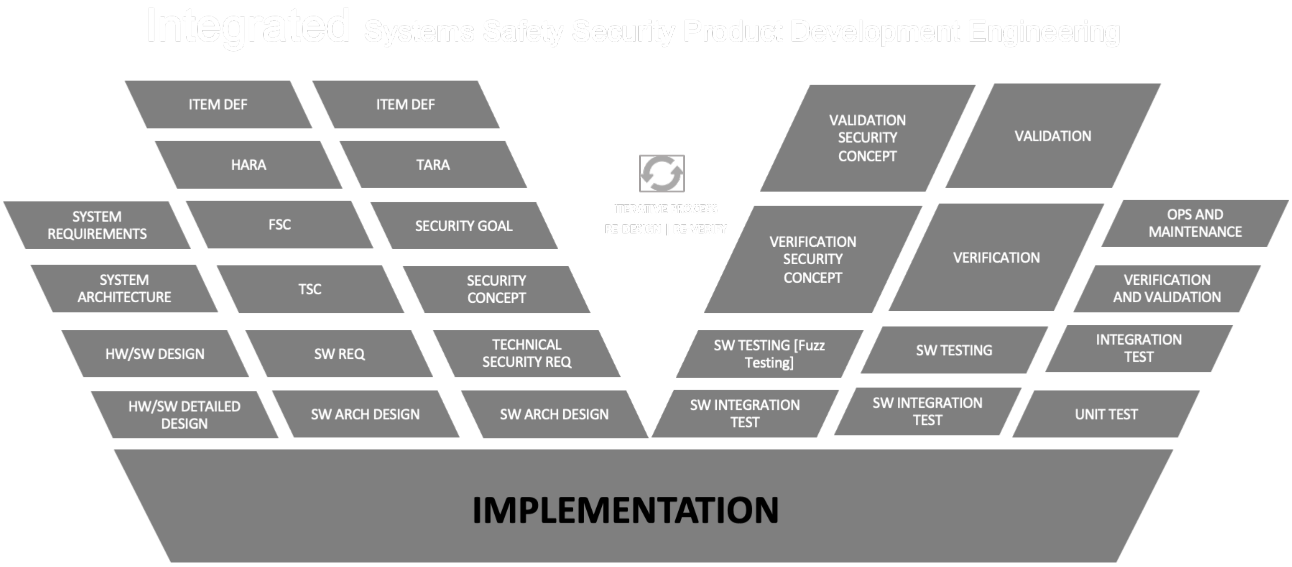

Figure 3: Integrated development model

By combining safety and security analyses, potential conflicts or synergies between requirements can be identified and addressed early in the development lifecycle. For example, a security requirement for secure communication protocols might conflict with a safety requirement for low-latency data transmission. An integrated analysis would facilitate the identification of such conflicts and enable the development of optimized solutions that address both safety and security needs.

Ok, so why is continual analysis of cybersecurity vulnerabilities important and how is this connected to risk assessment?

Continual analysis of cybersecurity vulnerabilities is imperative in the realm of remote teleoperation systems due to the ever-evolving nature of cyber threats and the potential severe consequences of a successful attack. This ongoing vulnerability assessment is intrinsically connected to risk assessment, as it provides crucial insights into the emerging attack vectors and their potential impact, enabling proactive risk mitigation strategies.

Vulnerability management in automotive systems is a multifaceted challenge, as these systems are complex, with components sourced from numerous suppliers and integrating various hardware and software elements. Collaboration among automotive suppliers and original equipment manufacturers (OEMs) is essential to address the evolving cybersecurity challenges in the automotive sector, as vulnerabilities can exist in any part of the supply chain or system architecture.

In recent years, attacks on automotive systems have increased, driven by the proliferation of connected vehicles and the availability of sophisticated hacking tools that make exploitation seemingly easier for malicious actors. This trend underscores the importance of incorporating such emerging threats into the threat analysis process for remote teleoperation systems, ensuring that the system's defences are proactively fortified against the latest attack techniques.

Even after taking care of all aspects of security during the design phase, the risks associated with threat vectors cannot be eliminated completely over the lifetime of a Telematics Control Unit (TCU) or other automotive electronic control units (ECUs). New vulnerabilities could be discovered in the ECU hardware or software components, increasing the risk factor after the product has entered the production phase. These vulnerabilities may arise from newly discovered software bugs, hardware flaws, or evolving attack methodologies that exploit previously unknown weaknesses.

Detecting these vulnerabilities and keeping an up-to-date risk register is crucial for ECU manufacturers to maintain the security posture of their products. This requires a sophisticated tool or platform that can assist cybersecurity analysts in quickly identifying components or subsystems with elevated risk scores based on the discovered vulnerabilities.

So, how is this project analysing cybersecurity vulnerabilities and risk management ?

The tooling landscape for safety and security analysis in the automotive industry presents significant challenges, particularly in the context of complex systems like remote teleoperation. The prevalent use of disconnected tool chains and siloed analysis processes by OEMs and suppliers can lead to incomplete assessments, missed dependencies, and ineffective risk mitigation strategies.

One of the major challenges is the disconnect between the tools and systems used for safety and security analysis. Traditionally, these analyses have been conducted separately, often by different teams using different methodologies and tools. This siloed approach can result in missed opportunities for identifying potential conflicts or synergies between safety and security requirements, leading to incomplete or ineffective risk assessments.

Moreover, the disconnected nature of these tools and analysis processes hinders the ability to seamlessly share and integrate findings across domains.

For example, the outcome of a security analysis, which may uncover potential vulnerabilities, cannot be easily fed into the safety analysis process to evaluate the potential impact on safety-critical systems. This lack of integration can lead to gaps in the overall risk assessment and mitigation strategies.

Another critical challenge is the limited support for continuous monitoring of threats and vulnerabilities throughout the product lifecycle. As new vulnerabilities and attack vectors emerge, it becomes crucial to re-evaluate the risk posture of the system and adapt security measures accordingly. However, many existing tools and processes are static, lacking the capability to dynamically incorporate evolving threat intelligence and vulnerability data.

To address these challenges, the automotive industry is recognizing the need for integrated tooling platforms that can bridge the gap between safety and security analyses. One such platform is CRISKLE™, which provides a comprehensive framework for conducting integrated safety and security risk assessments throughout the product lifecycle.

CRISKLE™ enables the consolidation of safety and security analyses within a unified platform, facilitating collaboration between safety and security experts. By combining threat modelling, vulnerability assessments, and safety hazard analysis, CRISKLE™ supports the identification of potential conflicts or synergies between safety and security requirements, enabling the development of optimized solutions that address both domains.

Furthermore, CRISKLE™'s lifecycle integration approach allows for continuous monitoring and updating of threat intelligence, vulnerability data, and risk assessments. This ensures that the system's risk posture is accurately evaluated and updated as new threats or vulnerabilities emerge, enabling proactive risk mitigation strategies.

By adopting integrated tooling platforms like CRISKLE™, as shown in Figure 4, automotive manufacturers and suppliers can overcome the challenges posed by disconnected tool chains and siloed analyses.

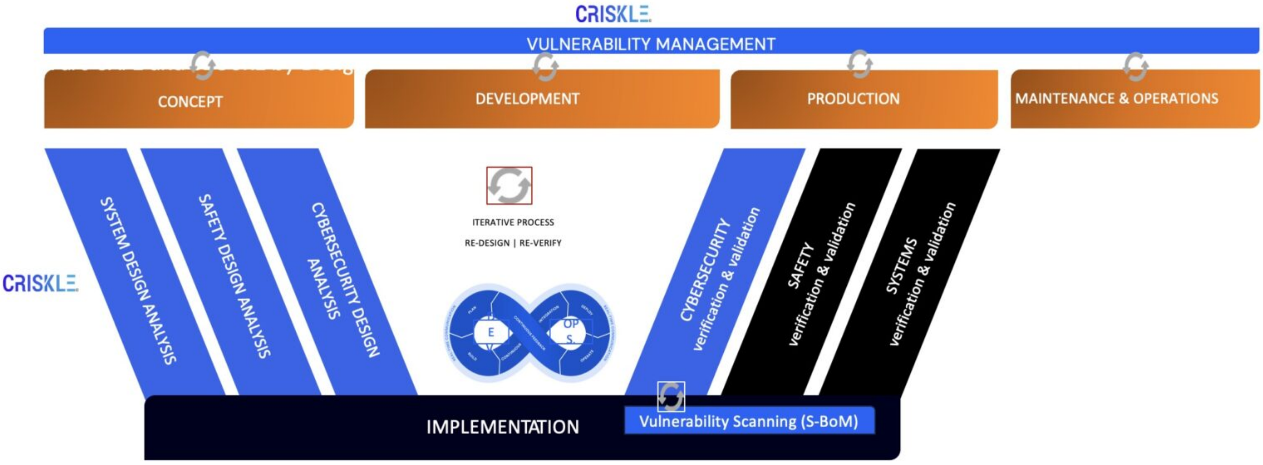

Figure 4: Integrated Development lifecycle

This approach fosters collaboration, enables comprehensive risk assessments, and supports continuous monitoring and adaptation to evolving threats, ultimately enhancing the safety and security of complex systems like remote teleoperation.

4.5 Telematics Control Unit (TCU) with Intrusion Detection System (IDS)

Ensuring the cybersecurity of remote teleoperation systems is a continuous endeavour that requires vigilant monitoring, vulnerability analysis, and proactive risk mitigation. At the heart of this effort lies the integration of an Intrusion Detection System (IDS) within the Telematics Control Unit (TCU), a critical component that acts as the communication gateway for connected vehicles. However, the effectiveness of the IDS itself must be safeguarded against potential cyber threats, as a compromised IDS could render the entire security architecture vulnerable.

The integration of an IDS within the TCU offers numerous benefits for enhancing the cybersecurity posture of remote teleoperation systems. By continuously monitoring network traffic, system logs, and other relevant data sources, the IDS can detect potential threats, anomalies, and indicators of compromise in real-time. This proactive threat detection capability is crucial for mitigating risks associated with unauthorized access attempts, man-in-the-middle attacks, distributed denial-of-service (DDoS) attacks, or the injection of malicious code into vehicle systems.

The IDS can leverage various techniques, such as signature-based detection (matching known attack patterns), anomaly-based detection (identifying deviations from normal behaviour), and machine learning models to identify potential threats. Upon detecting a potential intrusion, the IDS can generate alerts, initiate incident response processes, and potentially trigger failsafe measures to mitigate the impact of the attack.

However, the protection of the IDS itself from cyber threats is of paramount importance. A compromised IDS could allow attackers to bypass security controls, modify detection rules, or suppress alerts, effectively rendering the system blind to ongoing threats. Ensuring the integrity and resilience of the IDS is crucial to maintain its effectiveness and prevent it from becoming a vulnerability itself.

One approach to protecting the IDS is through the implementation of secure software development practices, including code reviews, penetration testing, and secure coding techniques. Additionally, the IDS software should be regularly updated with the latest threat intelligence and detection signatures to stay ahead of emerging attack vectors.

Another critical aspect is the secure deployment and management of the IDS within the TCU. This may involve measures such as secure boot processes, code signing, and encrypted communications between the

IDS and other components within the TCU or remote security operations centres. Strict access controls and privilege management should also be implemented to prevent unauthorized modifications or tampering with the IDS configuration or rules.

Furthermore, the TCU itself should be hardened against potential cyber threats, leveraging secure communication protocols, encryption, and authentication mechanisms to protect the integrity of data transmitted to and from the IDS. This defense-in-depth approach ensures that even if one layer of security is compromised, additional layers of protection can mitigate the risk and prevent further exploitation.

While the IDS plays a crucial role in monitoring and detecting threats from the outside world, it is equally important to protect the integrity of the IDS itself from internal threats or supply chain risks. This may involve implementing secure software update mechanisms, conducting regular vulnerability assessments, and establishing robust security practices throughout the supply chain and development lifecycle.

Collaboration among automotive manufacturers, suppliers, and cybersecurity experts is essential to stay ahead of evolving cyber threats and share best practices for securing critical components like the IDS and TCU. Industry-wide initiatives, such as vulnerability disclosure programs and threat intelligence sharing platforms, can help identify and address potential vulnerabilities proactively, further enhancing the overall security posture of remote teleoperation systems.

By integrating a robust IDS within the TCU and implementing multi-layered security measures to protect its integrity, automotive manufacturers can establish a comprehensive cybersecurity architecture for remote teleoperation systems. This holistic approach, combined with continuous vulnerability monitoring, risk assessment, and collaboration within the industry, is crucial for ensuring the safe and secure operation of these cutting-edge technologies.

5 Impacts of Regulations and Standards

5.1 Market Situation and Regulations

United Kingdom (UK)

The United Kingdom has taken a proactive stance in supporting the safe and rapid deployment of connected and automated driving technologies, recognizing the potential benefits these innovations offer to society. The UK government has been at the forefront of developing a regulatory framework that balances innovation with safety considerations.

One of the key legislative efforts in this domain is the Automated and Electric Vehicles Act 2018 (EV Act). This act paved the way for the legal framework surrounding the use of autonomous vehicles on UK roads. It addressed issues such as insurance liability, cyber security, and software updates, laying the groundwork for the eventual deployment of self-driving cars.

Building upon the EV Act, the UK government is expected to introduce an Automated Vehicles (AV) Bill in 2024. This upcoming legislation aims to further refine the regulatory landscape, addressing the unique challenges posed by autonomous driving technologies. The AV Bill is anticipated to provide a comprehensive set of regulations governing the testing, deployment, and operation of self-driving vehicles, ensuring that safety remains the top priority as these technologies become more widespread.

The UK's approach to regulating connected and automated driving technologies is closely aligned with international standards and best practices. In particular, the country follows the United Nations Economic Commission for Europe (UNECE) Regulation No. 155 (R155), which outlines specific cybersecurity requirements for vehicles. R155 mandates that manufacturers implement robust cybersecurity management systems and risk assessment processes throughout the vehicle's lifecycle, ensuring that these critical systems are designed, developed, and maintained with security as a fundamental consideration.

The UK's efforts in this domain extend beyond legislation, with significant contributions to the development of industry standards. The British Standards Institution (BSI) has been actively involved in the formulation of international standards related to connected and automated driving technologies. BSI representatives serve on various technical committees within the International Organization for Standardization (ISO), contributing their expertise and insights to shape global standards that promote safety, security, and interoperability.

Furthermore, the Centre for Connected and Autonomous Vehicles (CCAV), a joint policy unit between the Department for Transport and the Department for Business, Energy and Industrial Strategy, works closely with industry stakeholders to establish guidelines and best practices for the safe and secure deployment of these technologies. CCAV plays a critical role in fostering collaboration, facilitating knowledge sharing, and ensuring that the UK remains at the forefront of this rapidly evolving field.

Through this holistic approach, encompassing legislation, adherence to international standards, contributions to standard-setting bodies, and close collaboration with industry partners, the UK government is actively supporting the advancement of connected and automated driving technologies while prioritizing safety and security considerations. This proactive stance positions the UK as a leader in this domain, paving the way for the responsible and rapid adoption of these transformative technologies.

South Korea

South Korea has emerged as a leader in the development and deployment of connected and automated driving technologies, recognizing the potential economic and societal benefits these innovations offer. The South Korean government has taken a proactive approach to establishing a supportive regulatory framework that fosters innovation while prioritizing safety and security considerations.

South Korea has adopted the ISO/SAE 21434 standard and actively contributes to the development of global regulations and guidelines through its participation in various international organizations and forums, such as the United Nations Economic Commission for Europe (UNECE).

To support the automotive industry's transition to connected and automated driving, the South Korean government has established a national wide systemic structure to accelerating research, development, and deployment of these technologies.

- **Ministries**

Three Ministries - Ministry of Trade, Industry and Energy, Ministry of Land, Infrastructure and Transport, Ministry of Science and ICT – are mainly support the automotive industry’s evolution focusing on the Ministry’s core mandate.

The government implements various funding programs to support the automotive industry's transition through the respective agency. The agencies aim to accelerate the development of core technologies, foster collaboration between industry and academia, and nurture a skilled workforce capable of driving innovation in this field.

Notable among these are:

Korea Institute for Advancement of Technology (KIAT)

With a mandate to foster the development and commercialization of advanced technologies, KIAT serves supporting various industries, including automotive. Through strategic partnerships, funding initiatives, and technology transfer programs, KIAT facilitates the integration of cutting-edge technologies into diverse sectors, contributing to the nation's economic growth and global competitiveness.

Specifically within the context of automotive industry development, KIAT collaborates with stakeholders to accelerate research, development, and adoption of innovative technologies, ensuring Korea remains at the forefront of automotive innovation.

Institute of Information & Communications Technology Planning & Evaluation(IITP)

IITP is a dedicated organization established to support ICT R&D and promote information and communication technology and industry. It advocates for the integration of cutting-edge ICT into vehicles to improve safety, efficiency, and connectivity. Through facilitating the convergence of ICT with automotive engineering, IITP enhances Korea's standing in automotive innovation and global competitiveness.

- **Korea Autonomous driving Development Innovation Foundation(KADIF)**

KADIF stands as a dedicated task force, orchestrating collaborative efforts among various government agencies, industry stakeholders, and research institutions. It is an initiative born from the Self-Driving Technology Development Innovation Project Group, launched jointly with three related ministries and the National Police Agency. KADIF's primary objective is to lay the groundwork for the commercialization of level 4 autonomous vehicles by 2027. It is committed to enhancing the reliability of autonomous driving technology, attaining global leadership in technology, showcasing self-driving services accessible to the public, and advocating regulatory reforms for emerging industries while striving for global standards. This collaborative endeavour fosters a unified approach to policymaking, expediting the development of viable technology for connected and automated driving.

By adopting a holistic approach that encompasses regulatory frameworks, adherence to international standards, dedicated research and testing facilities, inter-agency collaboration, and investment in research and development, South Korea has positioned itself as a leader in the connected and automated driving landscape. This proactive stance supports the country's automotive industry while ensuring the safe and responsible deployment of these transformative technologies.

5.2 Supporting cybersecurity standards and regulations

5.2.1 Regulations and Standards

The following regulations play a key role in developing sustainable transportation solutions like remote teleoperations

- ISO 26262-1:2018(en) Road vehicles — Functional safety
- ISO/SAE 21434:2021(en) Road vehicles — Cybersecurity engineering

- ISO/IEC 27001:2022(en) Information security, cybersecurity, and privacy protection - Information security management systems — Requirements
- ISO/IEC 27039:2015(en) Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)
- ISO/DIS 7856 Intelligent transport systems Remote support for low-speed automated driving systems (RS-LSADS) – is under development.
- ISO/AWI TS 17691 - Road Vehicles - Principles for human remote support of automated driving systems – is under development.

5.2.2 Bills and framework

- National Institute for Standards and Technology (NIST) has put together a framework for Cybersecurity - https://www.nist.gov/cyberframework
- National Cyber Security Centre in the UK has set up an assessment framework - https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework
- National Cyber Security Centre in the UK has set up a Book of Knowledge to disseminate the knowledge via https://www.cybok.org/knowledgebase1_1/
- The Cybersecurity Maturity Model Certification Framework by the US Department of Defence - https://dodcio.defense.gov/CMMC/Model/
- UK Automated and Electric Vehicles Act 2018
- Automated Vehicles Bill [HL] - Parliamentary Bills

6 Conclusion

In conclusion, the development of a robust and secure remote teleoperation driving system is a complex undertaking that requires a holistic approach to addressing safety and security challenges. By integrating a next-generation Telematics Control Unit (TCU) with an Intrusion Detection System (IDS), this project aims to establish a comprehensive cybersecurity architecture capable of detecting and mitigating potential threats in real-time.

The adoption of the CRISKLE™ toolchain ensures a structured and integrated approach to safety and security analysis throughout the product lifecycle. CRISKLE™ facilitates the identification of potential conflicts or synergies between safety and security requirements, enabling the development of optimized solutions that address both domains.

Furthermore, the use of advanced testing and validation facilities, such as those offered by KATECH, allows for rigorous evaluation and certification of the remote teleoperation system against safety and security standards. This proactive approach to testing and verification instils confidence in the safety and reliability of the technology, while also promoting innovation by providing a clear pathway for manufacturers to bring their products to market.

By combining cutting-edge technology, robust security measures, and a comprehensive safety and security analysis framework, this project sets the stage for the responsible and secure deployment of remote teleoperation driving systems, paving the way for the future of connected and automated mobility.

7 References

[1] - https://www.gov.uk/government/organisations/centre-for-connected-and-autonomous-vehicles

[2] - https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf

[3] - https://smartcity.go.kr/en/2022/06/09/국토부-2030 년-자율주행-서비스-일상화-미래-모빌리티/

[4] - https://www.iso.org/standard/68383.html

[5] - https://www.iso.org/standard/56889.html

[6] – Cybersecurity regulations transform the Connected Car Ecosystem - https://www.frost.com/frost-perspectives/new-opportunities-and-vehicle-architectures-how-upcoming-cybersecurity-regulations-will-transform-the-connected-car-ecosystem