

# Cybersecurity in Motion: A Survey of Challenges and Requirements for Future Test Facilities of CAVs

Ioannis Mavromatis<sup>\*1</sup>, Theodoros Spyridopoulos<sup>3</sup>, Pietro Carnelli<sup>\*2</sup>, Woon Hau Chin<sup>2</sup>, Ahmed Khalil<sup>4</sup>, Jennifer Chakravarty<sup>4</sup>, Lucia Cipolina Kun<sup>4</sup>, Robert J. Piechocki<sup>4</sup>, Colin Robbins<sup>5</sup>, Daniel Cunnington<sup>5</sup>, Leigh Chase<sup>6</sup>, Lamogha Chiazor<sup>6</sup>, Chris Preston<sup>7</sup>, Rahul<sup>7</sup> and Aftab Khan<sup>\*2</sup>

<sup>1</sup>Digital Catapult, London, UK

<sup>2</sup>Bristol Research & Innovation Laboratory, Toshiba Europe Ltd., Bristol, UK

<sup>3</sup>School of Computer Science & Informatics, Cardiff University, Cardiff, UK

<sup>4</sup>Department of Electrical and Electronic Engineering, University of Bristol, Bristol, UK

<sup>5</sup>Nexor Ltd., Nottingham, UK,

<sup>6</sup>IBM Research, Winchester, UK,

<sup>7</sup>Honda R&D Europe (UK) Ltd., Reading, UK

## Abstract

The way we travel is changing rapidly, and Cooperative Intelligent Transportation Systems (C-ITSs) are at the forefront of this evolution. However, the adoption of C-ITSs introduces new risks and challenges, making cybersecurity a top priority for ensuring safety and reliability. Building on this premise, this paper presents an envisaged Cybersecurity Centre of Excellence (CSCE) designed to bolster research, testing, and evaluation of the cybersecurity of C-ITSs. We explore the design, functionality, and challenges of CSCE's testing facilities, outlining the technological, security, and societal requirements. Through a thorough survey and analysis, we assess the effectiveness of these systems in detecting and mitigating potential threats, highlighting their flexibility to adapt to future C-ITSs. Finally, we identify current unresolved challenges in various C-ITS domains, with the aim of motivating further research into the cybersecurity of C-ITSs.

Received on 26 October 2023; accepted on 07 December 2023; published on 31 December 2023

**Keywords:** C-ITS; Cybersecurity; CAV; Cybersecurity Centre of Excellence; Cybersecurity Ecosystem; Threat Detection/Mitigation

Copyright © 2023 I. Mavromatis *et al.*, licensed to ICST. This is an open access article distributed under the terms of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>), which permits unlimited use, distribution and reproduction in any medium so long as the original work is properly cited.

doi:10.4108/eetinis.v10i4.4237

## 1. Introduction

Cooperative Intelligent Transportation Systems (C-ITSs) and the Connected Autonomous Vehicles (CAVs), are expected to revolutionise the Mobility-as-a-Service (MaaS) paradigm [1]. As we move towards smarter and more sustainable cities, there will be numerous opportunities for MaaS use-cases in areas such as on-demand transportation, accessibility, and road safety [2]. However, these use cases will require specialised hardware, complex software implementations, and scalable data architectures [3]. C-ITSs integrate multiple entities for enhanced

transport solutions. As they grow, C-ITSs become complex System-of-Systems (SoS), where independent systems combine to achieve broader functionalities. This complexity introduces significant cybersecurity risks. The different “data surfaces”, communication interfaces, and Internet-facing entry points for such an ecosystem increase the potential vulnerabilities and attack surfaces within a C-ITS [4]. This is especially concerning as the increase in vehicle autonomy means a single attack point could have catastrophic effects on the entire C-ITSs ecosystem and the fleet of vehicles [5].

As CAV adoption increases, a robust cybersecurity assurance framework is needed to ensure safety and public trust [6]. Therefore, this paper presents the concept of a Cybersecurity Test and Evaluation Facility (CTEF) targeting C-ITSs and a CAV-enabled

\*Corresponding authors: Ioannis.Mavromatis@digicatapult.org.uk, (Pietro.Carnelli, Aftab.Khan)@toshiba-bril.com

Cybersecurity Centre of Excellence (CSCE) and a survey of the existing challenges and requirements for such frameworks. CTEF is meant to provide comprehensive testing, certification and monitoring services for CAVs. The cybersecurity considerations of a C-ITS should be tackled holistically [7]. Our proposed solution revolves around cybersecurity testing, evaluation and certification capabilities for future CAVs and related C-ITS infrastructure (e.g., future roadside CAV traffic coordination units), as well as provisions for live attack monitoring of future C-ITS implementations.

The proposed framework includes components for in-vitro, i.e., separate/“glass-walled”, testing facilities in isolated environments, in-situ, i.e., “on-the-premises”, realistic hardware/software evaluation using simulated environments, and in-vivo, i.e., real-world or live testing conditions in actual operational scenarios. It should also support scalable and extensible architectures, cybersecurity assessment schemes, and real-time monitoring of threats. CTEF is intended to investigate cybersecurity vulnerabilities and threats within a sub-system, system, or SoS fashion. To achieve the above, both virtual and physical test facilities are required.

Overall, this paper makes recommendations in four key areas - testing facilities, architectures, assessment schemes and ecosystem requirements. Based on an extensive study of existing best practices and requirements, we describe the methodology for achieving the CTEF’s vision and establishing a rigorous cybersecurity assurance program for CAVs. Our work discusses good practices, standards, considerations, and technological aspects (architectures, technologies and techniques) to accelerate the safe and secure development, trialling, testing and deployment of a cybersecure C-ITS.

Like any other CSCEs found in smart cities or smart factories, key principles like *futureproofing*, *scalability*, *extensibility*, *modularity*, *flexibility* and *reliability* need to be considered for such a framework [8]. The integration of new tools will enable continuous enhancement of the CTEF’s capabilities. Architectures based on concepts like fog computing [9], virtualisation [10] and cloud-native/serverless computing [11] are critical. Our work discusses their importance, adoption and integration within a unified framework. Detailed test regimes combining automated and manual testing are also described. Assurance frameworks aligned with standards like ISO 21434 [12] are discussed. Finally, the ecosystem needs of the CTEF in terms of expertise, infrastructure, and collaboration with regulators and academia are also highlighted.

This paper is structured as follows. Sec. 2 explores the foundational aspects of CAVs, describing the data and attack surfaces and the main system components found in C-ITSs. Related articles are described in Sec. 3,

**Table 1.** List of Acronyms.

Acronym	Description
3GPP	3rd Generation Partnership Project
ADAS	Advanced Driver-assistance System
ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
C2C	Car-2-Car
CAV	Connected Autonomous Vehicle
CA	Certification Authority
CIA	Confidentiality, Integrity and Availability
C-ITS	Cooperative Intelligent Transportation System
CPPS	Cyber-Physical Production System
CSCE	Cybersecurity Centre of Excellence
CTEF	Cybersecurity Test and Evaluation Facility
C-V2X	Cellular Vehicle-to-Everything
DoS	Denial-of-Service
FaaS	Function-as-a-Service
GDPR	General Data Protection Regulation
ITS	Intelligent Transportation System
MaaS	Mobility-as-a-Service
MitM	Man-in-the-Middle
ML	Machine Learning
NCSC	National Cybersecurity Centre
O-RAN	Open Radio Access Network
OSS	Open-Source Software
OTA	Over-the-Air
PaaS	Platform-as-a-Service
PKI	Public Key Infrastructure
QoS	Quality-of-Service
RAT	Radio Access Technology
SaaS	Software-as-a-Service
SAMM	Software Assurance Maturity Model
SCA	Software Composition Analysis
SDLC	System Development Life Cycle
SecaaS	Security-as-a-Service
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SoS	System-of-Systems
V2G	Vehicle-to-Grid
V2I	Vehicle-to-Infrastructure
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VANET	Vehicular Ad-hoc Network

providing insights into the existing literature. The core idea behind the paper is presented in Sec. 4, where we detail the requirements and its scope. Sec. 5 further discusses the architectural design of the CSCE. The test facilities' design and requirements are described in Sec. 6, explaining the in-vitro and in-situ testing and analysis. Sec. 7 presents the core technologies required within CSCE and aligns them with the requirements introduced earlier. The steps that should be taken for smooth integration with the real world are commented on in Sec. 8. The challenges identified across the various entities within CSCE are discussed in Sec. 9, addressing potential hurdles and considerations for a real-world integration and emphasising aspects like privacy and operational requirements. Sec. 10 concludes the paper and summarises our key findings and contributions. Finally, a table summarising all the acronyms can be found in Tab. 1.

## 2. Background

C-ITSs refers to transport systems where the cooperation between two or more sub-systems (e.g., personal, vehicle, roadside and central) enables and provides enhanced services, compared to the traditional Intelligent Transportation Systems (ITSs). C-ITSs utilise wireless communication links to enable real-time Vehicle-to-Everything (V2X) connectivity. This, in turn, enables far greater coordination between road users and the involved systems and creates safer and more efficient traffic flows [13].

A C-ITS reference architecture provides a common framework for planning, defining, and integrating all system components [14]. It essentially provides a common basis for planners and engineers with differing concerns to conceive, design and implement systems using a “common language”. Most critically, reference architectures can help perform attack surface analysis, identify threats, and understand *how* an attack could be executed.

The literature provides various reference architectures. Some lack important details to derive certain attack categories [15], while others are too intricate to interpret by vehicle manufacturers and CAV system designers [16]. For our work, we use the reference architecture from [14] as a basis, also shown in Fig. 1. This reference architecture depicts the main components for CAVs and the devices and peripherals that interact with a CAV, proposing a hybrid Functional-Communication viewpoint that balances the interactions' complexity and depth. More details about the architecture and a description of the components can be found in [14].

### 2.1. CAV Attack Surface

To identify attack surfaces that a threat agent would exploit, two questions should be considered, i.e., what a CAV does and how the CAV can be interacted with to be attacked. As depicted in Fig. 1, various communication buses and links across multiple physical and virtual devices and entities span both the “Cloud” and “Edge” layers.

Following that, we can define an attack surface that constitutes multiple entry points or attack vectors that a malicious user could exploit to gain control, enter or extract data, or perform other malicious activity within a C-ITS [17]. Any device, system, software, or actor (as shown in Fig. 1), both internal and external, that communicates with a CAV component contributes to the attack surface.

The “**digital data surface**” underpins the attack surface. This constitutes the individual data points that flow between system components. The system components will transfer data across the “surface” that could be vulnerable to manipulation and attack. We broadly refer to the “data surface” as the data points generated by CAV platforms and flow between local and networked components [3] (V2X). Finally, a single “data flow” could be described as the flow of information between two specific endpoints (blue lines in Fig. 1).

### 2.2. Modelling and Representing the Data Surface

The “data surface” resides “*above*” in the CAV platform, providing a logical representation of the platform. In other words, it could be described as a “data representation” of the system platform as seen from the network perspective. This abstraction is crucial for understanding the flow of data, its sources, and its consumers within the CAV ecosystem.

CAV systems can be considered as individual entities or SoSs – the latter being a way to group entities that provide a common service or function [18]. An individual CAV platform can be described in terms of:

- **Systems:** a collection of interconnected elements (hardware, firmware, software, etc.) that, combined, achieve specific functionality (or well-bounded set of functions). For instance, a navigation system in a CAV might combine GPS hardware, map software, and route optimisation algorithms.
- **Sub-systems:** individual instances of hardware, firmware and software that can be aggregated to form a system. For example, the GPS module can be a sub-system within the above-mentioned navigation system.
- **Devices:** components within sub-systems that generate or consume the actual data flowing through the CAV platform. The data could be simple data

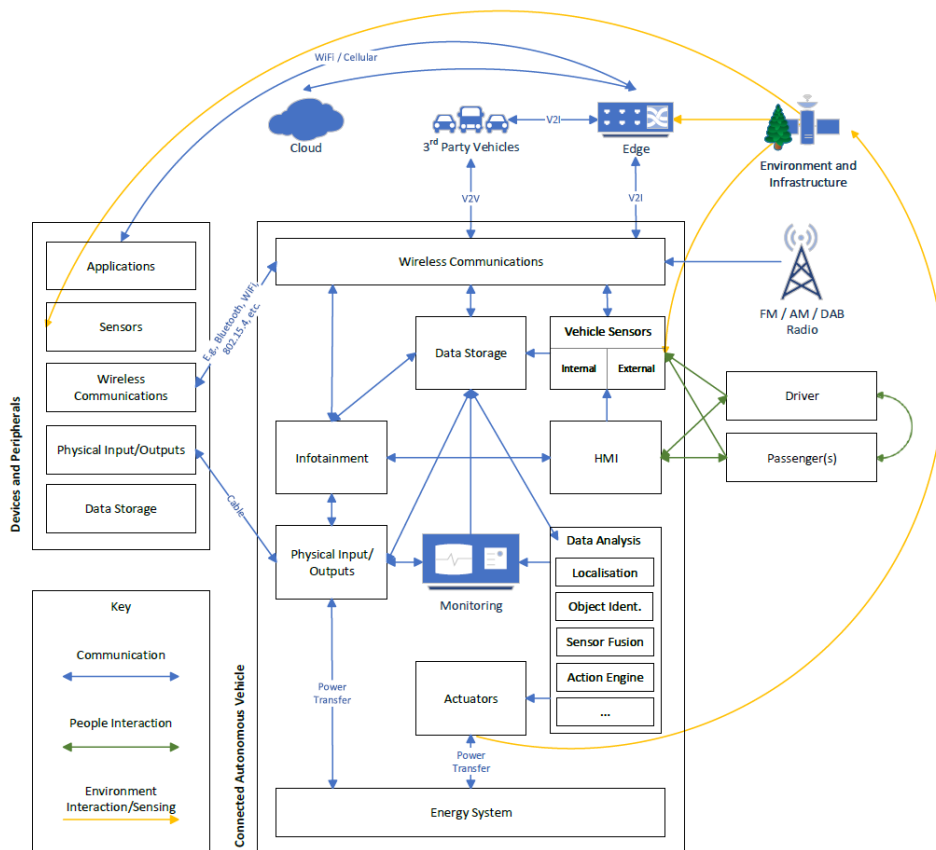


Figure 1. CAV and devices & peripherals reference architecture [14].

types such as numbers, strings, or more complex structures.

A system is a collection of sub-systems that provide a specific *service* or *capability*. The data systems can be described broadly as: 1) *producers*: entities that yield data, such as sensors or the output of processing functions; 2) *consumers*: entities that take data as input, such as applications components or the input to processing functions.

The data surface can be expressed geometrically across  $d$  dimensions with  $n$  data points. It is important to take into account the data types and structures (e.g., simple numeric variables or complex XML structures) as we create layers in the model for different types of data interactions. For instance, raw sensor data might be on one layer, processed data on another, and application-level data interactions on a third. Finally, for a more detailed model, one should include information about the time and frequency domains of the data interactions. This can help in understanding real-time requirements and optimising data flow for efficiency. Some more information about the above can be found in [18], described from the point of view of a Smart City scenario.

### 2.3. C-ITS Communication Domains

Having defined an attack surface and how the data are represented and modelled, we can later identify potential attack vectors, considering the different communication domains. The Car-2-Car (C2C) Communication Consortium identifies three key domains [19]:

- *Intra-vehicle domain*: The different systems and components inside the vehicle (e.g., sensors, onboard computers, infotainment system, Advanced Driver-assistance System (ADAS) features, powertrain, etc.).
- *Ad-hoc domain*: The Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication systems that allow real-time data exchange between vehicles and other entities on the road.
- *Infrastructure domain*: The fixed infrastructure systems like traffic management centres, roadside sensor networks, edge computing nodes, cellular base stations, etc., that provide connectivity support, traffic management, emergency response and other C-ITS services.



As C-ITSs are getting more complex, the above has been further extended recently, adding:

- *Central cloud domain*: The remote cloud computing infrastructure that provides additional services and capabilities to vehicles and transportation infrastructure. For example, it can offer intelligent decision-making agents for traffic management [20].
- *Personal domain*: The mobile devices, wearables and other gadgets carried by individuals that can connect to vehicles and infrastructure in a Vehicle-to-Pedestrian (V2P) fashion [21].
- *Enterprise domain*: The third-party service providers and businesses that are stakeholders in the C-ITS ecosystem [22]. For example, logistics companies managing fleets, insurance providers, location-based service companies, etc.

Sophisticated attacks may target multiple CAV components across various domains. Therefore, a single attack could exhibit multiple data flows across the data surface. In terms of potential CAV cyber-attacks that constitute the attack surface, an attacker may exploit vulnerabilities within the physical infrastructure (e.g., electric charging stations), perform adversarial modifications to sensor data [23, 24], perform poisoning attacks to intelligent agents [25], or perform network attacks that disrupt communications (e.g., a Denial-of-Service (DoS) attack [26]). For a comprehensive overview of various attack points that constitute the CAV attack surface, we refer the reader to [13, 14, 27, 28].

## 2.4. Security Objectives for a C-ITS

From a cybersecurity standpoint, and based on the above, the five main goals to be achieved are:

1. To model and understand potential attack vectors in complex CAV and C-ITS architectures.
2. To detect malicious network interactions, differentiating these amongst a high volume of valid interactions.
3. To distinguish tampered data from normal data and identify attacks in intelligent agents.
4. To protect CAVs and C-ITSs through the deployment of detection and mitigation techniques, limiting the impact of a cyber-attack given the interconnected nature of CAV systems.
5. To ensure the low-latency operation of the deployed detection and mitigation functionality.

The above points have been demonstrated in practice in the past. For example, authors in [29] demonstrated

how they exploited a vulnerability in the vehicle's infotainment system (connected via a cellular network) to remotely take control of the vehicle (goal no.1). In [30], a false data injection attack is demonstrated and the authors provide a way to detect and isolate the attack from regular data exchanged within a CAV application (goal no.2). A sensor fusion technique and a model to extrapolate the vehicle's position and project projection were used in [31] to mitigate against tampered speedometer data (goal no.3). The importance of mitigation strategies is discussed in [32], describing how Over-the-Air (OTA) updates can help manufacturers remotely patch vulnerabilities and reduce the potential impact of cyber-attacks (goal no.4). Finally, in [33], the importance of reliability and reduced overhead is discussed proposing a low-overhead model to identify malicious roadside basestations (goal no.5).

The exchange of data and the various wireless interfaces increase the potential attack vectors within a C-ITS. These threats can expose critical traffic systems and compromise the safety of all passengers and pedestrians. Therefore, it is essential to introduce a solid security framework. Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) [34] describes this framework in the context of three cybersecurity pillars, i.e., Confidentiality, Integrity and Availability (CIA). Briefly, the CIA defines:

1. **Confidentiality**: Restricts access to sensitive information based on the type of information disclosed. For example, confidential data from individual CAVs should be protected as it can be misused. Vehicle ID and speed data can easily identify if the vehicle violates speed limits [35]. Therefore, CAVs should use infrastructure network services to preserve anonymity.

2. **Integrity**: Guarantees the reliability and accuracy of the information and messages exchanged while preventing the alteration of the data from unauthorised intentions or authorised but unintended acts. For example, a sensor fusion mechanism could be used to avoid data modification. Abnormalities could be detected based on the information collected from different but complementary sensors (e.g., camera and LiDAR data). Later, the data could be either discarded or sanitised before being used [36].

3. **Availability**: Ensures authorised access to critical information and system. Availability aims to allow access rather than restrict it. For example, traffic information should be publicly available to all CAVs at any given time [37].

These three are the most crucial components of cybersecurity and form a model to guide policies for C-ITS information security. Balancing between them,

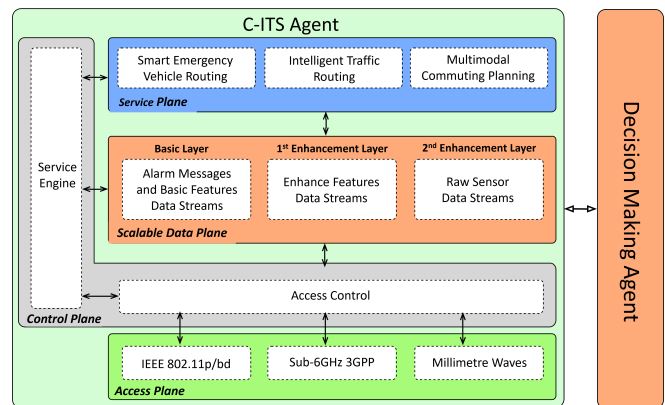
we can ensure high-quality security standards and policies without compromising the usability of a C-ITS. All cybersecurity services support one or more of these objectives. Similarly, all threats undermine one or more of these objectives. Comparing security systems using these metrics can aid designers in selecting between alternatives.

Trust and privacy are two vital aspects of C-ITSs cybersecurity. Trust is achieved by ensuring the exchanged information's integrity, authenticity, and confidentiality. On the other hand, privacy requires rigorous measures to protect personal data from unauthorised access and potential misuse. ETSI TS-102941 [38] highlights the significance of these principles in information exchange within transportation systems. The technologies integrated into CAVs and C-ITSs provide a way to track individuals and vehicles with heightened precision. Maintaining data privacy, such as the license plate or vehicle owner, becomes essential. For example, General Data Protection Regulation (GDPR)<sup>1</sup> establishes stringent data protection and privacy guidelines for individuals and serves as a gold standard for data handling worldwide. Adhering to GDPR provisions, a C-ITS can reinforce user trust, ensure compliance, and ensure the fundamental right of privacy for travellers, fortifying their confidence in the system.

## 2.5. C-ITS Concepts and System Design

Sec. 2.3 discussed the communication domains within a C-ITS. A C-ITS, being an SoS, is responsible for: i) handling scalable applications consisting of independent data flows, ii) employing multiple Radio Access Technologies (RATs) for each flow and mapping them on different layers according to target Quality-of-Service (QoS) constraints, iii) using intelligent agents for decision making. Fig. 2 shows an example of such a system, demonstrating the different data, control and access planes and some example services.

As seen in the literature, future C-ITS are meant to provide different types of services, each one with its own QoS requirements [3, 39]. This could be achieved by providing enhancement layers, extending the base layer's functionality and fulfilling the scalability and extensibility requirements. For example, [3] proposes three main communication planes: i) a base layer, usually based on IEEE 802.11p/bd, responsible for base safety critical message exchange, ii) an initial enhancement layer, based on sub-6GHz 3rd Generation Partnership Project (3GPP) standards and Cellular Vehicle-to-Everything (C-V2X) technologies, that can



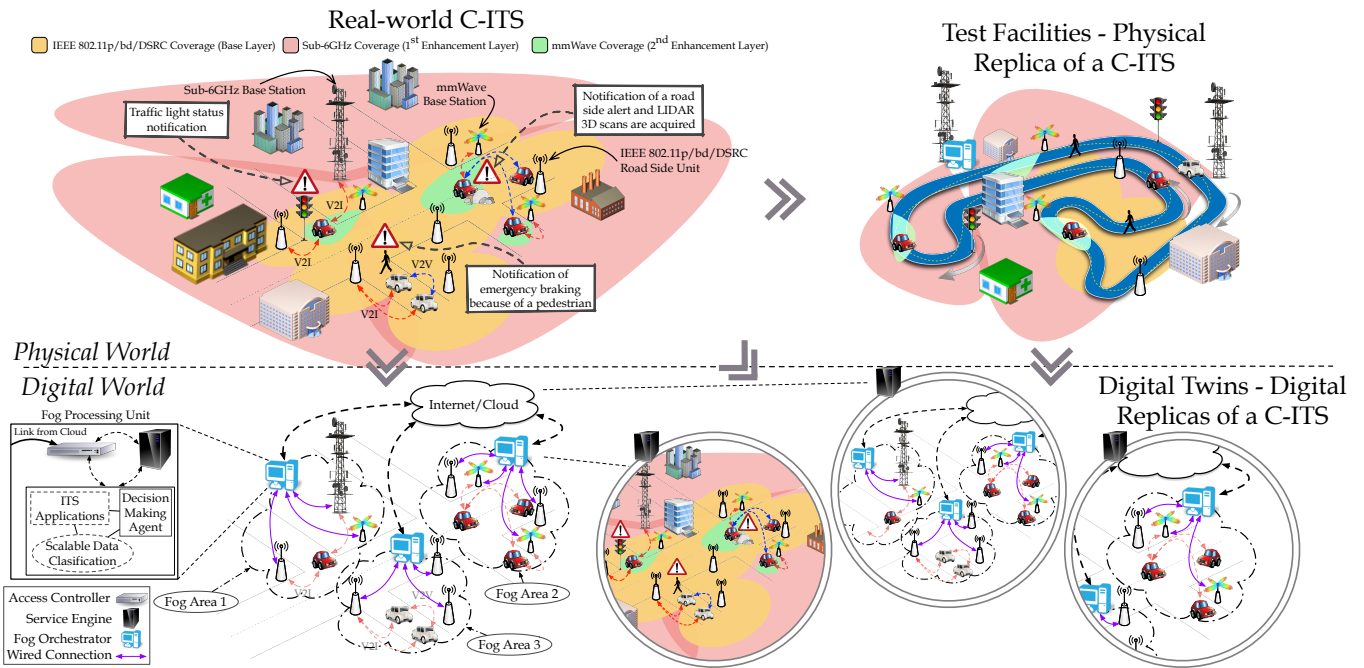
**Figure 2.** The high-level system design of an C-ITS system, showing the interaction between the communication domains, the data exchanged and the different services.

support services spanning over large geographical areas, iii) a second enhancement layer, based on Millimetre-Waves (using IEEE 802.11ad/ay or mmWave 5G NR), that fulfils the requirements for very high data rate and very low latency of the future C-ITS services (also seen in Fig. 2). These technologies and the different layers align with the principle of a scalable data infrastructure mentioned before. However, as described in Sec. 2.3, its one becomes an attack vector that should be taken into account within a C-ITS.

The computing infrastructure supporting a C-ITS is of paramount importance. It supports large-scale C-ITS-related applications such as road safety, traffic efficiency, multimodal commuting, smart parking, etc. For time-critical applications, a hybrid computing model using Cloud, Edge, and Fog paradigms [3, 39] for data analytics and knowledge discovery is required (left-hand side of Fig. 3). Bringing the computing resources closer to the “Edge” enables faster processing and data collection and minimises the network delays introduced by the several hops in the backbone connectivity. Edge processing capabilities are particularly important for Machine Learning (ML)-based solutions, as different types and quantities of machines can work together to accomplish specific objectives. Secs 2.1 and 2.4 briefly touched upon the attack surfaces related to the data plane and the importance of concrete security solutions.

Collected data should be managed appropriately in a C-ITS [11]. Data analysis or mining at the Edge can be performed in different ways. Usually, long-term data storage is handled by the Cloud plane. On the other hand, data that help with time-critical applications are stored in Edge/Fog nodes [9] that are designed to be always ready to use (Fig. 3). The acquired C-ITS data are usually processed by first inspecting their correctness by reviewing the type of data, error rectification, and data cleansing. The evaluated

<sup>1</sup>GDPR official website: <https://gdpr-info.eu/>



**Figure 3.** General overview of the considered C-ITS model and the connection with CSCE. Physical and Digital C-ITS Replicas will be provided within CSCE to enhance the cybersecurity and C-ITS operation.

data is then analysed by sophisticated algorithms, either rule-based or ML-based. Inconsistencies during processing are fixed, and amended data can be further analysed to derive information from it. C-ITS data transmission and analysis at the Fog offers several advantages, these being:

- **Low-latency services:** Analysing data at the collection source reduces the latency as the time needed to transmit is minimised.
- **Resource Management:** Vehicles or pedestrians (nodes) can join and leave the Fog plane at any time. Therefore, a high-speed resource management service will enable real-time network monitoring and control.
- **Bandwidth Management:** Due to the reduced data transmission, the available bandwidth can be better utilised for other purposes.
- **Location Awareness:** Location services help monitor and track the Fog nodes. This will enable the distributed fog nodes to form a multicast group to facilitate rapid decisions for C-ITS application.

The above could be pivotal in achieving a fully functional C-ITS. However, as the above sections show, a C-ITS is a very complex SoS with many moving parts and attack vectors. Moving from theory to practice and bringing C-ITSs and CAVs closer to the real world requires rigorous cybersecurity testing and

well-established frameworks to ensure the solutions' validity. Based on that, in the following sections, we delve into the importance and requirements for cyber test facilities – their architecture and the supporting ecosystem – for enabling the protection of large vehicle fleets and the future C-ITSs.

### 3. Related works

Research activities and industrial initiatives show significant advancements in the context of CAVs and C-ITS. Authors in [40] discussed the necessity for testing and certification for autonomous vehicles with a focus on cybersecurity and ML, highlighting the importance of testing sensors, actuators, and software running on CAVs. They also discuss the importance of accreditation schemes, the creation of vulnerability reporting databases, and how public-private partnerships should standardise testing regimes and processes. Real-world testbeds and facilities like UTAC Millbrook-Culham<sup>2</sup>, ASSURED CAV<sup>3</sup> and Testregion DigiTrans<sup>4</sup> already provide facilities for testing novel CAV and C-ITS services. Our work aims to provide a framework such that facilities like the aforementioned can become more

<sup>2</sup>UTAC Millbrook Testbed: <https://www.utac.com/>

<sup>3</sup>ASSURED CAV: <https://www.horiba-mira.com/assured-cav/>

<sup>4</sup>DigiTrans: <https://www.digitrans.expert/en/>



cybersecurity-aware, incorporating ways of testing and evaluating the cybersecurity of the services developed.

Similar facilities and CSCEs have been proposed in the past. An example is [41], where a cybersecurity research facility is presented. This facility focuses more broadly on general-purpose sensitive data cybersecurity experiments. Their lessons learned discuss the importance of disaster recovery, continuous updates and improvement of the testing facilities and proper management of participants and resources. The team in [42] advocates the importance of nurturing the cybersecurity workforce and presents a framework to improve the skills of potential cybersecurity actors. They highlight the importance of data-driven cybersecurity and various tools and technologies (e.g., cloud-native computing, containers, monitoring and intrusion detection tools, etc.) necessary for cybersecurity practitioners. Building upon the same ideas, our work will focus on the requirements of C-ITS-related test facilities, the technologies required to provide cybersecurity testing functionality and how the outcomes can be adopted in the real world.

Finally, existing works, e.g., [43–45] highlight the necessary evolution in the automotive and related standardisation landscape while providing ethics guidelines and upcoming regulations. Other works [13] focus on the challenges and threats faced by CAVs. We extend both concepts by discussing additional challenges originating from the real-world adoption of the different technologies and frameworks, identifying existing drawbacks in current standardisation activities. Finally, we touch upon the challenges arising from the operational requirements and the resilience required for a real-world system.

## 4. CSCE and CTEF System Description

In the previous sections, we briefly described an envisaged C-ITS and the key security objectives for that. A CSCE should build on these principles and provide the cybersecurity functionality required of a C-ITS. Our envisaged CSCE and its corresponding sub-systems, testing regimes, and relevant stakeholders ecosystem are shown in Fig. 4. The governmental agencies in the diagram are UK-based, but similar organisations are found in all countries and can be part of a given CSCE.

### 4.1. CSCE and its Testing Facilities Requirements

Our envisaged CSCE should provide two main functionalities. i.e., a testing, evaluation and certification facility and a provision for live monitoring and detecting threats in real-time within a C-ITS. The design and proposed solutions should be replicable in the real world with minor modifications. The testing facilities should provide the tools, environments and frameworks for investigating cybersecurity

vulnerabilities and threats within a sub-systemic, systemic, or SoS fashion, either in physical or digital infrastructures. This allows future C-ITS components and CAV manufacturers to run experiments within correctly set-up environments and test their proposed systems for cybersecurity vulnerabilities.

From the above sections, we can identify several requirements. The primary aim of the proposed CSCE is to provide cybersecurity research, test and evaluation services for C-ITSs in a *scalable, adaptable, modular and flexible* way. To achieve this goal, the CSCE should adhere to the following key requirements :

**CR1 – Identification and validation:** C-ITS-wide cyber threats must be identified and evaluated for their significance, likelihood and impact.

**CR2 – Convergence of virtual and physical world:** Both physical (e.g., conducted on a test track in an air-gapped scenario) and virtual (e.g., performed employing simulations and Digital Twins [46]) must be provided, with software and hardware testing support, i.e.:

- *In-vitro testing*, i.e., “sand-boxed” virtual environments to test C-ITS systems and components.
- *In-situ testing*, i.e., testing C-ITS systems interactions with each other and with cits related road-side infrastructure.

**CR3 – Integration of cybersecurity tools and technologies:** Various tools should be utilised to satisfy the safety, security and availability of C-ITS systems, e.g., tools for penetration testing activities or cloud-native security should be supported and provided.

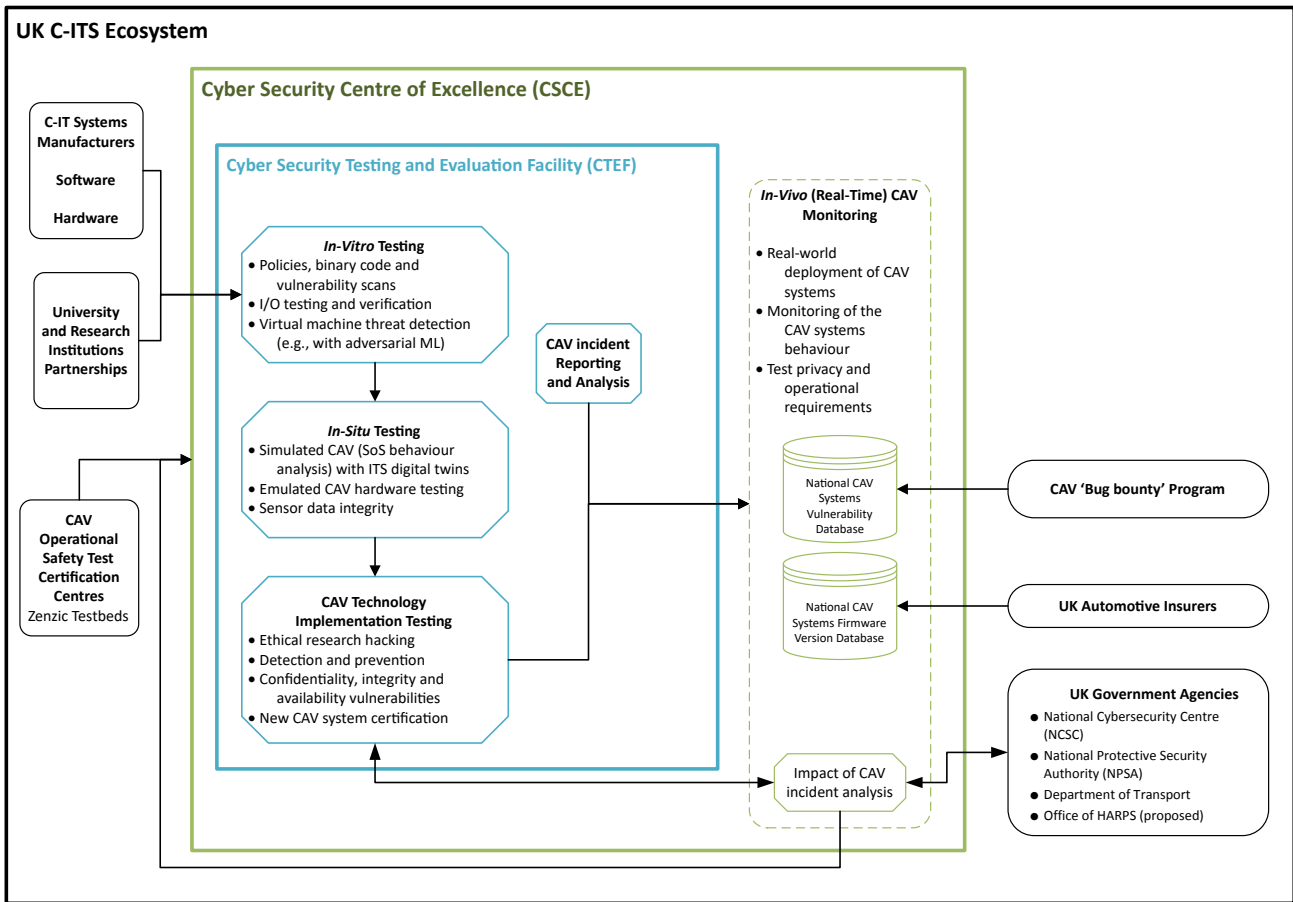
**CR4 – Maturing cybersecurity schemes:** The proposed cybersecurity mechanisms and the tools developed should be matured within cybersecurity incubators. The different components must align with the C-ITS operational requirements, before integrated into the main system.

**CR5 – Automated content curation process:** Bidirectional communication channels should be established that feed data and information from the real world to the test facilities and continuous integration mechanism for deploying the implemented solutions.

**CR6 – Continuous monitoring facilities:** The cybersecurity incidents must be effectively detected, mitigated and prevented in real-time.

**CR7 – Respond and recover mechanisms:** Fallback policies should be in place, so when an attack occurs, to immediately begin recovery.





**Figure 4.** Proposed Cybersecurity Centre of Excellence (CSCE, green box) organisational and operational structure within the UK Cooperative Intelligent Transportation System (C-ITS, black box). Within the CSCE, we propose a cybersecurity Testing and Evaluation Facility (CTEF, blue box) to allow for online (i.e., cloud-based software containerisation of CAV systems and C-ITS infrastructure emulators) testing. Live monitoring of CAVs operating in the UK combined with national CAV systems vulnerability and firmware version databases allows for rapid responses to security-related breaches.

**CR8 – Improved resilience:** A C-ITS must be operational even when affected by a cybersecurity event or attack.

Following the requirements of the CSCE, the supporting test facilities will be used as an “evaluation and testing” platform in an isolated fashion so that detection, mitigation and prevention mechanisms can be tested without affecting a real-world system. The following key requirements are recommended:

**TR1 – Extensibility:** All systems and subsystems must be extensible to allow the addition and testing of new security approaches, evaluation of new modules and security prototypes. Breaking down the testing into smaller manageable components makes it easier to achieve a highly secured system.

**TR2 – Distributed capabilities:** Distributed processing capabilities must be provided to ensure

scalable solutions and improve efficiency and performance.

**TR3 – Bidirectional Interaction with Intelligent Agents:** The testing platform should handle the training data and be able to apply policies generated by ML solutions. A set of good security policies and practices should follow, e.g., regular checks, balances, and reminders, confirming that a new security policy is being enforced.

**TR4 – Security-as-a-Service:** The testing pipeline must employ reconnaissance and penetration testing capabilities as well as vulnerability detection mechanisms in a Security-as-a-Service (SecaaS) fashion. This provides the flexibility to test different components dynamically and introduces a softwarisation and virtualisation approach into the test facilities.

**TR5 – High Adaptability:** The test infrastructure and pipeline must be built on a core baseline but be highly adaptable. The security level of one security domain can be adjusted without affecting the security levels of other domains or systems:

- The choice to conduct specific experiments that use individual systems, or SoS, represent specific architectures and work on different scenarios and use cases.
- Similar process activities must be grouped at the capability level. The capability level is used to assess the risk exposure of assets and processes and specify adequate and consistent security requirements.
- The testing platform must provide tools for threat detection of common network vulnerabilities and aggregated and systemic threats across large fleets of vehicles or C-ITS components.
- The test framework should be easily reset to the stable core functionality and be prepared for a new set of experiments. Significant security risks introduced during the experimentation of a system should be easily reverted back to the state that was proven to be more secure.

**TR6 – External cooperation:** The test facilities must facilitate cooperation with the industry, academia and government to maintain and improve security standards. Using defined security domains allows organisations to engage business partners in determining the appropriate security requirements for each cross-organisational information flow.

**TR7 – Existing development practices:** The test facilities must utilise existing well-established development practices but also allow collaborations with R&D to ensure up-to-date testing and state-of-the-art equipment and technologies are always used.

## 4.2. Scope and Key Characteristics of CSCE

The envisaged CSCE should be able to address the pressing concerns around the cyber threats for C-ITSs and CAVs. It should address both the technological risks as well as provide suggestions for the socio-technical aspects of the surrounding ecosystem (e.g., skills required, public engagement, training on secure practices, etc.). Three different entities will support the CSCE (Fig. 4):

**1. Cybersecurity Test and Evaluation Facility (CTEF):** CTEF is a large and complex SoS based on legacy and state-of-the-art technologies. Like all industrial control systems, CTEF will have unique performance, reliability and safety requirements. CTEF should replicate with high fidelity systems,

services and capabilities of a C-ITS and provide the tools for investigating cyber threats in an “*in-vitro*” or “*in-situ*” fashion. These tools can be physical or virtual implementations that duplicate the real-world interactions between the different systems.

**2. Cybersecure Real-world Intelligent Framework:** The knowledge acquired from the CTEF, should be easily transferable to the real-world. Of course, bidirectional interaction between the two entities is paramount, as identified cyber-threats in the real world should be replicated in CTEF and addressed with novel mitigation strategies in an “*in-vivo*” fashion. The real-time monitoring of systemic interactions can enhance the detection and prevention of risks. This framework should address traditional threats and consider behavioural aspects of CAVs and C-ITSs. The continuous operation of such a system, ensuring that disruptions will not affect the available services, is one of the key aspects that should be considered.

**3. CSCE Ecosystem:** The above physical and virtual infrastructure solutions can address the operational aspects of such a platform. However, the surrounding ecosystem and an incident analysis framework within that is critical. National C-ITS systems’ vulnerability, firmware version databases and bug bounty programs could provide the CSCE with relevant tests and firmware version requirements to ensure all components will be continuously monitored and checked against a set of minimum requirements. Finally, maturity models can ensure high-quality solutions. Understanding the causes of the incident and providing feedback to the test facilities will allow fast prototyping and quick dissemination of solutions. Therefore, our CSCE must be updated (through maturity cycles) in how it operates and accurately assesses future CAV systems.

The socio-technical aspects of CSCE should be extended beyond technology, intertwining human, organisational and technological facets. Addressing cybercrime from other avenues (human-centric, educational-centric, etc.) can reduce its effects. Apart from the social benefits, this could also unlock new revenue opportunities and added economic value, thus making the business aspects part of the ecosystem. The five socio-technical areas to be considered are as follows:

- **Human Factors:** Enhancing cybersecurity awareness is crucial. Training should focus on understanding risks, recognising vulnerabilities, and adopting protective best practices.
- **Public Engagement:** Trust in C-ITSs and CAVs is vital. Open dialogues can address concerns, dispel myths, and foster collective responsibility.

- **Organisational Dynamics:** Organisations should prioritise cybersecurity in strategies, policies, and operations. Regular audits and feedback loops ensure continuous improvement.
- **Collaborative Frameworks:** The complexity of C-ITSs and CAVs demands cross-sector collaboration. Shared initiatives can pool knowledge, resources, and best practices.
- **Regulatory and Policy Implications:** Evolving C-ITSs and CAV landscapes require adaptive regulations. Policymakers should collaborate with experts to develop robust, flexible rules prioritising safety while encouraging innovation.

### 4.3. The Different Dimensions of C-ITS Cybersecurity

A holistic approach to cybersecurity, addressing both human and technical dimensions, ensures a resilient transportation ecosystem. For the remaining paper, the above entities will be further described, focusing primarily on the test facilities and their integration with the real world. Within CSCE, and during the evaluation and testing of the different subsystems, different dimensions (layers) of cybersecurity should be considered for both C-ITSs and fleets of CAVs. These layers can be grouped as follows:

- **Baseline Information Systems Risk:** A CAV is an information system that inherits the standard cyber risks and issues associated with connected information technologies.
- **Domain-specific Risk:** CAV systems provide domain-specific functions and services, each creating specialised attack surfaces that may affect cybersecurity posture.
- **Consequential Risk:** As cyber-physical systems, the operations of CAV platforms have consequences in the physical world, and these must be reflected in the assessment and appraisal of CAV systems.
- **Emergent Risk:** The autonomous component of these platforms introduces risks relating to emergentism – that the system may autonomously arrive at and display behaviours not foreseen or intended by its creators.

## 5. CSCE Architecture and System Design

Secs. 2.5 and 4.1 discussed the requirement for a scalable, adaptable, modular, and extensible architecture. One pertinent paradigm is the Open Radio Access Network (O-RAN) architecture [47]. O-RAN is built on open interfaces and emphasises its disaggregated and virtualised architecture. It promotes cloud-native applications that are modular,

scalable, and easily upgradeable. We envision a similar architecture built upon microservices operating in a containerised cloud-native fashion. Such an architecture can facilitate our system’s dynamic optimisation and integration with multi-dimensional communication planes. Moreover, the CTEF can harness diverse and distributed multi-vendor environments, ensuring the robustness and flexibility of its cybersecurity mechanisms while still maintaining interoperability across the different systems and sub-systems [48]. A distributed design can overcome bottlenecks, especially during high-demand periods [49].

Overall, such an architecture will promote rapidly deploying highly extensible solutions easily transferable to the real world. This flexibility can enable integrating emerging technologies such as quantum computing, advanced AI algorithms, or new cybersecurity tools and tests. By providing finer-grained control over new features, we can speed up the development of new cybersecurity policies in the CTEF facilities, foster collaboration between research organisations, and provide a robust framework for research and innovation.

Two critical aspects of the system are its continuous learning and improvement and the focus on open standards and interoperability. Through real-time monitoring and feedback loops, CSCE can continuously learn from its operations, adapt to new threats, and improve its defences, ensuring the system remains robust and relevant. By adhering to open standards, the CSCE ensures seamless integration with other systems and provides a “common language” for various engineers.

Working in a SecaaS fashion, the CSCE can provide all the above-mentioned tools and services for automation, self-management and scalability in an as-a-service fashion. This will allow individuals and corporations to test their solutions without substantial capital outlays or complex initial implementations. When deployed in the real world, the solutions implemented can benefit from such an approach. The elasticity of these approaches and the benefit of short-lived virtualised platforms can reduce the “window of opportunity” for attackers while maintaining availability, fast response times, disaster recovery and promoting vendor partnership and collaborations.

Finally, our CTEF and CSCE will advocate for Digital Twin implementations, allowing cybersecurity solutions to be demonstrated using real-world data in virtual environments. This ensures that developed solutions will be directly applicable in the real world. A high-level conceptual diagram of this architecture can be seen in Fig. 3. The following sections will discuss the requirements for the testing facilities, the technologies

that can facilitate the proposed CTEF and CSCE and existing challenges.

## 6. Designing a CTEF

As explained earlier, the CTEF assesses the cybersecurity of software and hardware C-ITS components. It is essential to perform a comprehensive analysis that includes both “in-vitro” and “in-situ” testing to ensure fast sample analysis and improved system performance. In the upcoming sections, we will provide a detailed description of these two testing categories along with their corresponding requirements.

### 6.1. CTEF: In-vitro Testing and Analysis

In-vitro testing is an automated analysis of software samples outside their system context. It can identify malicious software through static and dynamic analysis in isolated virtual environments [50]. In-vitro testing can minimise the overhead and resource utilisation of time-consuming penetration tests and systemic behavioural analyses and serves as the entry point for software samples to be tested in the CTEF or in parallel with in-situ tests.

In-vitro testing should meet traditional IT malware analysis requirements [51, 52]. The operational requirements that a C-ITS introduces are not considered at this stage since they are addressed in the in-situ tests. However, in-vitro tests should still provide efficient and scalable functionality to accommodate many concurrent tests. Sec. 6.2 provides the methodology for in-vitro testing, and Tab. 2 summarises the key functional requirements. More specifically, we have:

**VTR1 – Detection of known malware:** Malicious software is identified by evaluating specific instructions and/or byte sequences against known vulnerability databases. An efficient automated signature generation method should be implemented, as described in [53], to reduce the time required for static analysis, also linked to a requirement for continuous integration (Req. VTR7).

**VTR2 – Detection of unknown malware:** Zero-day attacks, i.e., malware that exploits vulnerabilities not known before and malware that transforms their code to evade signature-based detection mechanisms, must be detectable within CTEF, rendering traditional signature-based malware detection tools as insufficient. ML strategies could be employed to detect such malicious behaviours [54]. Potential datasets for that are NSL-KDD [55] and its extensions, consisting of 125k samples and 41 features, EMBER [56], with more than 1M samples, and more. The detection capability can be

Table 2. Requirements for In-vitro testing and analysis.

Req.	Requirement Description
VTR1	Must be able to detect existing malware
VTR2	Must be able to detect unknown malware
VTR3	Must be able to detect software vulnerabilities
VTR4	Must consider and defend against attacks to the detection mechanisms
VTR5	Must be scalable to allow concurrent testing and analysis of multiple CAV software samples
VTR6	Must enable an easy transition to a clear state
VTR7	Must be updatable on the fly to incorporate new cyber threat detection capabilities
VTR8	Must be isolated from the outside world to avoid network contamination
VTR9	Must be able to provide multiple OS environments for testing and analysis
VTR10	Must maintain a log of scanned software and produce relevant reports
VTR11	Should allow a user to create an account and test their software
VTR12	Software samples that are to be tested should not be visible to anyone apart from the user that submitted the software

based on detecting anomalies in the normal operation of the virtual environment when the software sample is executed in it (anomaly detection using unsupervised learning) or on the similarities in the behaviour of the software sample with the behaviour of known malware (supervised learning).

**VTR3 – Software vulnerabilities detection:** Bad coding practices and security holes in the software can result in vulnerabilities. Other malicious software and malevolent actors can exploit these code vulnerabilities. In the CTEF, vulnerability detection will be realised in two ways:

- ML techniques can be used to automate the detection of vulnerabilities in the source code [57]. The existence of a large open source codebase favours the training of ML (e.g., multiclass classification of source code vulnerabilities using deep learning or Recurrent Neural Networks when only binaries are available).
- Where the source code is unavailable, ML techniques will be used to automate the detection of vulnerabilities in the binary code [58].



**VTR4 – Defence against adversarial ML:** ML can detect unknown malware and vulnerabilities, but it is vulnerable to attacks such as input manipulation, model attack and model theft that aim to force deliberate misclassification of inputs [59]. CTEF must consider defence strategies against these attacks and also integrate new solutions into the implemented pipelines, leveraging its extensibility and scalability (Req. **VTR5**).

**VTR5 – Scalability:** In-vitro testing will use cloud-native services for scalability and concurrent testing. Tests will run in ephemeral and isolated environments (e.g., in the cloud or containers) [49], as presented in Figure 5. The environments must reset to their initial state after each test.

**VTR6 – Easy restoration to a clean state:** Similar to Req. **VTR5**, virtualised environments will enable easy reset and restoration of the system to a clean state after the end of a test [49]. This, in conjunction with multiple virtual environments, will allow for more efficient operation, improving the overall performance of the CTEF.

**VTR7 – Update on the fly:** In-vitro tests must stay updated with new cyber threats. ML-based detection models must be regularly retrained to avoid concept drift over time [25] and improve their detection capability. Additionally, adopting multiple well-supported open-source signature-based malware detection tools will further improve the detection effectiveness. Finally, virtualised environments can enable real-time updates and integration of new detection capabilities.

**VTR8 – Avoid network contamination:** Using virtualised testing environments will enable the isolation of the in-vitro tests from the outside world, thus avoiding network contamination. The virtual environments must be appropriately set up to avoid external network connections.

**VTR9 – Multiple OSs:** Similar to Req. **VTR8**, the use of virtualised environments will enable the running of a variety of operating systems, which in turn will allow software execution and behaviour analysis in the appropriate set-up.

**VTR10 – Logging and reporting:** Each test in the in-vitro environment will be logged along with the test output in a centralised database. The database will keep a record of all users and software tested. The CTEF must follow traditional IT systems-based information risk management and privacy policies and regulations (e.g. ISO 27001 [60], GDPR, etc.) to ensure appropriate data privacy and protection.

**VTR11 - User interaction:** The CTEF should provide a user interface to allow users to upload their software for testing. Similarly to Req. **VTR10**, the user interfaces and backend implementations should adhere to best practices and standards for IT systems-based information risk management (e.g. ISO 27001 [60], GDPR, etc.).

**VTR12 – Manufacturers Confidentiality:** To ensure manufacturers’ confidentiality, software samples for testing will only be accessible to the submitting user. Virtual environments used in testing must not be accessible by other users and will be reset and restored after each test. Data stored in the CTEF must be visible only to the user whose software generated the data.

## 6.2. High-Level Design for In-vitro tests

The in-vitro testing is broken down into four subtests: static analysis, dynamic (behavioural) analysis, vulnerability detection in the source code and vulnerability detection in the binary code as shown in Fig. 6. Each subtest will be executed in an isolated virtual environment addressing the Reqs. **VTR5** to **VTR9**.

Scheduling optimisation can be performed by a “hypervisor/orchestrator” -(Fig. 6). After submitting the software samples to be tested, the hypervisor can determine the number of virtual environments needed and the scheduling of subtests. We expect the number of virtual environments needed to be dynamically changed so that software samples that fail one of the subtests do not consume system resources. The complexity and performance of each subtest will also be considered in the scheduling process. For instance, static analysis is much faster and resource-light than dynamic analysis; as such, in a single sample analysis case, static analysis should always precede dynamic analysis. Resource allocation/deallocation and subtask scheduling will be automated to further improve the testing system’s performance.

So, based on the above, we envision an in-vitro environment that will consist of four components (Fig. 7):

1. the user interface allowing user registration and software submission to the system in a secure way,
2. the CTEF management and configuration system providing the appropriate APIs to run the desired tests and user management, test configuration and logging capabilities,
3. the hypervisor for spawning virtual tests and optimise the use of resources in a cloud-native manner, and finally,
4. the actual tests that will be run in the spawned virtual environments.

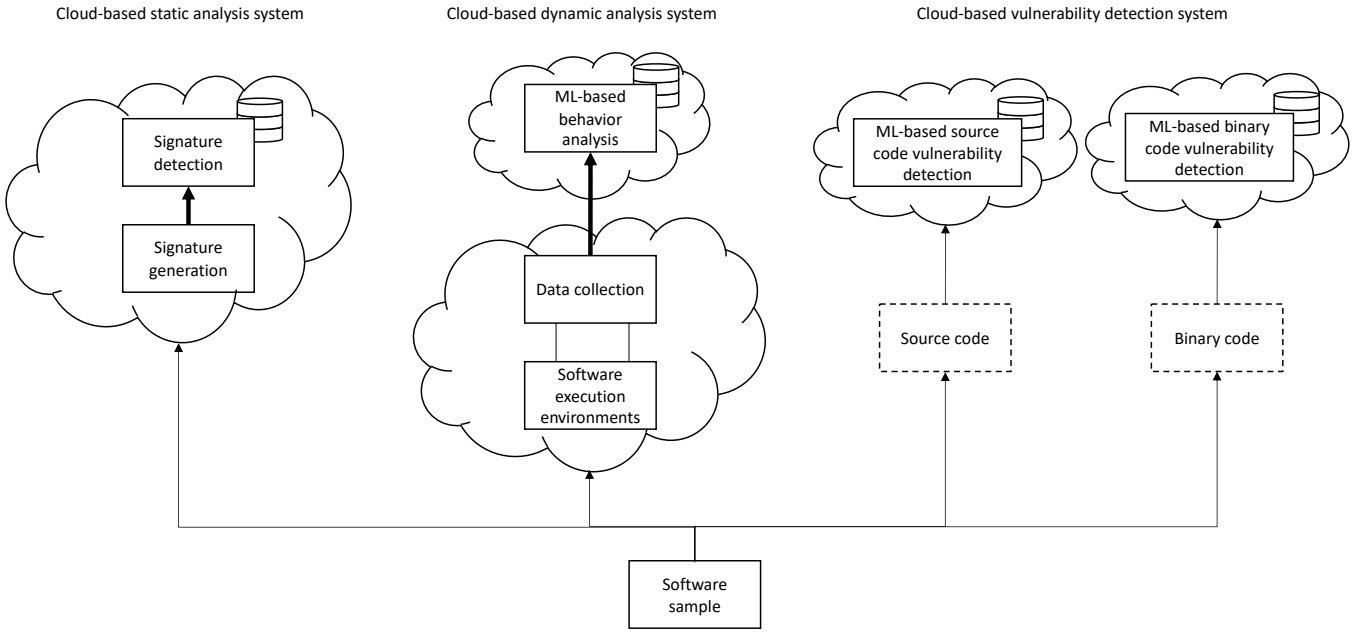


Figure 5. Example of an in-vitro's cloud-based software analysis system.

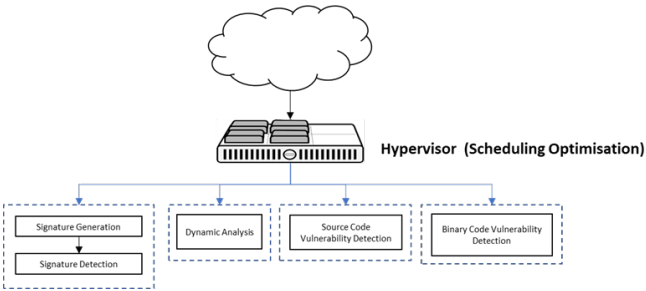


Figure 6. In-vitro CTEF testing and optimisation regime.

	TESTS	(static, dynamic, vulnerability detection)
	HYPERVISOR	(management and optimization of virtual environments)
	CTEF MANAGEMENT	(user management, privacy and authentication, test logs, APIs etc.)
	USER INTERFACE	(user registration, user authentication, software submission)

Figure 7. In-vitro high-level architecture diagram.

### 6.3. CTEF: In-situ Testing and Analysis

In-vitro testing can detect malicious software and vulnerabilities but does not account for the interaction between CAV and C-ITS infrastructure. In-situ tests allow CAV systems to interact with virtual CAVs and C-ITS-related environments, providing a more realistic evaluation of software and hardware components. For example, a malicious CAV may aim to brake suddenly at a busy intersection to block or collide with other vehicles. While triggering the CAV braking control sequence may not seem suspicious or malicious on its

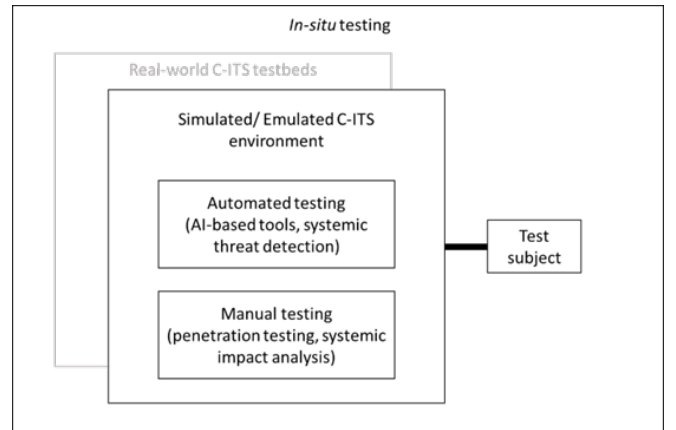


Figure 8. Proposed in-situ testing scheme.

own, the context of where the CAV stopped, i.e., in the middle of a busy intersection, suggests malicious behaviour. In-situ testing aims to fill this gap by providing realistic C-ITS environments for testing and evaluation.

Rigorous, transparent, and replicable cybersecurity in-situ testing of new hardware and software will occur in simulated C-ITS environments in C-ITS testbeds. Testing environments will evaluate the security of new technologies and analyse their impact on the system's operations and performance. These tests will not replace traditional penetration testing techniques. On the contrary, in-situ tests will be operated as automated standalone tests in conjunction with penetration testers while emulating real-world C-ITS scenarios (Fig. 8). In such a setup, penetration tests will investigate

Table 3. Requirements for In-situ testing and analysis.

Req.	Requirement Description
ST1	Must be run in a configurable C-ITS test environment
ST2	Must support multiple C-ITS configurations
ST3	Must support simulation of processes and devices
ST4	Must support all data flows identified in C-ITS
ST5	Must include a diverse range of devices and protocols
ST6	Must produce performance metrics based on the C-ITS operational requirements
ST7	Must detect vulnerabilities by performing penetration tests
ST8	Must run a series of cyber attack scenarios
ST9	Must provide tools to perform penetration tests
ST10	Must detect links between cyber-attack scenarios and misuse scenarios
ST11	Must provide data logging capability for all data flows
ST12	Must provide the tools to perform behaviour analysis for threat detection
ST13	Must enable an easy transition to the initial/clean state
ST14	Must keep the complexity of experimental infrastructure at check
ST15	Must be designed with scalability and flexibility in mind in order to be transferable to the real world

the V2X data flows within an C-ITS. The collected data will be analysed using ML-based approaches to detect potential systemic malicious behaviours. Sec. 6.4 provides the methodology for in-vitro testing and analysis, and Tab. 3 summarises its requirements. The requirements are tailored to the needs of a C-ITS and account for the lessons learned from previous cyber-security testbeds [61]. Briefly, we have:

**ST1 – Configurable C-ITS test environment:** In-situ tests should run in simulated/emulated C-ITS environments, either digital (a computerised simulation of a C-ITS) or real-world (e.g., Zenic’s testbeds<sup>5</sup>). In-situ testing could be based on the packet-level vehicular simulation frameworks such as Veins [62] integrated with traffic simulators such as SUMO [63]. This will allow for the monitoring

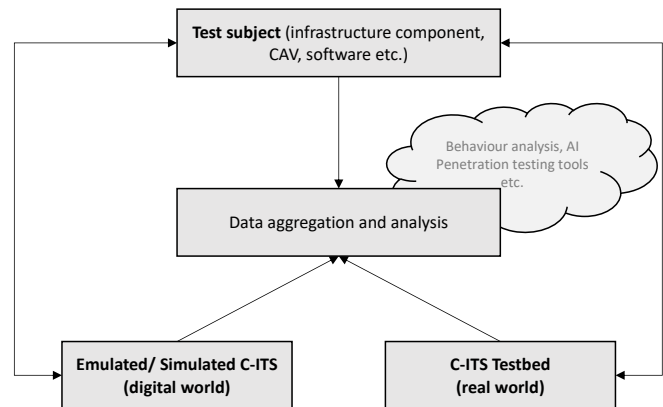


Figure 9. In-situ high-level interconnections.

and analysis of communication patterns and the detection of network anomalies. CAV or C-ITS related hardware and software could be “plugged in” to the simulated environment and interact with digital entities (simulated vehicles and/or infrastructure) at the network level (Fig. 9).

**ST2 – Support multiple C-ITS configurations:** The use of a digitally simulated C-ITS environment will enable the deployment of a variety of different scenarios with different system configurations. These configurations must align with the requirements of real-world C-ITS testbeds to ensure rapid development, testing and deployment.

**ST3 – Simulation of devices or processes:** The simulated C-ITS environment can enable the simulation of devices and processes and create more realistic and complex scenarios. Exposing various APIs can enable an easier connection between the tested software and the simulation framework.

**ST4 – Support all data flows in C-ITS:** To better mimic the real world, the simulator/emulator used must support all data flows identified in a C-ITS (as described in Secs. 2.1 and 2.2 and shown in Fig. 1).

**ST5 – Diverse devices and protocols:** The C-ITS and vehicular communication protocols (e.g., IEEE ITS-G5, 3GPP LTE, etc.) should be supported by the simulation frameworks, implementing the different standards. Additionally, cybersecurity tools used to evaluate the security of the software/hardware undergoing testing must be compatible with these communication protocols.

**ST6 – Performance metrics:** A baseline profile should represent the system’s behaviour without adding other software or hardware. This profile, generated before any modification, can be compared to the network performance achieved (jitter, throughput, etc.)

<sup>5</sup>Zenic C-ITS Testing in the UK: <https://zenic.io/testbed-uk/>

after adding the new software or hardware to the testing environment.

**ST7 – Vulnerabilities detection/Penetration testing:** Penetration tests can provide insight into the likelihood of a threat occurring and how successful a cyber attack could be<sup>6</sup>. Such capabilities must be incorporated in in-situ testing. Following the guidelines on cybersecurity provided by the US Department of Transportation [64], the scope of the penetration tests should include security policies, devices, applications, networks, access controls, communications and configurations that can compromise the C-ITS. In-situ penetration tests will consider the following:

- **Infrastructure:** Includes field devices such as traffic sensors, traffic control and signalling, public messaging etc. and the wireless and wired networks that support them.
- **Traveller:** Encompasses the devices used by the traveller to access C-ITS services (e.g. traffic or emergency notifications).
- **CAVs:** Software and hardware found in CAVs and communication with other entities in a C-ITS.
- **Communications:** Includes the communication components of the C-ITS. These include various wireless technologies such as Wi-Fi, WiMAX, mmWAVE, cellular networking, etc.

Finally, tests should be provided on all categories, i.e., black, grey and white box testing [65]. These tests should be structured based on the attack scenarios we describe in Req. ST8 and cover all phases of a cyber attack, as described by the Cyber Kill Chain Model [66].

**ST8 – Cyber attack scenarios:** Penetration tests must be structured on a series of cyber attack scenarios tailored to C-ITS, as discussed in [26, 67]. The selection of the attack scenarios is controlled by the penetration tester, depending on the component to be tested. Attack scenarios can be categorised into Physical, Wireless, Network and Vehicular Ad-hoc Networks (VANETs). Tab. 4 summarises the attack scenarios, excluding organisation attacks, against components in a C-ITS. More details about these attacks can be found in [27, 28].

**ST9 – Penetration testing tools:** To enable the execution of the attack scenarios described in Req. ST8, in-situ will also provide the appropriate penetration testing tools described by the Penetration Testing Execution Standard [68]. The testing tools will be integrated into a penetration testing suite and executed

in a cloud-native-based approach inside a virtualised environment. Tools must be compatible with all technologies and communication protocols in C-ITS.

**ST10 – Link cyber attacks to misuse scenarios:** To allow for better threat analysis, in-situ testing will link the attack scenarios presented in Tab. 4.

**ST11 – Data flow collection and storage:** To enable better analysis and aid for research and development, all data flows must be stored anonymously and securely. Furthermore, the tests and actions should be logged and aligned with the stored data. Data stored can aid in researching and developing new cybersecurity tools and testing methods.

**ST12 – ML-based threat detection:** Appropriate ML-based threat detection algorithms should be used to detect abnormal behaviour within the simulated C-ITS environment. Threat detection must be performed before and after penetration tests to ensure the detection of malicious changes in the system that exploit vulnerabilities. This will allow for the detection of malicious hardware/software as well as vulnerability exploitation, as highlighted in Fig. 10.

**ST13 – Easy transition to initial state:** Virtualised environment must return to an initial state after testing. By doing so, we can ensure that controlled environments are always used for experimentation.

**ST14 – Managing the complexity:** A digital network management system should be deployed to oversee the operation of the CTEF as tests are being carried out. The management system should be responsible for the following operations:

- Register new tests.
- Allow the configuration of a new C-ITS testing environment (in case of a digital simulation) or connect to real-world C-ITSs testing environments.
- Spawn new C-ITS simulation environments (in case of a digital simulation). The tested SW/HW will be “plugged ” into the simulation environment.
- Capture, store, and visualise all generated data within the C-ITS (digital or real-world) testing environment. Present system performance metrics.
- Analyse the generated data using cloud-based ML-driven cybersecurity tools (aligns with Req. ST12).
- Initiate cloud-based penetration testing platform to be used by the facility’s penetration testers (aligns with Reqs. ST7, ST8 and ST9).
- Log executed tests and results.
- Update the data analysis tools and the penetration testing platform to address new threat vectors.

<sup>6</sup>NCSC penetration guide for testing: <https://www.ncsc.gov.uk/guidance/penetration-testing>



**Table 4.** Cyber attacks against C-ITS.

Attack Types	Attacks
<b>Physical Attacks</b> (attacks deployed by having physical access to the component to be tested)	<ul style="list-style-type: none"> <li>• Physically connecting to exposed ports, e.g., USB, serial, etc.</li> <li>• Using brute force or guessing credentials on a device</li> <li>• Sniffing network traffic between a device and the backend</li> <li>• Scanning the secured/closed network to discover the topology</li> <li>• Deleting files on the compromised C-ITS device/system</li> <li>• Dumping firmware to recover credentials and configuration</li> <li>• MitM attacks using exposed wires/cables to intercept data</li> <li>• Physically tamper with a device to steal/compromise data, modifying a device, etc.</li> <li>• Connecting a removable storage device loaded with malware to install</li> <li>• Sending improper commands to the controller and backend servers</li> <li>• MitM attack communications and sending false data to backend servers</li> <li>• Pivoting a C-ITS device as a trusted entry point into the corporate network</li> <li>• Exploiting vulnerabilities in software, hardware, protocols, OS, etc.</li> </ul>
<b>Wireless Attacks</b> (attacks deployed against or/and via wireless communications)	<ul style="list-style-type: none"> <li>• Spoofing V2V, V2I, and I2I messages broadcast to traffic and the rest of the C-ITS ecosystem</li> <li>• Sniffing wireless transmissions, e.g., using the car’s Wi-Fi</li> <li>• Remotely transmitting and installing malicious firmware</li> <li>• Electronic jamming of wireless transmissions to disrupt operations</li> <li>• MitM attack with wireless transmission to intercept and/or modify data</li> <li>• Exploiting vulnerabilities in software, hardware, protocols, OS, etc.</li> <li>• Using vehicle Wi-Fi as an entry point into the controller area network (CAN) bus and then to the on-board diagnostics (OBD), telematics control unit (TCU), and in-vehicle infotainment (IVI)</li> <li>• The remote hijacking of vehicle controls via compromised CAN bus</li> <li>• Installing malicious third-party apps in a car’s infotainment system</li> <li>• Attacking via a malicious app installed on a phone connected to the car’s Wi-Fi</li> <li>• Electronic jamming of vehicle’s safety systems, e.g., radar, ultrasonic sensors, etc.</li> </ul>
<b>Network Attacks</b> (attacks that take advantage of the connection of C-ITS components to the Internet (Internet-exposed C-ITS systems))	<ul style="list-style-type: none"> <li>• Identifying and abusing device misconfigurations</li> <li>• Exploiting vulnerabilities in legacy software and hardware</li> <li>• Installing malware/spyware on systems</li> <li>• Uploading and installing malicious firmware</li> <li>• Launching DDoS attacks on internet exposed C-ITS infrastructure and backend servers</li> <li>• Exploiting vulnerabilities in software, hardware, protocols, OS, etc.</li> <li>• Credential brute-forcing and abusing weak authentication mechanisms</li> <li>• SQL injection attacks</li> <li>• Cross-site scripting (XSS) attacks</li> <li>• Session hijacking attacks</li> <li>• DNS spoofing and hijacking attacks</li> <li>• Pass the Hash attacks</li> <li>• Pass the Ticket attacks (Kerberos)</li> <li>• Sending improper commands to the controller and backend servers</li> <li>• Pivoting an ITS device as a trusted entry point into the corporate network</li> </ul>
<b>Attacks against VANETs</b> (attacks exploiting Vehicular Ad Hoc Networks)	<ul style="list-style-type: none"> <li>• Sybil</li> <li>• DDoS</li> <li>• Blackhole</li> <li>• Wormhole</li> <li>• False information</li> <li>• Replay</li> <li>• Passive eavesdropping</li> </ul>

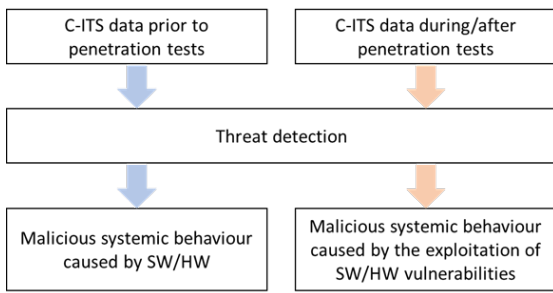


Figure 10. In-situ C-ITS threat detection.

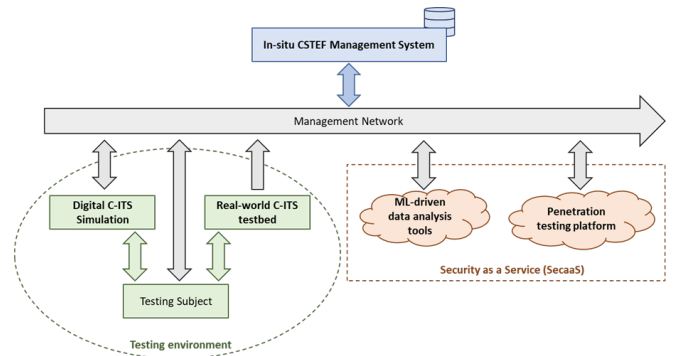


Figure 11. In-situ high-level architecture diagram.

- Terminate running tests.

CTEF must follow traditional IT systems-based information risk management and privacy policies and regulations (e.g. ISO 27001 [60], GDPR, etc.) to ensure user data privacy and cyber protection. More information is provided in Sec. 2.4.

**ST15 – Transferability to the real world:** In-situ tests and solutions must be designed with scalability and flexibility in mind. This allows easy integration into the real world. The adoption of a SecaaS approach, along with the use of simulated C-ITS environments, satisfy the two requirements. Using a single management network to which all tools and testing environments are connected favours the extensibility.

#### 6.4. High-Level Design for In-situ tests

In-situ CTEF is broken down into five stages as presented in Fig. 11. This includes the Management System, the Digital C-ITS simulation, the Real-world C-ITS testbed, the ML-driven data analysis tools and the penetration testing platform.

The data analysis tools and penetration testing platform will run cloud-natively. Penetration testers can use the platform to run the attack scenarios described in Req. ST8. The penetration testing platform can be implemented independently of the other components. The ML data analysis tools depend on data from the digital and real-world C-ITS simulations. ML algorithms will be trained with simulator data and then improved with real-world data.

The C-ITS simulation environment can be cloud-based or locally implemented. Cloud-based simulations offer flexibility but add latency. Local implementation reduces latency and favours flexibility and scalability while better representing a C-ITS environment. The management network connects SecaaS, testing environments, and the CTEF Management System. Real-world testbeds will also be used, and existing ones will be adapted to grant SecaaS platforms access to data planes.

## 7. Technical & Functional Specification

This section describes the technologies that will provide CTEF with the modularity, extensibility, scalability and robustness required. We align each technology’s benefits with the requirements described in Sec. 4.1. As known, each state-of-the-art technology solves many issues but also brings new challenges, so in the following sections, we will delve into the cybersecurity challenges that need to be addressed for all the presented technologies.

### 7.1. Microservices Architecture in Cybersecurity

A microservice architecture [69] is a set of services loosely coupled to implement an application. These services provide finer-grained control over an entire application that operates as a whole. Microservices are rapidly gaining popularity in the System Development Life Cycle (SDLC) community as they facilitate continuous delivery for larger applications and more straightforward adaptation when the requirements are updated. The benefits with regards to cybersecurity and CSCE are summarised as follows:

- **Granular Security Controls:** As each microservice handles a specific function (e.g., TLS certificate dissemination, encryption of persistent data, etc.), security measures can be applied with more precision. This granularity facilitates independent scaling within a SoS to meet varying security demands and counteract specific threats (aligns with Reqs. CR3, CR8, TR1, and TR2).
- **Diverse Defense Mechanisms:** The flexibility of microservices allows each service to be developed using different languages or frameworks. This diversity makes it harder for attackers to exploit a systemic vulnerability, as each service could potentially present a unique defensive profile (aligns with Reqs. CR3, and TR1).
- **Isolated Incident Management:** With modular design, breaches or vulnerabilities in one service

do not necessarily compromise others. Isolation enables efficient troubleshooting and targeted fixes, enhancing the robustness of the overall system. Testing processes are streamlined since issues can be narrowed down quickly (aligns with Reqs. **CR1** and **TR1**).

- **Secure Continuous Delivery:** Implementing security measures in microservices ensures that changes across the application's lifecycle are introduced without compromising security. When cross-functional teams, including developers, operations, and testing teams, focus on a single service, integrating security measures becomes an intrinsic part of the delivery process (aligns with Reqs. **CR5**, **CR6**, **TR6**, and **TR7**).
- **Proactive Threat Detection:** Continuous and robust monitoring ensures real-time oversight of the security landscape. In case of security anomalies or a service malfunction, predefined mitigation strategies can immediately spring into action, be it to restart a compromised service or initiate countermeasures against potential threats (aligns with Req. **CR6**).

## 7.2. Cloud-native Architectures for Cybersecurity

A cloud-native infrastructure serves as the backbone to support the microservices approach vital for use-cases like C-ITS and Smart Cities [70]. This approach is widespread in many Smart City, Robotics, and Infrastructure projects (e.g., as in [71, 72]) and aligns with the key concepts for future C-ITSs [3]. Cloud-native architecture harnesses the inherent capabilities of cloud computing to enhance the security and efficiency of systems. Key benefits include automation of microservices, horizontal and vertical scaling, and resilience. This enables easier management and operations of complex microservices-based systems [48].

Smart Cities and C-ITSs are both inherently exposed to cyber threats due to their wide digital footprint. A cloud-native approach offers:

- **Secure Automated Deployment:** Cloud-native ensures that deployment and management of numerous microservices are automated, reducing human error and potential security vulnerabilities (aligns with Reqs. **TR1** and **TR5**).
- **Dynamic Scaling:** As systems experience varying demand, cloud-native offers adaptive scaling without compromising security standards (aligns with Req. **TR1**).
- **Resilience:** By leveraging distributed architectures, resilience is assured even in the face of concentrated cyber attacks (aligns with Req. **CR8**).

- **Managed Security Services:** Cloud-native encourages the use of managed cloud services, like secure databases, encrypted messaging, and robust storage solutions, enhancing the security ecosystem (aligns with Req. **TR2**).

This architectural advantage ensures that the CTEF and its subsystems remain agile, responsive, and secure against evolving threats. Cloud-native infrastructure becomes pivotal when meeting the SecaaS specifications mentioned in **TR4**. By integrating Software-as-a-Service (SaaS) principles, security services are not only provisioned on-demand but also fortified and elastic. Overall, a well-designed cloud-native architecture will provide the foundation for CTEF and the extensibility and adaptability required for such a system.

## 7.3. Containerisation of Software and Orchestration

Containers are not just resource-efficient alternatives to traditional virtual machines but also enhance security by isolating application processes. Containerisation Software (e.g., Docker<sup>7</sup>, LXC<sup>8</sup>, etc.) are cloud-native ecosystems that encapsulate applications in containerised environments, abstracting them from potential vulnerabilities of the underlying machinery. They are beneficial for the following reasons:

- **Scalability:** Containers facilitate rapid, secure scaling from testing to deployment, ensuring no compromised components scale along (aligns with Req. **TR1**).
- **Resilient:** The inherent resilience of containers ensures that potential breaches do not persist, as containers can self-recover, minimising exposure (aligns with Req. **CR8**).
- **Distributed:** Their distributed nature not only aids in resource management but also decentralises potential attack vectors, reducing single points of failure (aligns with Req. **TR2**).
- **Portability:** Enables the application to run on various locations, i.e., on-premises, in a public cloud, or in a private cloud. Its independence from the host OS minimises the exposure to potential vulnerabilities there (aligns with Req. **CR3**).

For future C-ITS, a container orchestration layer that emphasises security is crucial [73]. Container orchestration is used to manage the lifecycle of containers, especially in large, dynamic environments.

<sup>7</sup>Docker: Platform-as-a-service for OS-level virtualisation: <https://www.docker.com/>

<sup>8</sup>LXC: Userspace interface for Linux Kernels: <https://linuxcontainers.org/lxc/>

Container orchestration can be used to control and automate many tasks, such as:

- Provisioning and deployment of containers (Req. **CR3**).
- Redundancy and availability of containers (Req. **CR8**).
- Scaling up or removing containers to spread application load evenly across host infrastructure
- Moving and rescheduling containers from one host to another. This ensures high availability of the services even when one or many hosts are offline or malfunctioning (Req. **TR5**).
- External exposure of services running in a container with the outside world (Reqs. **CR3** and **TR6**).
- Load balancing and service discovery between containers. This can help find the available services within the virtual network (Req. **TR5**).
- Monitoring the health of the containerised applications and the host infrastructure (Req. **CR3**).

Such a flexible architecture can significantly benefit the massive growth of heterogeneous devices connected to such networks. The most popular tool for container orchestration currently is Kubernetes<sup>9</sup>. Kubernetes is an open-source production-grade container-orchestration system for automating application deployment, scaling, and management.

The benefits of container orchestration have been investigated in various Smart City and C-ITS deployments, e.g., in [74, 75]. These works show that benefits are related to these environments' delay-sensitive and data-intensive services. These requirements are crucial for such systems. Using computing resources closer to the end nodes (i.e., at the Edge or the Fog) can reduce overall end-to-end delay. Such an approach was followed in [76]. Authors in this work designed a network-aware scheduling approach for container-based applications in Smart City deployment. Their approach builds on Kubernetes, enhancing the default scheduling mechanism available.

#### 7.4. Serverless and Functions-as-a-Service

Serverless computing and Function-as-a-Service (FaaS) are emerging cloud architecture patterns that can provide significant cybersecurity benefits for CAVs and C-ITSs. The idea behind serverless is to “focus on the application, not the infrastructure”. In a serverless model, applications run in short-lived,

stateless containers triggered by specific events and fully managed by the cloud provider [77]. Resources are allocated dynamically and “on-demand”. This contrasts traditional servers and virtual machines that run continuously regardless of utilisation.

For intelligent transportation systems, a serverless approach reduces the attack surface in several key ways:

- Ephemeral function containers disappear after execution, minimising the “window of opportunity” for compromises (aligns with Req. **CR8**).
- Automated scaling removes resource management tasks vulnerable to misconfiguration (aligns with Req. **CR7**)
- Stateless functions have no data at rest to exploit (aligns with Reqs. **CR8** and **TR4**).
- Granular access controls can be applied per function (aligns with Req. **CR1**).

Additionally, FaaS capabilities allow transportation services to scale elastically on demand. This is critical for maintaining QoS during unexpected traffic spikes or DDoS attacks. While an initial request may take longer to be handled than an application hosting platform, caching may enable subsequent requests to be handled within milliseconds.

By leveraging serverless and FaaS, C-ITS, cybersecurity researchers and engineers can focus on developing discrete functions that can be scaled, updated, and secured independently. This flexible architecture aligns well with the dynamic nature of transportation systems. When combined with event-driven scaling, serverless allows C-ITSs to be resilient and adaptive to evolving demands and threats.

## 8. In-vivo Monitoring and Protection

The CTEF offers a comprehensive cybersecurity analysis for C-ITS components in isolated settings, but real-world C-ITS infrastructure protection is vital. CTEF is constructed to allow its tools to integrate seamlessly with real-world C-ITS systems. All the technologies described in Sec. 7 can facilitate this integration and swiftly adapt new cybersecurity measures and ML solutions, ensuring minimal transition time for actual C-ITS systems. Furthermore, adopting maturity models ensures the selection and integration of high-quality solutions, reducing the risk of potential damage from faulty software or hardware. Incorporating “Digital Twins” [46] further boosts the quality of solutions, ensuring the security, resilience, interoperability, and other fundamental requirements of a C-ITS. These tools also offer insights into the system’s capabilities and help mitigate potential risks

<sup>9</sup>Kubernetes: Production-grade container orchestration: <https://kubernetes.io/>



or adverse outcomes. The following sections describe how CTEF tools can be used in the real-world setup.

### 8.1. Maturing Cybersecurity Tools

In conjunction with its operation as a testing and evaluation facility, CTEF can also provide its services (testing environments and SecaaS platforms) for the development of cybersecurity incubators to perform research, development and maturity of new C-ITS cybersecurity tools and algorithms (aligns with Req. CR4). Starting with risk assessment frameworks (like ISO 27001 [60]), the risks identified can be mitigated, leading to mature, real-world-ready solutions.

The maturity readiness should be considered for the different tools and frameworks incubated. Well-known frameworks could be used for that like Capability Maturity Model Integration (CMMI)<sup>10</sup>, or the Cybersecurity Capability Maturity Model (C2M2)<sup>11</sup>. Internal frameworks could also be developed that better align with C-ITS organisations and systems. For example, authors in [78] describe a maturity model that can evaluate the performance of an organisation in a continuous and level-based way. The works [79, 80] provide a good foundation for existing (or the lack of) end-to-end cybersecurity maturity assessment frameworks and ways forward to extend this area.

Using virtualised cloud-based cybersecurity platforms and simulated C-ITS environments allows easier deployment of cybersecurity testbeds where new tools and techniques can be developed and tested. The new tools will be matured within CTEF's cybersecurity incubators to verify that they operate in accordance with the C-ITS operational requirements, as described in the in-situ testing and analysis of CTEF, before integrated into CTEF's main SecaaS platform.

### 8.2. Cybersecurity of the Real-world Infrastructure

Both the in-vitro and the in-situ testing and evaluation tools and services that compose the CTEF will follow a SaaS approach; thereby, they will provide the scalability and flexibility needed to be applied to larger systems such as a real-world C-ITS. Furthermore, since CTEF tools will operate with C-ITS's operational requirements in mind (e.g., protocols, data flows, delays, etc.), they can be easily integrated into the real world. The only difference between CTEF and the real world, apart from the size of the system, is the need for continuous monitoring and security evaluation in a

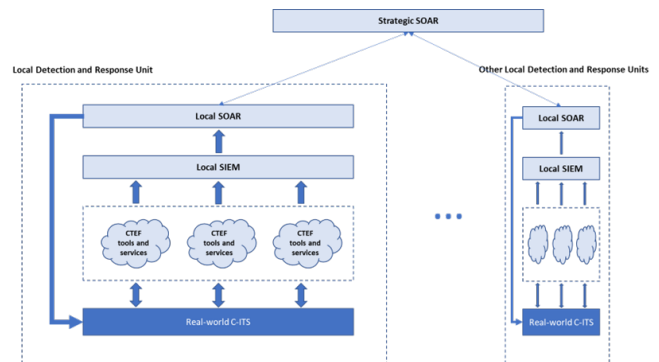


Figure 12. Cybersecurity of the real-world C-ITS infrastructure.

C-ITS environment due to the highly dynamic nature of the system and the ever-changing threat landscape (aligns with Reqs. CR5 and CR5).

For that purpose, localised Security Information and Event Management (SIEM) systems must be overlooking the real-world C-ITS, collaborating with localised CTEF-like implementations in a distributed manner. Each SIEM will inform a localised Security Orchestration, Automation and Response (SOAR) system responsible for triaging the data and responding to threats by taking remediation steps (aligns with Req. CR5 and CR7). To allow organisation-wide strategy-driven decision-making, a strategic SOAR will aggregate information from local SOARs for monitoring purposes and also inform the organisation's strategy back to the local SOAR. An example of such an approach can be found in [81], where a SOAR dynamically deploys behavioural honeypots to enhance network intrusion detection and security measures. The above approaches can ensure that tools and strategies are implemented under a comprehensive risk management strategy (as discussed in [82]).

Fig. 12 illustrates our view of the cyber protection of real-world C-ITSs. In conjunction with the proposed CTEF, they will deliver holistic and continuous cybersecurity to C-ITS in a distributed, cloud-based manner. This approach will enable the use of the CTEF testing and evaluation tools outside CTEF, extending their exploitability.

### 8.3. Digital Twins and Digital Network Oracles

Sec. 6.3 discussed the importance of reconfigurable C-ITS test environments, the importance of the data, and the logging/measuring capabilities that should be incorporated in CSCE. As it is evident, evaluating potential solutions in the real world could be very dangerous and raise privacy concerns. Therefore, the alternative solution is using "Digital Twins" [46]. The term describes a virtual simulation of the physical world and assets – whether it is a vehicle, the road

<sup>10</sup>Capability Maturity Model Integration (CMMI): <https://www.isaca.org/enterprise/performance-improvement-solutions>

<sup>11</sup>Capability Maturity Model (C2M2) <https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2>

infrastructure, or just a street of a major city (aligns with Req. CR2).

Through data and feedback from both simulations and the real world, a Digital Twin can develop autonomy, learn from and reason from its environment. A Digital Twin is a “*digital living simulation*” that brings all the data and models together, attempts to replicate salient features of the real world, and updates itself from multiple sources to represent its physical counterpart. There are already various attempts in the literature to capture different aspects of a C-ITS, such as [46] that describes a reference information sharing model, [83] that presents a lightweight traffic situation awareness Digital Twins, etc.

Recently, the concept of “Digital Network Oracles”, i.e., an augmented “Digital Twin”, was introduced [84]. The added capability refers to a particular architecture, which allows for the Digital Twin to be queried sequentially, to which it responds with the state of the “virtual world”. With such capabilities, the Digital Twin can train iterative learning (e.g., Reinforcement learning) controllers for inferential and prediction tasks.

A Digital Network Oracle is a virtual representation of physical assets in Cyber-Physical Production Systems (CPPSs) and can comprise several Digital Twins. If a Digital Twin is equipped with the following four characteristics: synchronisation with the physical assets, active data acquisition, the ability to simulate, and sequential bidirectional interaction with intelligent agents, the definition of this replica is transformed into a Digital Network Oracle. An oracle deployed in CSCE should have the following features:

- Automated detection of changes in scenarios in the real world and dealing with missing information in the digital domain.
- Automated detection of interdisciplinary dependencies and consistency checking of mechanics, electrics and software domain changes.
- Automated adaptation and changes in the models of the Digital Twin.

Moreover, an important feature required is the cross-domain (or cross-asset) synchronisation. Systems or sub-systems simulated in a Digital Twin do not adhere to the same simulation steps and are rather challenging to synchronise. Some existing synchronisation approaches have been demonstrated recently in different fields. For example, the cross-domain relationships of different assets were evaluated using semantic technologies [85] or using lifecycle management systems [86] to edit the existing sub-models within a Digital Twin. To the best of our knowledge, these ways are partially or not

automated and cannot be easily applied to the dynamic environments of a C-ITS.

Lastly, regarding active data acquisition, such a system should require:

- Acquisition of operational data from physical assets and processing and analysing the data.
- Provide various assistance functions, such as diagnosis and predictive quality.
- The ability to sample process data in a highly accurate manner and to assign it to the corresponding Digital Twin.
- Data unification or data curation.

Software modules and decentralised systems could be employed for such an approach. Furthermore, standardised connector interfaces ensure that shared data are being generated in the field, and standardised collectors (i.e., software modules) can collect the data in the Cloud or the Edge. Two aspects of a Digital Network Oracle, i.e., the ability to simulate and the bidirectional interaction with intelligent agents (e.g., in a Reinforcement Learning context), are also paramount. Examples of that can be found in [84, 87].

Digital Twins are expected to lead the experimentation on digital infrastructures in the near future. However, the complexity introduced when designing and developing such systems is tremendous. Especially when connecting different Digital Twins to create national Digital Twins able to emulate extensive complex scenarios, standard good practices should be followed between the different tools.

## 9. Challenges and Vulnerabilities

The emerging technologies discussed in earlier sections undeniably enhance the capabilities of C-ITSs and contribute to a more comprehensive cybersecurity approach. Yet, introducing nascent technologies often brings new challenges and potential vulnerabilities. These issues need addressing before full integration into any system. Transitioning from controlled environments, like the CTEF, to real-world applications presents its own set of challenges. This section delves into the challenges and solutions associated with the technologies above, standardisation efforts, and the vulnerabilities that might arise when applied in real-world scenarios.

### 9.1. Wireless Communication Plane Challenges

Sec. 2.3 touched upon the communication domains within a C-ITS, and Sec. 2.5 discussed the architecture of its future wireless plane. The wireless standards mentioned are grounded in the renowned OSI model. The ETSI TS 102 940 standard [88] delineates security

requirements on a per-layer basis (Fig. 13). This suggests the implementation of multiple security measures to safeguard a system. Additionally, the ETSI TS 102 942 [89] standard offers a structure for access control in C-ITS, encompassing authentication, authorisation, and cryptographic certificate issuance.

Threat analysis is mandated for all V2X communications. Such analyses have been proposed in past works such as [90]. Broadly, the attack surfaces correspond with the communication domains described in Sec. 2.3. Each domain has its unique characteristics and requirements, leading to unique vulnerabilities. Exploiting these vulnerabilities can lead to the attacks presented in Tab. 4. Existing literature presents standards that address the security of specific technologies and protocol stacks (e.g., ETSI TS 133 501 [91] and 3GPP 33.501 [92] deal with the 3GPP 5G system security), while others (e.g., ETSI TS 102 940 [88], ETSI TS 102 942 [89]), deal more with the communication domains within a C-ITS. To encapsulate the challenges:

- Varied authentication and authorisation levels are essential for C-ITS stations to access networks and services.
- Point-to-point communications require confidentiality. Broadcast messages do not have specific requirements.
- Privacy measures, like pseudonym changes, for preventing tracking of C-ITS stations.
- Access control involving initialisation, enrolment and authorisation credentials ensures only trusted stations in the network.
- Trust and enrolment guidelines emphasise secure storage of keys and cryptographic operations.
- Security services, such as integrity and replay protection, are layered using defined access points.
- A Public Key Infrastructure (PKI) architecture must manage credentials, certificate trust lists, and a Misbehavior Authority for detecting and revoking misbehaving devices.

More details about the standards related to the wireless communication planes and the in-vehicle communication domains can be found in [44, 45].

## 9.2. Open-source Software Challenges

While the prevailing opinion is that well-maintained open-source solutions are typically more secure, their open nature implies that vulnerabilities are also accessible by malicious actors. If not updated regularly, these vulnerabilities can be exploited. Authors in [93]

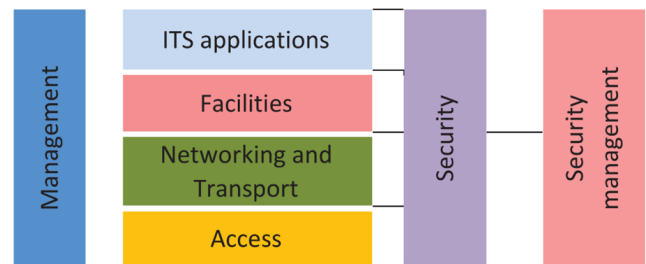


Figure 13. C-ITS security layers architecture [88].

provide an overview of the software product quality problems, security issues and certain challenges confronting the Open-Source Software (OSS). The challenges associated OSS include:

- **Public Exposure of Vulnerabilities:** Issues and vulnerabilities are often publicly listed on databases like the National Vulnerability Database<sup>12</sup>. Organisations that do not address these promptly can become targets of malicious actions.
- **Intellectual Property Risks:** Open-source components might inadvertently infringe on intellectual property rights due to the lack of standard commercial controls.
- **Operational Inefficiencies:** Organisations might struggle to track and update open-source components, leading to potential risks.
- **Developer Malpractices:** Open-source components might become outdated or might not undergo rigorous testing. Poor coding habits can result in defective code that is hard to update or monitor.

To mitigate these challenges, organisations should adopt to Software Assurance Maturity Models (SAMMs) as outlined in existing literature [94] or in publicly available open frameworks (e.g., OWASP SAMM [95]). These tools evaluate and improve software security practices, building balanced software security assurance and demonstrating security assurance improvements through an iterative process.

When deploying OSS, it is crucial to exercise extra caution. The unique nature of OSS demands specialised solutions to identify vulnerabilities, like Software Composition Analysis (SCA) tools (or vulnerability scanners as otherwise known). Moreover, adhering to best practices related to software inventories, licensing, and continuous threat monitoring is vital throughout the SDLC and software lifecycle [96]. As discussed, software vulnerability detection can leverage traditional SCA tools or employ advanced technologies,

<sup>12</sup>NIST: National Vulnerability Database <https://nvd.nist.gov/>

including ML algorithms, for both source [57] and binary [58] code analysis. Just like with proprietary software, security responsibility should not rest solely with the vendor, allowing for transparent security patch resolutions.

### 9.3. Security and Authorisation Challenges

Security and authorisation in C-ITS primarily focus on ensuring the safe and reliable exchange of information among interconnected vehicles and infrastructure. This must be achieved while preserving the privacy and trustworthiness of the participating entities. As technology rapidly evolves and networked systems grow in scale, these challenges grow in complexity. We can categorise these challenges as follows:

- **Regulation and Policy Adaptation:** Crafting detailed security policies specifically for C-ITSs and addressing any shortcomings or gaps in current standards.
- **Identity Management and Privacy:** Handling the complex dynamics of digital certificates, from their issuance to revocation, and verifying the identity of devices and components within a C-ITS.
- **Resource Constraints and Scalability:** Ensuring processes, such as certificate revocation, remain efficient and prompt, even as the system expands.
- **Decentralisation and Dynamic Trust Evaluation:** Shifting towards decentralised infrastructure solutions and dynamically adjusting participant trust levels to maintain consistent system integrity.

The European Commission has tasked the C-ITS Platform with defining a security policy [97] to bolster the security of C-ITS. This policy governs the use of certificates, especially concerning short-range communications between vehicles, pedestrians, and the infrastructure network. ETSI standards already outlined a mechanism for disseminating and revoking certificates [89, 98]. Existing standard limitations have been the subject of various research endeavours. For instance, the study in [99] describes a novel architecture and a new trust model for a root Certification Authority (CA). In C-ITS, CA is an entity that issues digital certificates and can be an integral part of the infrastructure network. Moreover, the CA is responsible for revoking certificates associated with compromised or misbehaving entities. The study in [99] combines certifications, web tokens, and transport layer security to guard against eavesdropping, malicious alterations, and MitM attacks. Proposing a PKI supported by short-living tokens that are never reused minimises the impact of stolen tokens.

Similarly, vehicle identities can be substituted with multiple abstract short-lived identifiers, i.e.,

pseudonyms. The study in [100] explores this concept. The CA issues these pseudonym credentials and verifies a vehicle's eligibility to share data by retaining its ID. This ensures location privacy since consecutive messages are signed using different pseudonyms. However, this approach demands more computational resources, potentially affecting system scalability and the efficiency of the revocation process. The Pseudonymous PKI (PPKI) method was examined in a smart grid context [101], revealing that a single revocation scheme might not meet the overhead and security requirements of all smart grid applications.

Considering the decentralised infrastructure solutions proposed for future C-ITSs, efficient decentralised PKI solutions are recommended. For example, authors in [102] describe a learning game involving vehicles that utilise certificates distributed amongst themselves. These certificates can be revoked if a trust value drops below a set threshold. The environment rewards or penalises vehicles based on their actions in the game.

### 9.4. Virtualisation & Container Orchestration Challenges

Virtualisation technologies, such as 5G O-RAN, enable mapping virtual machines (VMs) and containers to physical resources. This facilitates designing and deploying novel SecaaS algorithms and features for future C-ITS [103]. However, this new architecture poses security concerns, especially when users lose physical control over their computation and data. The primary attack vectors include:

- **Architectural attacks:** These exploit the abstraction layer between physical hardware and virtualised systems. For instance, VMs on the same network can be vulnerable to simultaneous attacks, simplifying unauthorised access.
- **Hypervisor-based attacks:** These target hypervisor or container orchestration software vulnerabilities, leading to issues like resource exhaustion or VM sprawl.
- **(Mis)configurations:** Cloning or copying images in a virtual environment can inadvertently deploy unwanted infrastructure components. This can introduce configuration drifts, making managing and securing the environment harder.

Mitigating these risks for VM hypervisors involves implementing policies for VM lifecycle management, controlling VM image creation and use, and ensuring quick recovery to a secure (initial/clean) state [104]. The security of the hypervisor is crucial, and managing rapidly deployed environments is vital. Similar principles apply to containers and their orchestrators.



For 5G-enabled computing solutions, such as O-RAN, the confidentiality of 5G services remains intact due to the distinction between RAN and core services. As described in [105], the data exchanged between containers undergo encryption and decryption at each function. This is also highlighted in security standards by 3GPP [92, 106]. The introduction of 5G O-RAN overcomes previous hardware and vendor lock-in concerns, promoting a more open hardware future. The standardisation of O-RAN also addresses risks related to poorly managed open-source solutions (as introduced in Sec. 9.2).

However, while O-RAN and cloud-native implementations offer significant benefits (Sec. 7.2), the added abstraction layers necessitate enhanced security. Ensuring secure interoperability in a complex multi-vendor environment is essential. Configuration errors can expose mission-critical resources and application traffic. Moreover, API management and security become paramount [107]. Both the host systems and applications within containers must be safeguarded from threats like privilege escalation attacks [108]. Finally, applications inside the containers should also be protected from external risks (e.g., ransomware gaining access to a container) [105].

### 9.5. Vulnerabilities in Serverless Architectures

In serverless architectures, providers like AWS Lambda or Google Cloud Functions typically handle the security of all cloud components. However, this does not exempt developers from all responsibilities. Key implications of adopting serverless architectures include:

- **Data Leakage:** Serverless functions are stateless, leading to sensitive data being stored externally and increasing leakage risks during data transfers.
- **Multi-tenancy:** Without dedicated servers for each service or user, functions run on shared resources. Misconfigurations can expose sensitive data or compromise system security.
- **Increased Attack Surface and Complexity:** Fragmenting applications into multiple serverless functions can expand potential attack vectors. Additionally, the ephemeral nature of these functions limits the time developers have to identify and address issues, complicating malicious event-data injection countermeasures.
- **Third-party Dependencies:** Relying on third-party software (open source, libraries, packages, etc.) in serverless development can be challenging to manage and increase the risk of inadequate security testing.

The inherent multi-tenancy of serverless computing introduces unique security threats. Features like

pay-as-you-go and automatic scalability, while advantageous, can be exploited in DoS attacks, leading to unexpected costs for application owners [109]. Many challenges in serverless computing mirror those in virtualised and containerised applications. The study in [109] categorises serverless computing's security challenges into four domains: 1) resource isolation, 2) security monitoring, 3) security control, and 4) data protection. The authors also provide a detailed analysis of the risks in each domain and suggest potential mitigation strategies.

In conclusion, serverless architectures promise cost savings, scalability, and administrative ease, but they also introduce new security challenges. To safeguard serverless applications, continuous monitoring and automated security tools are paramount. Best practices include refining function permissions, enhancing logging and monitoring mechanisms, and ensuring robust data encryption.

### 9.6. Challenges with the Real-world Integration

The technologies discussed in Sec. 7 aim to seamlessly integrate with real-world C-ITS. By introducing abstraction, virtualisation, and containerisation, we can separate cybersecurity applications and C-ITS services from hardware dependencies. This framework facilitates the scaling of envisioned solutions, ensuring that real-world C-ITS can swiftly adopt new cybersecurity frameworks and ML-based solutions. Such an approach guarantees production-grade operation within the CSCE.

Furthermore, the maturity model introduced in Secs. 8.1 and 8.2 ensures that solutions, when deployed in the real world, are of high quality, thus minimising potential catastrophic impacts from flawed software or hardware. In essence, a maturity model gauges the progress in embedding security into daily operations and the strategic undertakings of C-ITS. The Digital Twins and Digital Network Oracles introduced in Sec. 8.3 further bolsters the solutions the CSCE provides. They help establish key requirements of a C-ITS, such as security, resilience, and interoperability.

However, despite the advantages of these technologies and strategies, several challenges arise in real-world integration:

**Privacy.** C-ITS applications often process user identification data (e.g., usernames, registration plates, etc.), which must be protected against unauthorised access and comply with local privacy regulations (such as GDPR). Even applications that do not process personal information can inadvertently de-anonymise users when data is correlated with other datasets. The challenge lies in ensuring that cybersecurity tools designed for or within CTEF, consider data privacy when applied to real-world scenarios. Authors in [110]

identify this as an issue in the EU Regulation on the Free Flow of Non-personal Data [111]. Data anonymity is a major issue that has to be investigated in the context of C-ITS. Within the proposed CSCE, the challenge lies in ensuring that cybersecurity tools designed for or within CTEF, an isolated C-ITS environment, consider data privacy when applied to real-world scenarios.

**Operation.** C-ITS environments, with their diverse hardware, software, and network platforms, have strict operational requirements. As noted in [112], many C-ITS services (e.g., a crash avoidance system) rely on communications with very low latency and other QoS characteristics. Traditional cybersecurity approaches may not be suitable due to the unique nature of C-ITS. This highlights the need to develop new cybersecurity tools tailored to C-ITS. CTEF can play a pivotal role in the research and development efforts required, providing space for incubating novel activities and testing existing ones for their applicability in a C-ITS.

**Resilience of a Real-world System.** The fusion of legacy and modern technologies in industrial control and enterprise IT, combined with emerging technologies within CAV platforms, leads to a new era of resilience challenges. The CSCE plays a pivotal role in navigating these challenges, leveraging metrics like the Mean Time Between Failure and standards such as Safety Integrity Levels (SIL) [113] and IEC 62061 [114].

The evolving landscape of cyber threats demands a dynamic approach to resilience, especially in cybersecurity. Established standards, from STIX [115], provide a foundation for understanding threats, sharing intelligence and countering them. Cybersecurity models such as MITRE's ATT&CK framework [116] can help evaluate resilience concerning Threat Actors / Actor groups and their use of exploits/intrusion sets. The even-evolving data and the CAV's platform robustness against attacks can be described in terms of Tools, Techniques and Procedures (TTPs). Adopting new technologies like ML introduces complexities, necessitating a more granular, component-level assessment of resilience.

In this interconnected age, a holistic approach to resilience is paramount. This encompasses the: 1) integration of old but stable and new but unpredictable technical solutions, 2) continuous evaluation of the resilience as the systems and threats evolve, 3) proactive strategies, aiming to defend and anticipate, adapt, and evolve in the face of emerging challenges, 4) stakeholder collaboration including technology providers, regulatory bodies, and end-users, and 5) training and awareness ensuring that those involved in the design, deployment, and operation of C-ITS platforms are well-trained and aware of the latest threats and best practices.

Building resilience in real-world systems, especially as complex as C-ITSs, is challenging but essential. It requires combining technical solutions, continuous evaluation, stakeholder collaboration, and human-centric approaches. As the world becomes more connected and technology continues to evolve, the importance of resilience will only grow.

## 10. Conclusion

The ongoing digital transformation of transportation systems unveils a plethora of opportunities and challenges. At the centre of these challenges lies cybersecurity, which has become not only a technical priority but also a societal obligation. The CSCE and CTEF frameworks outlined in this paper offer a structured approach to address these cybersecurity challenges, always with an eye on the seamless integration of emerging technologies into real-world scenarios. Our work underscored the importance of robust testing mechanisms and facilities, detailing the key technologies for providing the required functionality. We portrayed our envisaged requirements across the in-situ, in-vitro, and in-vivo domains of a prospective C-ITS. Additionally, we delved into the inherent challenges within each domain, offering insights on the adopted technologies or suggestions for future research pathways. A multi-layered security strategy is essential to counteract the diverse array of attack vectors. Integrating ML-powered intelligent agents can strengthen detection capabilities, offering a proactive attitude towards threat identification and mitigation. As the transportation sector gravitates towards real-world C-ITS deployments, continuous monitoring becomes paramount. Safeguarding CAV services is vital and guarantees their peak performance and continuous operation. Moving forward, the focus should remain on enhancing cybersecurity, fine-tuning detection methodologies, and broadening the spectrum of real-world testing scenarios.

**Acknowledgement.** This work was supported in part by Toshiba Europe Ltd. and in part by the CAVShield project (grant no. 133898, UK Research and Innovation, Innovate UK).

## References

- [1] D'OREY, P.M. and FERREIRA, M. (2014) ITS for Sustainable Mobility: A Survey on Applications and Impact Assessment Tools. *IEEE Trans. Intell. Transp. Syst.* 15(2): 477–493. doi:10.1109/TITS.2013.2287257.
- [2] BARRETO, L., AMARAL, A. and BALTAZAR, S. (2018) Urban Mobility Digitalization: Towards Mobility as a Service (MaaS). In *Proc. of Int. Conf. Int. Sys.*: 850–855. doi:10.1109/IS.2018.8710457.
- [3] MAVROMATIS, I., TASSI, A., RIGAZZI, G., PIECHOCKI, R.J. and NIX, A. (2018) Multi-Radio 5G Architecture for

- Connected and Autonomous Vehicles: Application and Design Insights. *EAI Endorsed Trans. Ind. Netw. Intell. Syst.* 4(13). doi:10.4108/eai.20-3-2018.154368.
- [4] PARKINSON, S., WARD, P., WILSON, K. and MILLER, J. (2017) Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. *IEEE Trans. Intell. Transp. Syst.* 18(11): 2898–2915. doi:10.1109/TITS.2017.2665968.
- [5] AMANULLAH, M.A., LOKE, S.W., BARUWAL CHHETRI, M. and DOSS, R. (2023) A Taxonomy and Analysis of Misbehaviour Detection in Cooperative Intelligent Transport Systems: A Systematic Review. *ACM Comput. Surv.* 56(1): 38. doi:10.1145/3596598.
- [6] PANDEY, M. and SEETHARAMAN (2022) A Review of Factors Impacting Cybersecurity in Connected and Autonomous Vehicles (CAVs). In *Proc. of CoDIT*, 1: 1218–1224. doi:10.1109/CoDIT55151.2022.9804071.
- [7] SEDAR, R., KALALAS, C., VÁZQUEZ-GALLEGO, F., ALONSO, L. and ALONSO-ZARATE, J. (2023) A Comprehensive Survey of V2X Cybersecurity Mechanisms and Future Research Paths. *IEEE Open J. Commun. Soc.* 4: 325–391. doi:10.1109/OJCOMS.2023.3239115.
- [8] TALEBKHAH, M., SALI, A., GORDAN, M., HASHIM, S.J. and ROKHANI, F.Z. (2023) Comprehensive Review on Development of Smart Cities Using Industry 4.0 Technologies. *IEEE Access* 11: 91981–92030. doi:10.1109/ACCESS.2023.3302262.
- [9] TASSI, A., MAVROMATIS, I., PIECHOCKI, R., NIX, A., COMPTON, C., POOLE, T. and SCHUSTER, W. (2019) Agile Data Offloading over Novel Fog Computing Infrastructure for CAVs. In *Proc. of IEEE VTC2019-Spring*: 1–6. doi:10.1109/VTCSpring.2019.8746302.
- [10] WEN, L., RICKERT, M., PAN, F., LIN, J. and KNOLL, A. (2023) Bare-Metal vs. Hypervisors and Containers: Performance Evaluation of Virtualization Technologies for Software-Defined Vehicles. In *Proc. of IEEE IV*: 1–8. doi:10.1109/IV55152.2023.10186789.
- [11] KEMP, G., VARGAS-SOLAR, G., DA SILVA, C.F., GHODOUS, P., COLLET, C. and AMAYA, P.L. (2015) Towards Cloud Big Data Services for Intelligent Transport. In *Proc. of ISPE ICCE*, 2: 377 – 385. doi:10.3233/978-1-61499-544-9-377.
- [12] (2021) *Road Vehicles — Cybersecurity Engineering*. Standard, International Organization for Standardization.
- [13] ROBERTS, A., MAENNEL, O. and SNETKOV, N. (2021) Cybersecurity Test Range for Autonomous Vehicle Shuttles. In *Proc. of IEEE EuroS&PW*: 239–248. doi:10.1109/EuroSPW54576.2021.00031.
- [14] MAPLE, C., BRADBURY, M., LE, A.T. and GHIRARDELLO, K. (2019) A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis. *Applied Sciences* 9(23). doi:10.3390/app9235101.
- [15] DOMINIC, D., CHHAWRI, S., EUSTICE, R.M., MA, D. and WEIMERSKIRCH, A. (2016) Risk Assessment for Cooperative Automated Driving. In *Proc. of ACM Workshop on CPS-SPC* (Association for Computing Machinery): 47–58. doi:10.1145/2994487.2994499.
- [16] (2023) *Architecture Reference for Cooperative and Intelligent Transportation*. Tech. report, United States Department of Transport.
- [17] GUPTA, S., MAPLE, C. and PASSERONE, R. (2023) An Investigation of Cyber-Attacks and Security Mechanisms for Connected and Autonomous Vehicles. *IEEE Access* 11: 90641–90669. doi:10.1109/ACCESS.2023.3307473.
- [18] FANG, Y., SHAN, Z. and WANG, W. (2021) Modeling and Key Technologies of a Data-Driven Smart City System. *IEEE Access* 9: 91244–91258. doi:10.1109/ACCESS.2021.3091716.
- [19] AL-SULTAN, S., AL-DOORI, M.M., AL-BAYATTI, A.H. and ZEDAN, H. (2014) A Comprehensive Survey on Vehicular Ad Hoc Network. *J. Netw. Comput. Appl.* : 380–392doi:10.1016/j.jnca.2013.02.036.
- [20] GONZÁLEZ, D., PÉREZ, J., MILANÉS, V. and NASHASHIBI, F. (2016) A Review of Motion Planning Techniques for Automated Vehicles. *IEEE Trans. Intell. Transp. Syst.* 17(4): 1135–1145. doi:10.1109/TITS.2015.2498841.
- [21] MALIK, R.Q., RAMLI, K.N., KAREEM, Z.H., HABELALMATEE, M.I., ABBAS, A.H. and ALAMOODY, A. (2020) An Overview on V2P Communication System: Architecture and Application. In *Proc. of IICETA*: 174–178. doi:10.1109/IICETA50496.2020.9318863.
- [22] (2018) *Intelligent transport systems — Cooperative ITS — Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s)*. Standard, International Organization for Standardization.
- [23] MAVROMATIS, I., SANCHEZ-MOMPO, A., RAIMONDO, F., POPE, J., BULLO, M., WEEKS, I., KUMAR, V. et al. (2023) LE3D: A Lightweight Ensemble Framework of Data Drift Detectors for Resource-Constrained Devices. In *Proc. of IEEE CCNC*: 611–619. doi:10.1109/CCNC51644.2023.10060415.
- [24] MAVROMATIS, I. and KHAN, A. (2023) Demo: LE3D: A Privacy-preserving Lightweight Data Drift Detection Framework. In *Proc. of IEEE CCNC*. doi:10.1109/CCNC51644.2023.10060554.
- [25] KUPPA, A. and LE-KHAC, N.A. (2022) Learn to Adapt: Robust Drift Detection in Security Domain. *Comput. Electr. Eng.* 102. doi:10.1016/j.compeleceng.2022.108239.
- [26] HUQ, N., VOSSELER, R. and SWIMMER, M. (2018) *Cyberattacks against Intelligent Transportation Systems: Assessing Future Threats to ITS*. Tech. rep. URL [https://documents.trendmicro.com/assets/white\\_papers/wp-cyberattacks-against-intelligent-transportation-system.pdf](https://documents.trendmicro.com/assets/white_papers/wp-cyberattacks-against-intelligent-transportation-system.pdf).
- [27] HUQ, N., VOSSELER, R. and SWIMMER, M. (2018) *Cyberattacks against Intelligent Transportation Systems: Assessing Future Threats to ITS*. Tech. report, TrendLabs.
- [28] SAKIZ, F. and SEN, S. (2017) A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV. *Ad Hoc Networks* 61: 33–50. doi:https://doi.org/10.1016/j.adhoc.2017.03.006.
- [29] MILLER, C. (2019) Lessons Learned from Hacking a Car. *IEEE Design & Test* 36(6): 7–9. doi:10.1109/MDAT.2018.2863106.
- [30] ZHAO, C., GILL, J.S., PISU, P. and COMERT, G. (2022) Detection of False Data Injection Attack in Connected and Automated Vehicles via Cloud-Based Sandboxing.



- IEEE Trans. Intell. Transp. Syst.* 23(7): 9078–9088. doi:10.1109/TITS.2021.3090361.
- [31] DASGUPTA, S., RAHMAN, M., ISLAM, M. and CHOWDHURY, M. (2022) A Sensor Fusion-Based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles. *IEEE Trans. Intell. Transp. Syst.* 23(12): 23559–23572. doi:10.1109/TITS.2022.3197817.
- [32] GHOSAL, A., HALDER, S. and CONTI, M. (2020) STRIDE: Scalable and Secure Over-The-Air Software Update Scheme for Autonomous Vehicles. In *Proc. of IEEE ICC*: 1–6. doi:10.1109/ICC40277.2020.9148649.
- [33] ABHISHEK, N.V., AMAN, M.N., LIM, T.J. and SIKDAR, B. (2022) DRiVe: Detecting Malicious Roadside Units in the Internet of Vehicles With Low Latency Data Integrity. *IEEE Internet Things J.* 9(5): 3270–3281. doi:10.1109/JIOT.2021.3097809.
- [34] (2017) *Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT)*. Tech. rep., U.S. Department of Transportation.
- [35] JOLFAEI, A. and KANT, K. (2019) Privacy and Security of Connected Vehicles in Intelligent Transportation System. In *Proc. of IEEE/IFIP DSN-S*: 9–10. doi:10.1109/DSN-S.2019.00010.
- [36] BECKMANN, H., KROPP, V. and EISSFELLER, B. (2014) New Integrity Concept for Intelligent Transportation Systems (ITS) for Safety of Live (SoL) Applications. In *Proc. of IEEE/ION PLANS*: 982–988. doi:10.1109/PLANS.2014.6851463.
- [37] LI, W., XIAO-NING, Z. and ZHENG-YU, X. (2010) Research on Traffic Information Demand and Supply Analysis of Comprehensive Traffic Information Platform. In *Proc. of Third International Symposium on Information Processing*: 384–388. doi:10.1109/ISIP.2010.64.
- [38] (2018) *ETSI TS 102 941: Trust and Privacy Management*. Standard, European Standards Organization (ESO).
- [39] MAALLOUL, S., ANISS, H., KASSAB, M. and BERBINEAU, M. (2021) Classification of C-ITS Services in Vehicular Environments. *IEEE Access* 9: 117868–117879. doi:10.1109/ACCESS.2021.3105815.
- [40] BALDINI, G. (2018) *Testing and Certification of Automated Vehicles (AV) Including Cybersecurity and Artificial Intelligence Aspects*. Tech. report, Joint Research Centre (JRC).
- [41] BECK, F., LAHMADI, A. and FRANÇOIS, J. (2021) HSL: a Cyber Security Research Facility for Sensitive Data Experiments. In *Proc. of IFIP/IEEE Int. Symp. on IM*: 956–961.
- [42] KOSE, Y., OZER, M., BASTUG, M., VARLIOGLU, S., BASIBUYUK, O. and PONNAKANTI, H.P. (2021) Developing Cybersecurity Workforce: Introducing CyberSec Labs for Industry Standard Cybersecurity Training. In *Proc. of CSCI*: 716–721. doi:10.1109/CSCI54926.2021.00184.
- [43] SCHOITSCH, E. and SCHMITTNER, C. (2020) Ongoing Cybersecurity and Safety Standardization Activities Related to Highly Automated/Autonomous Vehicles. In ZACHÄUS, C. and MEYER, G. [eds.] *Proc. of AMAA*: 72–86.
- [44] RATHORE, R.S., HEWAGE, C., KAIWARTYA, O. and LLORET, J. (2022) In-Vehicle Communication Cyber Security: Challenges and Solutions. *Sensors* 22(17). doi:10.3390/s22176679.
- [45] IVANOV, I., MAPLE, C., WATSON, T. and LEE, S. (2018) Cyber security standards and issues in V2X communications for Internet of Vehicles. In *Proc. of Living in the Internet of Things: Cybersecurity of the IoT*: 1–6. doi:10.1049/cp.2018.0046.
- [46] THONHOFFER, E., SIGL, S., FISCHER, M., HEUER, F., KUHN, A., ERHART, J., HARRER, M. et al. (2023) Infrastructure-Based Digital Twins for Cooperative, Connected, Automated Driving and Smart Road Services. *IEEE Trans. Intell. Transp. Syst.* 4: 311–324. doi:10.1109/OJITS.2023.3266800.
- [47] POLESE, M., BONATI, L., D'ORO, S., BASAGNI, S. and MELODIA, T. (2023) Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges. *IEEE Commun. Surveys Tuts.* 25(2): 1376–1411. doi:10.1109/COMST.2023.3239220.
- [48] GANNON, D., BARGA, R. and SUNDARESAN, N. (2017) Cloud-Native Applications. *IEEE Cloud Computing* 4(5): 16–21. doi:10.1109/MCC.2017.4250939.
- [49] NAKATA, R. and OTSUKA, A. (2021) CyExec\*: A High-Performance Container-Based Cyber Range With Scenario Randomization. *IEEE Access* 9: 109095–109114. doi:10.1109/ACCESS.2021.3101245.
- [50] SIKORSKI, M. and HONIG, A. (2012) *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software* (No Starch Press). doi:10.5555/2181153.
- [51] ASLAN, O.A. and SAMET, R. (2020) A Comprehensive Review on Malware Detection Approaches. *IEEE Access* 8: 6249–6271. doi:10.1109/ACCESS.2019.2963724.
- [52] SETHI, K., KUMAR, R., SETHI, L., BERA, P. and PATRA, P.K. (2019) A Novel Machine Learning Based Malware Detection and Classification Framework. In *Proc. of Int. Conf. Cyber Secur*: 1–4. doi:10.1109/CyberSecPODS.2019.8885196.
- [53] GRIFFIN, K., SCHNEIDER, S., HU, X. and CHIUH, T.C. (2009) Automatic Generation of String Signatures for Malware Detection. In *Proc. of RAID* (Springer Berlin Heidelberg): 101–120. doi:10.1007/978-3-642-04342-0\_6.
- [54] VINAYAKUMAR, R., ALAZAB, M., SOMAN, K.P., POORNACHANDRAN, P. and VENKATRAMAN, S. (2019) Robust Intelligent Malware Detection Using Deep Learning. *IEEE Access* 7: 46717–46738. doi:10.1109/ACCESS.2019.2906934.
- [55] TAVALLAEI, M., BAGHERI, E., LU, W. and GHORBANI, A.A. (2009) A Detailed Analysis of the KDD CUP 99 data set. In *Proc. of IEEE Symposium on CISDA*: 1–6. doi:10.1109/CISDA.2009.5356528.
- [56] ANDERSON, H.S. and ROTH, P. (2018) EMBER: An Open Dataset for Training Static PE Malware Machine Learning Models. *arXiv*.
- [57] AKTER, M.S., SHAHRIAR, H. and BHUIYA, Z.A. (2023) Automated Vulnerability Detection in Source Code Using Quantum Natural Language Processing. In WANG, G., CHOO, K.K.R., WU, J. and DAMIANI, E. [eds.] *Proc. of Ubiquitous Security* (Springer Nature Singapore): 83–102. doi:10.1007/978-981-99-0272-9\_6.
- [58] SCHAAD, A. and BINDER, D. (2023) Deep-Learning-Based Vulnerability Detection in Binary Executables. In JOURDAN, G.V., MOUNIER,



- L., ADAMS, C., SÈDES, F. and GARCIA-ALFARO, J. [eds.] *Proc. of Foundations and Practice of Security* (Springer Nature Switzerland): 453–460. doi:10.1007/978-3-031-30122-3\_28.
- [59] ZIZZO, G., HANKIN, C., MAFFEIS, S. and JONES, K. (2019) Adversarial Machine Learning Beyond the Image Domain. In *Proc. of DAC 2019* (Association for Computing Machinery). doi:10.1145/3316781.3323470.
- [60] (2022) *Information Security Management Systems*. Standard, International Organization for Standardization.
- [61] GREEN, B., LEE, A., ANTROBUS, R., ROEDIG, U., HUTCHISON, D. and RASHID, A. (2017) Pains, Gains and PLCs: Ten Lessons from Building an Industrial Control Systems Testbed for Security Research. In *Proc. of CSET*.
- [62] SOMMER, C., GERMAN, R. and DRESSLER, F. (2011) Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis. *IEEE Trans. Mob. Comput.* **10**(1): 3–15. doi:10.1109/TMC.2010.133.
- [63] LOPEZ, P.A., BEHRISCH, M., BIEKER-WALZ, L., ERDMANN, J., FLÖTTERÖD, Y.P., HILBRICH, R., LÜCKEN, L. *et al.* (2018) Microscopic traffic simulation using sumo. In *Proc. of ITSC*: 2575–2582. doi:10.1109/ITSC.2018.8569938.
- [64] (2019) *Cybersecurity and Intelligent Transportation Systems: A Best Practice Guide*. Tech. rep., U.S. Department of Transportation. URL <https://rosap.ntl.bts.gov/view/dot/42461>.
- [65] (2010) *Open Source Security Testing Methodology Manual (OSSTMM)*. Tech. rep., Institute for Security and Open Methodologies (ISECOM). URL <https://www.isecom.org/OSSTMM.3.pdf>.
- [66] STRAUB, J. (2020) Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATT'I&'CK and STRIDE Frameworks as Blackboard Architecture Networks. In *Proc. of IEEE SmartCloud*: 148–153. doi:10.1109/SmartCloud49737.2020.00035.
- [67] SAKIZ, F. and SEN, S. (2017) A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems. *Ad Hoc Netw.* **61**: 33–50. doi:10.1016/j.adhoc.2017.03.006.
- [68] NICKERSON, C., KENNEDY, D., SMITH, E., RABIE, A., FRIEDLI, S., SEARLE, J., KNIGHT, B. *et al.* (2014) *Penetration Testing Execution Standard*. Standard.
- [69] BLINOWSKI, G., OJDOWSKA, A. and PRZYBYŁEK, A. (2022) Monolithic vs. Microservice Architecture: A Performance and Scalability Evaluation. *IEEE Access* **10**: 20357–20374. doi:10.1109/ACCESS.2022.3152803.
- [70] RUSTI, B., STEFANESCU, H., IORDACHE, M., GHENTA, J., BREZEANU, C. and PATACHIA, C. (2019) Deploying Smart City Components for 5G Network Slicing. In *Proc. of EuCNC*: 149–154. doi:10.1109/EuCNC.2019.8802054.
- [71] FARNHAM, T.D., JONES, S., AIJAZ, A., JIN, Y., MAVROMATIS, I., RAZA, U., PORTELLI, A. *et al.* (2021) UMBRELLA Collaborative Robotics Testbed and IoT Platform. In *Proc. of IEEE RoboCom*. doi:10.1109/CCNC49032.2021.9369615.
- [72] BÜCH, D. and ESCH, M. (2023) CiTe: A Testbed for Smart City Applications and Architectures. In *Proc. of IEEE COINS*: 1–6. doi:10.1109/COINS57856.2023.10189229.
- [73] MORAVCIK, M. and KONTSEK, M. (2020) Overview of Docker Container Orchestration Tools. In *Proc. of ICETA*: 475–480. doi:10.1109/ICETA51985.2020.9379236.
- [74] YANG, S., REN, Y., ZHANG, J., GUAN, J. and LI, B. (2021) KubeHICE: Performance-aware Container Orchestration on Heterogeneous-ISA Architectures in Cloud-Edge Platforms. In *Proc. of IEEE ISPA/BDCloud/SocialCom/SustainCom*: 81–91. doi:10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.0000000.
- [75] BÖHM, S. and WIRTZ, G. (2022) Cloud-Edge Orchestration for Smart Cities: A Review of Kubernetes-based Orchestration Architectures. *EAI Endorsed Trans. Smart Cities* **6**(18). doi:10.4108/eetesc.v6i18.1197.
- [76] SANTOS, J., WAUTERS, T., VOLCKAERT, B. and DE TURCK, F. (2019) Towards Network-Aware Resource Provisioning in Kubernetes for Fog Computing Applications. In *Proc. of IEEE NetSoft*: 351–359. doi:10.1109/NETSOFT.2019.8806671.
- [77] MCGRATH, G. and BRENNER, P.R. (2017) Serverless Computing: Design, Implementation, and Performance. In *Proc. of IEEE ICDCSW*: 405–410. doi:10.1109/ICDCSW.2017.36.
- [78] GHAFARI, F. and ARABSORKHI, A. (2018) A New Adaptive Cyber-security Capability Maturity Model. In *Proc. of IST*: 298–304. doi:10.1109/ISTEL.2018.8661018.
- [79] SELAMAT, A., MARICAN, M.N.Y., OTHMAN, S.H. and RAZAK, S.A. (2022) An End-To-End Cyber Security Maturity Model For Technology Startups. In *Proc. of IEEE ICOCO*: 185–190. doi:10.1109/ICOCO56118.2022.10031900.
- [80] MARICAN, M.N.Y., RAZAK, S.A., SELAMAT, A. and OTHMAN, S.H. (2023) Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review. *IEEE Access* **11**: 5442–5452. doi:10.1109/ACCESS.2022.3229766.
- [81] BARTWAL, U., MUKHOPADHYAY, S., NEGI, R. and SHUKLA, S. (2022) Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots. In *Proc. of IEEE DSC*: 1–8. doi:10.1109/DSC54232.2022.9888808.
- [82] ANDRADE, R.O., YOO, S.G., TELLO-OQUENDO, L. and ORTIZ-GARCÉS, I. (2020) A Comprehensive Study of the IoT Cybersecurity in Smart Cities. *IEEE Access* **8**: 228922–228941. doi:10.1109/ACCESS.2020.3046442.
- [83] LIU, Q., QI, X., LIU, S., CHENG, X., KE, X. and WANG, F. (2022) Application of Lightweight Digital Twin System in Intelligent Transportation. *IEEE J. Radio Freq. Identif.* **6**: 729–732. doi:10.1109/JRFID.2022.3212169.
- [84] MAVROMATIS, I., PIECHOCKI, R., SOORIYABANDARA, M. and PAREKH, A. (2020) DRIVE: A Digital Network Oracle for Cooperative Intelligent Transportation Systems. In *Proc. of IEEE ISCC*. doi:10.1109/ISCC50000.2020.9219683.
- [85] FELDMANN, S., KERNSCHMIDT, K. and VOGEL-HEUSER, B. (2014) Combining a SysML-based Modeling Approach and Semantic Technologies for Analyzing Change Influences in Manufacturing Plant Models. *Procedia CIRP* **17**: 451 – 456. doi:10.1016/j.procir.2014.01.140.

- [86] WALLA, W. and KIEFER, J. (2011) Life Cycle Engineering – Integration of New Products on Existing Production Systems in Automotive Industry. In HESSELBACH, J. and HERRMANN, C. [eds.] *Proc. of Globalized Solutions for Sustainability in Manufacturing*: 207–212. doi:10.1007/978-3-642-19692-8\_36.
- [87] NIE, L., WANG, X., ZHAO, Q., SHANG, Z., FENG, L. and LI, G. (2023) Digital Twin for Transportation Big Data: A Reinforcement Learning-Based Network Traffic Prediction Approach. *IEEE Trans. Intell. Transp. Syst.* : 1–11doi:10.1109/TITS.2022.3232518.
- [88] (2018) *ETSI TS 102 940: ITS communications security architecture and security management*. Tech. rep., European Standards Organization (ESO).
- [89] (2012) *ETSI TS 102 942: Intelligent Transport Systems (ITS) Security - Access Control*. Tech. rep.
- [90] FESTAG, A., NOECKER, G., STRASSBERGER, M., LÜBKE, A., BOCHOW, B., TORRENT-MORENO, M., SCHNAUFER, S. et al. (2008) Network on Wheels: Project Objectives, Technology and Achievements. In *Proc. of IEEE/IFIP DSN-S*: 9–10.
- [91] (2020) *ETSI TS 133 501: Security architecture and procedures for 5G System*. Tech. rep.
- [92] (2023) *3GPP 33.501: Security Architecture and Procedures for 5G System*. Tech. rep.
- [93] HAIDER, S., KHALIL, W., AL-SHAMAYLEH, A.S., AKHUNZADA, A. and GANI, A. (2023) Risk Factors and Practices for the Development of Open Source Software From Developers' Perspective. *IEEE Access* 11: 63333–63350. doi:10.1109/ACCESS.2023.3267048.
- [94] WEN, S.F. (2017) Software Security in Open Source Development: A Systematic Literature Review. In *Proc. of FRUCT*: 364–373. doi:10.23919/FRUCT.2017.8250205.
- [95] (2022) *Software Assurance Maturity Model: A Guide to Building Security into Software Development*. Tech. rep.
- [96] KENGO OKA, D. (2021) *Software Composition Analysis in the Automotive Industry*, 91–110. doi:10.1002/9781119710783.ch6.
- [97] (2018) *Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) Phase 2*,". Tech. rep.
- [98] (2021) *ETSI TS 103 097: Security header and certificate formats*. Tech. rep., European Standards Organization (ESO).
- [99] LU, M., BLOKPOEL, R., FÜNFROCKEN, M. and CASTELLS, J. (2018) Open Architecture for Internet-based C-ITS Services. In *Proc. of ITSC*: 7–13. doi:10.1109/ITSC.2018.8569941.
- [100] PETIT, J., SCHAUB, F., FEIRI, M. and KARGL, F. (2015) Pseudonym Schemes in Vehicular Networks: A Survey. *IEEE Commun. Surv. Tuto.* 17(1): 228–255. doi:10.1109/COMST.2014.2345420.
- [101] MAHMOUD, M.M.E.A., MIŠIĆ, J., AKKAYA, K. and SHEN, X. (2015) Investigating Public-Key Certificate Revocation in Smart Grid. *IEEE Internet Things J.* 2(6): 490–503. doi:10.1109/JIOT.2015.2408597.
- [102] KUMAR, N., IQBAL, R., MISRA, S. and RODRIGUES, J.J. (2015) An Intelligent Approach for Building a Secure Decentralized Public Key Infrastructure in VANET. *J. Comput. Syst. Sci.* 81(6): 1042–1058. doi:10.1016/j.jcss.2014.12.016.
- [103] TORKURA, K.A., SUKMANA, M.I., CHENG, F. and MEINEL, C. (2017) Leveraging Cloud Native Design Patterns for Security-as-a-Service Applications. In *Proc. of IEEE SmartCloud*: 90–97. doi:10.1109/SmartCloud.2017.21.
- [104] LOZANO, S., LUGO, T. and CARRETERO, J. (2023) A Comprehensive Survey on the Use of Hypervisors in Safety-Critical Systems. *IEEE Access* 11: 36244–36263. doi:10.1109/ACCESS.2023.3264825.
- [105] SULTAN, S., AHMAD, I. and DIMITRIOU, T. (2019) Container Security: Issues, Challenges, and the Road Ahead. *IEEE Access* 7: 52976–52996. doi:10.1109/ACCESS.2019.2911732.
- [106] TEPPA, P. and NORRMAN, K. (2018) *Security in 5G RAN and core deployments*. Tech. rep., The Ericsson Research Foundation. URL <https://www.ericsson.com/en/reports-and-papers/white-papers/security-in-5g-ran-and-core-deployments>.
- [107] DÍAZ-ROJAS, J.A., OCHARÁN-HERNÁNDEZ, J.O., PÉREZ-ARRIAGA, J.C. and LIMÓN, X. (2021) Web API Security Vulnerabilities and Mitigation Mechanisms: A Systematic Mapping Study. In *Proc. of CONISOFT*: 207–218. doi:10.1109/CONISOFT52520.2021.00036.
- [108] POPE, J., RAIMONDO, F., KUMAR, V., MCCONVILLE, R., PIECHOCKI, R., OIKONOMOU, G., PASQUIER, T. et al. (2021) Container Escape Detection for Edge Devices. In *Proc. of ACM SenSys*: 532–536. doi:10.1145/3485730.3494114.
- [109] LI, X., LENG, X. and CHEN, Y. (2023) Securing Serverless Computing: Challenges, Solutions, and Opportunities. *IEEE Network* 37(2): 166–173. doi:10.1109/MNET.005.2100335.
- [110] CHATZIMICHALI, A. and CHRYSOSTOMOU, D. (2019) Human-data Interaction and User Rights at the Personal Robot Era. In *Proc. of ICRES*.
- [111] (2018) *Regulation (EU) 2018/1807 of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union*. Tech. rep., European Union.
- [112] FYSARAKIS, K., ASKOXYLAKIS, I.G., KATOS, V., IOANNIDIS, S. and MARINOS, L. (2017) *Security Concerns in Cooperative Intelligent Transportation Systems* (Taylor & Francis Group). doi:10.1201/b21885-16.
- [113] TOROK, A., SZALAY, Z. and SAGHI, B. (2022) New Aspects of Integrity Levels in Automotive Industry-Cybersecurity of Automated Vehicles. *IEEE Trans. Intell. Transp. Syst.* 23(1): 383–391. doi:10.1109/TITS.2020.3011523.
- [114] (2021) *Safety of Machinery*. Standard, International Electrotechnical Commission.
- [115] SADIQUE, F., CHEUNG, S., VAKILINIA, I., BADSHA, S. and SENGUPTA, S. (2018) Automated Structured Threat Information Expression (STIX) Document Generation with Privacy Preservation. In *Proc. of IEEE UEMCON*: 847–853. doi:10.1109/UEMCON.2018.8796822.
- [116] ROY, S., PANAOSIS, E., NOAKES, C., LASZKA, A., PANDA, S. and LOUKAS, G. (2023) SoK: The MITRE ATT&CK Framework in Research and Practice. *Arxiv*.