Vehicular Communications 55 (2025) 100967

Contents lists available at ScienceDirect

Vehicular Communications

journal homepage: www.elsevier.com/locate/vehcom

Architecture-based governance for secure-by-design Cooperative Intelligent Transport Systems

Tanja Pavleska [a,*], Massimiliano Masi [b], Giovanni Paolo Sellitto [c,1], Helder Aranha [d,1]

[a] Jozef Stefan Institute, Ljubljana, Slovenia
[b] Autostrade Per L'Italia SpA, Via Bergamini 50, Rome, 00118, Italy
[c] Rome, Italy
[d] Lisbon, Portugal

ARTICLE INFO

Keywords:
Security by design
Cooperative Intelligent Transport Systems
Standard lock-in
Governance
Interoperability

ABSTRACT

Cooperative Intelligent Transport Systems (C-ITS) involve a complex network of diverse components that communicate with each other and with their environment. These systems are essential for improving transport efficiency, enabling smoother movement of people and goods, and supporting economic growth. However, due to their highly connected nature, C-ITS face major challenges related to cybersecurity and interoperability—both of which are directly linked to safety. Managing evolving software and standards while ensuring security places a heavy burden on architects, security experts, and organizational stakeholders.

In this work, we propose a methodology to support the secure design and deployment of C-ITS systems. The approach is based on established standards and adaptable to other critical sectors, such as healthcare, energy and smart cities, but is here tailored to the specific context of the transport domain. Our main contribution is a governance-based framework for secure deployment of standards, aimed at addressing the problem of standards maintenance, interoperability, and architectural sustainability. We demonstrate its application through a real-world use case involving secure vehicle-to-infrastructure (V2I) communication.

1. Introduction

The road transport sector is a key enabler of modern infrastructure, supporting both economic activity and public mobility. Recognized as an Operator of Essential Services (OES) under the NIS Directive [12], this sector, particularly through intelligent transport systems, plays a vital role in ensuring safe, efficient, and resilient mobility. To maintain this role, it is important to secure the growing digital interconnectivity of road transport systems. Globally, Cooperative Intelligent Transport Systems (C-ITS) and Advanced Driver Assistance Systems (ADAS) are advancing rapidly, with major efforts underway in the USA [55], Europe [10] and Australia [49]. These technologies enable real-time communication between vehicles, infrastructure, and road users, helping to relay real-time information about hazards, traffic conditions, and road signals. This exchange improves road safety, reduces environmental impact, and optimizes infrastructure use.

However, greater connectivity also introduces new cybersecurity and governance challenges. C-ITS and ADAS increasingly operate within a complex digital ecosystem of interconnected components from multiple vendors, making the systems more vulnerable to attacks such as data manipulation, unauthorized access, or service disruptions [11]. To address this, security must be embedded from the start, not added later. This calls for a structured, architecture-based approach that provides a consistent, scalable, and future-ready foundation for cybersecurity and governance across the transport ecosystem.

In Europe, efforts for securing and harmonizing C-ITS have been led by CEN (TC 278), ETSI, and ISO, under the European Commission's Mandate M/453. These standardization initiatives made significant progress in defining core communication and security standards. However, maintaining alignment and consistency across different standards remains a major challenge. ETSI standards are tailored to the European regulatory and technical landscape, while ISO develops standard for global use. This difference in scope can result in mismatches between regional and international specifications. As a result, systems aligned with one standards may face compatibility issues when interacting with systems based on another, especially when legacy infrastructure is still in operation. This fragmentation can hinder global C-ITS deployment and complicate cross-border interoperability.

* Corresponding author.
E-mail addresses: atanja@e5.ijs.si (T. Pavleska), mmasi@autostrade.it (M. Masi), gogiampaolo@gmail.com (G.P. Sellitto), hmspider@gmail.com (H. Aranha).
[1] Independent Scholar.

https://doi.org/10.1016/j.vehcom.2025.100967
Received 14 June 2024; Received in revised form 5 August 2025; Accepted 13 August 2025

Available online 21 August 2025

Compounding this issue is the need to manage for backward and forward compatibility when standards evolve. Failure to ensure smooth transitions can lead to technological lock-in, where older solutions persist due to compatibility constraints, ultimately slowing innovation and long-term sustainability in C-ITS. The governance of C-ITS security must therefore account for the full lifecycle of standards - from their initial adoption to long-term maintenance and updates - ensuring that both new and existing technologies can co-exist without compromising interoperability.

To address these challenges, a comprehensive governance framework is essential, that would:

- Ensure interoperability at syntactic, semantic, and legal levels, enabling smooth communication across diverse C-ITS deployments.
- Embed security-by-design principles from the outset, strengthening resilience across the C-ITS ecosystem.
- Provide mechanisms for updating policies and standards, ensuring systems remain aligned with evolving regulations.
- Prevent vendor lock-in by promoting modular, open standards, thus supporting long-term adaptability and innovation.

Despite these needs, realizing such governance remains challenging in the absence of strong, coordinated regulatory support. In Europe, the European Commission proposed a governance framework for C-ITS, but this was ultimately rejected by the Council of the European Union.[2] As a result, the sector currently lacks a unified legal structure, which hinders progress toward a secure, interoperable, and sustainable C-ITS landscape.

In this study, we propose an architecture-based governance framework and a supporting methodology to address these gaps. Drawing from established standards already applied in sectors like healthcare, energy, and smart cities, we adapt these practices for the specific challenges of the Internet of Vehicles (IoV).

Our contribution focuses on three core objectives: 1) Addressing challenges in standard maintenance, interoperability and sustainability through a structured governance model that reduces fragmentation and prevents standard lock-in; 2) Introducing a methodology based on Enterprise Architecture (EA) principles to ensure that security is integrated by design throughout C-ITS development; and 3) Demonstrating the approach in a proof-of-concept implementation, focusing on secure vehicle-to-infrastructure (V2I) communication within real-world C-ITS deployments. A comprehensive implementation of the methodology contains a formalization of the entire procedure and a step-by-step guide for its secure deployment of RSUs is openly available on Github [53]

This paper is structured as follows: Section 2 situates our work within the broader research landscape, highlighting its contribution and differentiation from existing approaches. Section 3 lays the theoretical foundation of the proposed methodology. The approach is further detailed in Section 4, formalizing C-ITS as a standardized domain and defining the overall governance methodology. Section 5 demonstrates the methodology in a proof-of-concept case study, focusing on secure ITS Station deployment. Section 6 summarizes the approach and outlines future research directions for addressing security, interoperability and governance in C-ITS, and Section 7 concludes the paper.

2. Related Work

2.1. Overview of existing approaches

Despite progress in secure-by-design practices and emerging technologies, several critical challenges remain in securing C-ITS [60]. These include issues related to standardization, scalability, privacy, legacy infrastructure, interoperability, and dynamic operational environments, all of which require effective governance strategies [6].

Numerous studies have exposed *vulnerabilities* in current C-ITS architectures. For instance, Ranaweera et al. identify security vulnerabilities in 5G-based C-ITS use cases deployed in Multi-access Edge Computing environments [59]. Similarly, as communication and automation evolve within the automotive sector, new attack surfaces emerge, particularly in in-vehicle networks and Internet-of-Vehicles (IoV) technologies [52]. These systems are vulnerable to a range of cyberattacks, including denial-of-service (DoS), spoofing, man-in-the-middle attacks, and data breaches. Additional research highlights the importance of securing GPS systems, with emphasis on spoofing attack scenarios and detection mechanisms [16].

A secure C-ITS architecture must incorporate several key *components* for ensuring the overall security and resilience of the system: identity and access management, intrusion detection and prevention, data encryption, data anonymization, and privacy-enhancing technologies [64,19,52,2]. However, technical safeguards alone are not sufficient. Long-term security requires *robust governance mechanisms*, including well-defined security policies and standards, thorough risk management procedures, regular third-party security audits, and effective collaboration among stakeholders.

Several studies have identified limitations and inconsistencies in existing standards, highlighting the need for improvement [23,32]. In particular, Koshiyama et al. argue for the inclusion of algorithm auditing to assess risks in Artificial Intelligence (AI)- and Machine Learning (ML)-enabled systems, proposing a governance and compliance framework [14]. Yet despite these efforts, the issue of standard lock-in persists. A lack of widely adopted, standardized security protocols continues to hinder interoperability and increases the complexity of securing large-scale, multi-stakeholder C-ITS environments.

Enterprise Architecture (EA)-based governance is well-established in several critical sectors. Frameworks such as TOGAF [39], Zachman [35], and SAIF [44] offer structured approaches for achieving technological, environmental, and economic sustainability by supporting systematic design-time reasoning over abstract architectural artifacts. A notable example of an EA-driven methodology is Integrating the Healthcare Enterprise (IHE),[3] which promotes the coordinated use of established standards to improve interoperability in healthcare information systems. The (IHE) architecture is based on specific building blocks called *profiles*, which regulate how existing standards should be applied to address operational use cases. The IHE framework has received widespread recognition, being endorsed by the European Commission (through *Decision 2015/1302* and *Commission Recommendation 2019/800 on the European Electronic Health Record Exchange Format*, the World Health Organization [41], and the U.S. Department of Health and Human Services Interoperability Standards Advisory [56].

The healthcare sector is not alone in adopting EA-based models. Other domains, such as Smart Grid and Industry 4.0, also rely on architectural frameworks rooted in EA principles. For example, the Smart Grid Architectural Model (SGAM) [37] has been widely applied to energy distribution, electric mobility, and smart city infrastructures. These efforts have paved the way for using EA in broader critical infrastructure contexts.

Building on these established approaches, our methodology introduces an architecture-based governance framework tailored specifically to C-ITS. In addition to aligning with EA principles, it incorporates mandatory security countermeasure definitions as part of the design process. This integration strengthens the system's security-by-design and supports the creation of domain-specific security profiles, helping ensure that both interoperability and cybersecurity are addressed systematically from the outset. In comparison, Zeinab et al. [25] propose

[2] See, for e.g. https://www.europarl.europa.eu/doceo/document/A-9-2022-0265_EN.html.

[3] https://www.ihe.net/.

a framework for classifying security risks across layers such as sensing, communication, and protocol. While valuable, their approach falls short of providing a unified architecture for securing C-ITS systems. Similarly, Chattopadhyay et al. [8] propose a security-by-design model for autonomous vehicles, addressing specific threats and countermeasures. However, their approach omits critical infrastructure components, such as roadside units and back-end integration. Other efforts also suggest security countermeasures, but they lack an overarching framework to contextualize or apply them consistently [15].

Additional studies, such as [51], present architecture frameworks aligned with our design principles, but they do not explicitly address security requirements or integrate policy-driven security governance. Similarly, although [65] explores how architecture principles relate to security goals in C-ITS, it does not provide explicit mechanisms for embedding security-by-design or defining context-sensitive security objectives. Our contribution builds upon these foundations by introducing a security-aware EA framework (Section 3.1), which enables systematic reasoning over abstract yet context-aware architectural elements. This creates a structured foundation for embedding security-by-design principles throughout system development.

Among prior efforts, the work most closely related to ours is the Integrating the Energy System (IES) project [20,34], addressed similar challenges in the Smart Grid sector. The IES project adopted the IHE methodology, established governance committees, engaged stakeholders, and conducted testing events to ensure interoperability. While our work draws inspiration from this process, we go further by introducing a structured approach for automatically defining and updating security countermeasures based on the asset lifecycle, ensuring continuous adaptability to evolving threats in C-ITS environments.

Our methodology consolidates the fragmented perspectives of the presented approaches into a cohesive security architecture that treats security as a fundamental architectural concern. It builds on the RAMI 4.0 reference model, widely adopted for Internet of Things (IoT) systems, and applies it to the broader context of road transport infrastructure. Within this framework, we structure the entire life cycle of information assets,[4] enabling consistent mapping of assets to risks and appropriate countermeasures. Unlike prior approaches that emphasize one-time risk analysis, our framework supports continuous security governance. It prescribes a methodology for defining, eliciting, and updating security measures as system components evolve, ensuring that security-by-design principles are embedded from initial design through deployment and maintenance.

2.2. Literature-based Comparative Analysis

To contextualize our contribution, Table 1 compares the proposed methodology against the most prominent approaches in the domains of C-ITS, enterprise architecture, and infrastructure security. Each column in the comparison reflects a distinct and well-defined criterion, grounded in both the functional requirements of secure C-ITS deployment and the capabilities observed in the literature.

Modularity assesses whether the approach supports composable and reusable components or profiles, allowing architectural elements (e.g., security policies, message structures) to be decoupled and adapted across deployments. Our method is modular by design, supporting building-block based architectures modeled after RAMI 4.0. **Security-by-design** integration evaluates whether security requirements are embedded into the system architecture at design time, rather than added afterwards. The proposed methodology embeds security using the RMIAS model, enabling early selection of countermeasures based on classified assets.

With **interoperability lifecycle support**, we evaluate whether the methodology enables not just one-time interoperability, but its governance over time (e.g., versioning of standards, updates to integration profiles). This is a core capability of our approach via the lifecycle management of profiles. **Governance alignment** checks whether a formal governance structure (e.g., committees, roles, validation processes) is integrated into the methodology. We adopt a two-committee model inspired by IHE (Planning and Technical Committees), which ensures oversight and version management.

Automation & workload reduction refers to the degree to which tasks like compliance checking or countermeasure selection are automated or tool-assisted. Our method automates profile validation and security mapping via asset classifications, minimizing manual engineering effort. Finally, **domain-specificity to C-ITS** flags whether the approach directly addresses C-ITS scenarios and standards. Our profiles and use case are explicitly designed around ETSI, C-Roads,[5] and real RSU deployments.

From the table, it becomes evident that, while most approaches address some of the aspects, all of them lack an adaptive governance model for security and interoperability. Moreover, they focus primarily on threat modeling (e.g., risk assessment, cryptographic solutions), depending on a long-running system with a history of behaviors. In contrast, we introduce a formalized process for security countermeasure selection using the RMIAS, providing a goal-based security approach that can also include historical threat data. Moreover, unlike conventional standards-driven interoperability efforts (such as those by ETSI and ISO) and purely compliance-based frameworks, our method proactively prevents standard lock-in by enabling continuous profiling and adaptation mechanisms.

3. Background Concepts and Methodological Preliminaries

This section presents the foundational concepts that underpin our design methodology. Section 3.1 outlines the role of Enterprise Architectures and explains how applying EA principles to C-ITS can enhance both technological and organizational sustainability. Section 3.2 introduces the reference architecture model used to structure solution architectures for C-ITS deployments. Section 3.3 details the security model adopted to ensure security-by-design, highlighting its adaptability and integration with the selected architectural framework. Section 3.4 presents the Integrating the Healthcare Enterprise (IHE) governance model, an established methodology from the healthcare domain. We explain its relevance to C-ITS and how its concepts can be adapted to address similar interoperability and security challenges. These components are integrated in Section 4, where we present a unified, generic methodology for secure-by-design C-ITS development, which is then applied in a real-world scenario in Section 5.

3.1. Interoperability as an Enterprise Architecture concern

Interoperability is a fundamental pillar of security and governance that ensures smooth data exchange and system integration. In our work, we adopt the *interoperability levels* defined by the Healthcare Information and Management Systems Society (HIMSS) [43]: *foundational interoperability,* enabling basic data exchange between systems; *structural* or *syntactical*, which specifies the format and structure of messages; and *semantic interoperability*, which ensures that the exchanged data is interpretable and usable across systems. These levels span various aspects, including communication protocols, data formats, and legal agreements governing information sharing. When data access is hindered by syntactic mismatches (e.g., SOAP vs. REST), semantic inconsistencies (e.g., varying units of measurement), or conflicting legal frameworks (e.g., cross-border data restrictions), it can compromise more than efficiency, directly impacting system availability, a core tenet of the ISO 27001

[4] The “assets to protect”.

[5] https://www.c-roads.eu/platform.html.

Table 1
Comparison of our approach with existing methods: ✗ denotes lack of addressing the particular aspect; ✓ denotes presence of elements that address the aspect; ✓̸ denotes partial addressing of the aspect.

Approach	Security-by-design	Governance framework	Architecture approach	Automation & workload reduction	C-ITS domain-specific
Our Methodology	✓ Integrated through RAMI 4.0, RMIAS	✓ Governance of standards based on an IHE	✓ Uses modular building blocks, EA principles	✓ Automates security countermeasures	✓ Yes
Zeinab et al. [25]	✗ Focus only on risk classification	✗ No explicit governance model	✗ No modularity, focuses on risk layers	✗ Manual security assessment	✗ No
Chattopadhyay et al. [8]	✓̸ Threat-based only, lacks full infrastructure integration	✗ Security-focused, lacks governance structure	✓ Limited modularity, focus on vehicle-level security	✗ Manual evaluation of threats and responses	✓̸ Partially (focus on autonomous vehicles)
Integrating the Energy System (IES) [20]	✗ Focus on interoperability without structured security	✓ Uses IHE methodology for interoperability governance	✓ Modular and interoperability-driven	✗ Focus on interoperability, not automation	✗ No
Ranaweera et al. [59]	✓̸ Focus on vulnerabilities, lacks proactive security integration	✗ No explicit governance model, focuses on security threats	✗ Non-modular, focus on edge computing vulnerabilities	✗ Manual vulnerability assessment	✓ Yes
Santa et al. [62]	✗ Evaluates C-ITS messaging but does not embed security-by-design	✗ Lacks governance mechanisms, evaluation-focused	✗ Protocol evaluation only, no architecture approach	✗ Security evaluation requires manual configuration	✓ Yes
Koshiyama et al. [14]	✓̸ AI-driven algorithm for compliance-checking	✓̸ Algorithm auditing framework only	✗ Non-adaptable and non-modular approach	✓ AI-assisted compliance monitoring	✓ Yes
Yoshizawa et al. [23]	✓ A security and privacy model for V2X communication	✗ Only mentions a need for scalable security policies	✓ Supports modular security layers for V2X systems	✓ Automates risk detection	✓ Yes
Satunin & Babkin [63]	✗ Uses multi-agent system for ITS, does not incorporate security-by-design	✓̸ Focuses on auction-based approach, partial governance only	✗ Multi-agent ITS framework, lacks structured modular approach	✓̸ Multi-agent system automates ITS decision-making, but not security	✓ Yes
Traditional standards-based approaches	✗ Security added post-design	✓̸ Established standards (ETSI, ISO), but risk of lock-in	✗ Static standards with limited adaptability	✗ Compliance must be manually ensured	✗ No

Confidentiality-Integrity-Availability (CIA) triad. In safety-critical domains like C-ITS, the lack of semantic interoperability must never lead to consequences such as vehicle collisions, emphasizing the need for reliable and always-accessible data.

A key barrier to maintaining interoperability over time is the lack of governance for the standards development lifecycle. Without such governance, systems face standard lock-in, where rigid adherence to fixed standards prevents the adoption of improvements or new technologies. As standards evolve to fix bugs or add features, vendors may adopt updates inconsistently, resulting in fragmented systems and reduced interoperability. This raises the complexity and cost of project management, requiring ongoing coordination across stakeholders.

To address this, our methodology incorporates an Enterprise Architecture (EA) approach that supports modular design and lifecycle governance. We treat each system component as a standardized (architecture) building block within a structured architectural framework. This allows standards to be embedded at the building block level, ensuring that the Reference Architecture inherits these standards and passes them on to individual solution architectures. These building blocks expose only their interfaces while abstracting internal details, simplifying integration and maintenance. By encapsulating evolving standards in modular components, our EA-based approach ensures that interoperability is maintained over time, supporting long-term compatibility, scalability, and security across C-ITS and other critical infrastructure systems.

3.2. Architecture-based approach

Adopting a layered approach enables designers to systematically address interoperability challenges at each stage of system development. This separation of concerns proves especially valuable for cross-cutting issues such as security, allowing consistent and formal treatment across the entire architecture. By isolating architectural layers, experts can work within their respective domains while maintaining coherent communication across disciplines and abstraction levels.

The Reference Architecture Model for Industry 4.0 (RAMI 4.0) was formulated to establish a unified strategy for achieving interoperability and architectural consistency in Industry 4.0 environments [22,42,33]. Its structure, illustrated in Fig. 1, is organized along three distinct axes, each representing a different perspective on system design.

The first axis presents the six RAMI 4.0 architectural layers (from top to bottom): the *Business layer* covers financial, legal, and organizational considerations; the *Functional layer* captures the services provided by architectural components and their runtime environments; the *Information layer* handles data modeling and semantics, supporting semantic interoperability; the *Communication layer* defines how systems access information and services, including protocols like REST, SOAP, DSRC, and 5G). The *Integration layer* bridges the physical and digital worlds, including elements such as human-machine interfaces; and the *Asset layer* represents the physical components of the system, such as sensors, actuators, SCADA systems, and C-ITS stations.

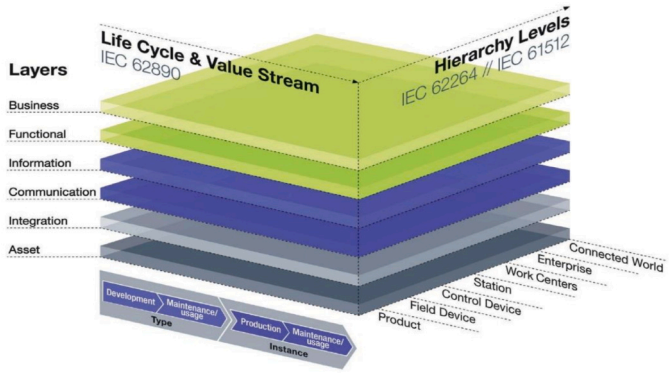

Fig. 1. The Reference Architecture Model for Industrie 4.0.

The second axis, *Life Cycle and Value Stream*, distinguishes between an asset's *Instance* (e.g., a deployed or operational unit) and *Type* (e.g., prototype or specification). This axis ensures that both design-time and runtime concerns are addressed, and that assets are consistently maintained throughout their lifecycle.

The third axis, *Hierarchy Levels*, spans from individual Products and Field Devices (e.g., sensors) to Control Devices, Stations, and Enterprises, culminating in the Connected World - the interface point between internal systems and the external digital ecosystem. This axis enables scalable modeling from local components to cross-organizational and global interactions.

RAMI 4.0 is highly adaptable and technically well-suited for systems built on IoT technologies. Its flexibility has already been demonstrated in other critical domains, for example, it has been used to design secure architectures for medical devices in the e-Health sector [5]. Building on this precedent, our work extends the use of RAMI 4.0 to the C-ITS domain, demonstrating its relevance in mobility infrastructures.

3.3. Security-by-design

The stringent security and architectural demands inherent in critical infrastructures, compounded by the global scarcity of security expertise, highlight the necessity for a comprehensive approach that: (a) integrates security from the earliest stages of system design rather than treating it as an afterthought; (b) spans the entire lifecycle of systems and products; (c) reduces long-term dependence on specialized security expertise; and (d) supports flexible and adaptable security provisioning. The methodology presented in this paper addresses all four of these principles. It promotes a sustainable design process that embeds security and compliance requirements as core elements, ensuring long-term architectural integrity.

The current architecture reference models for critical sectors referenced in security handbooks [38,13] usually adopt a threat-based security approach. These methods depend on historical system behavior to define countermeasures. However, this poses limitations, particularly during the design of new systems where such data is unavailable. Furthermore, threat-based models struggle to keep pace with evolving security requirements. To overcome these challenges, we incorporate the Reference Model for Information Assurance and Security (RMIAS) [9]. Unlike traditional threat-based methods, RMIAS starts by defining high-level security goals aimed at protecting business-critical assets and ensuring the continuity of operations. These goals are established independently of prior system behavior, making the model more suitable for use in early design phases and for novel systems lacking historical data. This goal-based strategy enhances adaptability and facilitates integration with organizational change management processes. It also promotes collaboration between business experts, who possess deep insights into *what* needs protection and the associated business risks, and security experts, who excel in understanding *how* to safeguard the asset against technical risks. By aligning security measures with business priorities from the outset, RMIAS supports proactive security planning and helps ensure that risk management evolves in step with organizational needs.

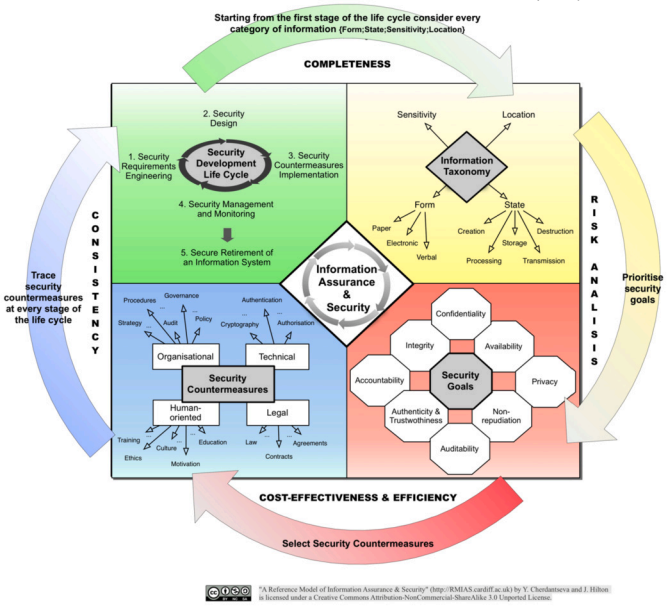

Fig. 2. Reference Model for Information Assurance and Security.

The model consists of four *dimensions*, as shown in Fig. 2:

- **Security Life-cycle** dimension illustrates how security is built up along the system's development life-cycle. It must be seamlessly embedded into the arbitrarily chosen Development Life-cycle, so that the outcomes of the former address the security concerns in each stage of the latter. This combination is called Security Development Life-cycle (SDLC).
- **Information Taxonomy** characterizes the nature of information being protected.
- **Security Goals** dimension contains a broadly applicable list of security goals. *Security goal* is the desirable ability of an Information System to resist a category of threats. Examples of goals are: Confidentiality, Integrity, Availability, Non-repudiation, etc.
- **Security Countermeasures** dimension categorizes the countermeasures available for the protection of information assets. It is a process that helps to achieve security goals and/or mitigate identified risks and vulnerabilities. Despite the goal-based nature of RMIAS, it can be successfully combined with threat-based approaches, as described in [24], to enhance the set of countermeasures according to given threat assessments.

By combining the RAMI 4.0 and RMIAS models, our approach makes it easier to design secure systems from the ground up. Security requirements are directly linked to specific parts of the system architecture, and protection measures are selected automatically based on the type of asset being protected, eliminating the need for manual assessments at every step. Moreover, the layered structure of RAMI 4.0 helps simplify this process by allowing experts to concentrate only on the layers relevant to their role, without needing to understand the full system in detail. As a result, standardized models can automatically propose security measures based on how different components interact, reducing the workload for security professionals and making the system easier to maintain over time.

3.4. Governance scheme for C-ITS

A strong governance framework is essential for C-ITS to manage its diverse stakeholders, including vehicle manufacturers, infrastructure

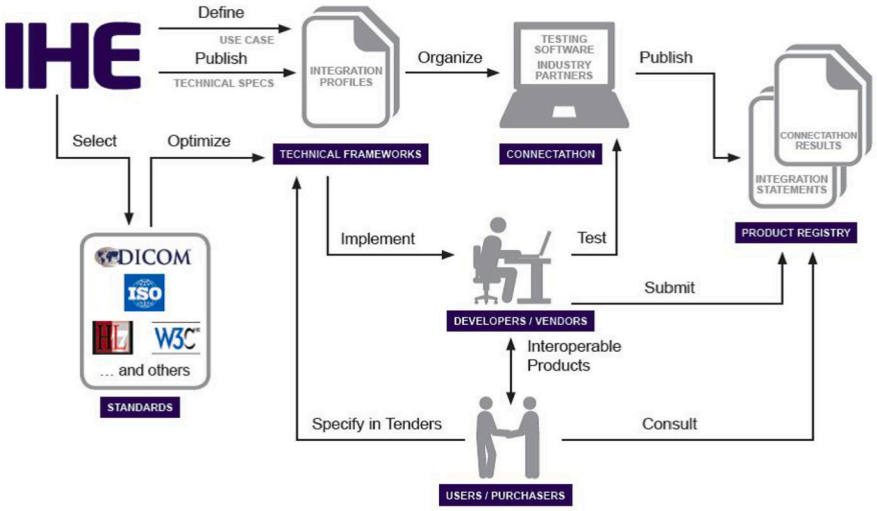

Fig. 3. The IHE Process. (Source: https://www.ihe.net/about_ihe/ihe_process/).

providers, and service developers. Many critical sectors use EA-based mechanisms to enforce governance rules and ensure interoperability. One advanced example is the Integrating the Healthcare Enterprise (IHE) initiative in healthcare.

IHE was designed to promote the coordinated use of established standards to address specific domain needs (initially for healthcare, but now well established in other critical sectors as well), ensuring interoperability between systems from different vendors. It includes frameworks for securing data and ensuring privacy, which are critical for C-ITS, where sensitive information about vehicles and infrastructure must be protected. Moreover, IHE has a proven track record in developing multi-stakeholder governance structures that manage the complexity of integrating various systems while ensuring regulatory compliance and fostering effective communication and cooperation.

The IHE governance model operates on three key principles: *selecting existing standards* using specific criteria like market penetration, security and support to specific use cases*creating standards-based specifications* by profiling the standards to establish interoperability and security by design; and *quality assurance*, by organizing public events called **Connect-a-thons**, where products are tested for compliance with their specifications.

Fig. 3 illustrates the overall process through which the IHE governance model is established for each IHE domain.

Each use case presenting interoperability challenges within the IHE framework undergoes scrutiny by a panel of technicians. Following open discussions and consultations, the technicians identify the relevant standards, capable of addressing the specific problem. These selected standards are subsequently incorporated into a *profile*. *Profiles represent a distinct set of functionalities encompassing implementation details encapsulated by **actors**, along with optional **transactions**, thus delineating the architecture's variability points*.[6] Profiles serve as the fundamental elements within the IHE methodology and they include profile use cases,[7] which are describing the intended context in which the profile should be used. They encapsulate governance principles that streamline standards, ensuring interoperability. Governed by a structured life-cycle, profiles uphold sustainability while serving as the *de-facto* building blocks within a Reference Architecture, integrating functionalities aimed at addressing

	Q1	Q2	Q3	Q4
Define Use Case				
Publish Technical Specs				
Testing Software				
Implementation				
Test				

Fig. 4. The IHE Process: timeline.

specific use cases. The integration profiles are structured within technical frameworks, each dedicated to a specific domain, and are publicly disseminated. Validation of the profile implementation by vendors is done during events known as Connect-a-thons, where necessary quality assurance measures are taken.

Fig. 4 illustrates the typical timeline for developing integration profiles following the IHE process. The cycle begins with the submission of a use case proposal to the Planning Committee, which typically requires 2–3 months to evaluate and formalize. Once approved, the Technical Committee initiates the drafting of the technical specification. This drafting phase also lasts approximately 2–3 months, during which the integration profile is defined. Concurrently, usually starting two months into drafting, testing tools are developed, and vendors begin implementing the profiles in preparation for validation. Full-scale interoperability testing, such as Connect-a-thon events, generally takes place 9–12 months after the initial use case proposal, allowing for synchronized development and early conformance testing.

IT architects design IHE-based architectures through formal procedures, by using profiles, and *grouping* them according to specific *grouping rules*. The operation of grouping consists of *merging* different profile functionalities to build complex use cases. The grouping rules are implemented as pointers to other profiles, indicating whether the use of such pointed profiles is mandatory or optional. This mechanism allows the grouped profiles to evolve independently. When grouping, a new profile is created that contains the combined use cases and defines all the actors and the transactions of the original profiles [48]. Some groupings are mandatory and defined by the IHE experts, representing the inter-profile dependencies that help in minimizing the decisions related to system design. In general, profiles are grouped by the IT architect to address a given use case. The final combination of profiles is named a *target solution architecture*.

The governance framework mandates that the achievement of Interoperability must be proven through successfully testing with at least three other vendor implementations, under the supervision of referees (appointed by IHE) at the Connect-a-thon. After successful testing, vendors publish their capabilities in *integration statements*. Integration

[6] Variability points are configurable design options within a system that allow architects to adapt parts of the system to meet specific quality goals, such as performance, security, or scalability.

[7] The concept of a *profile use case* should not be confused with the general term *use case*. The former refers to a specific instance of a case indicated within a profile.

statements are publicly available for sector policymakers, IT architects, and project managers to use and create tenders based on IHE profiles. They also know which global vendor implemented the profiles devised for specific architectures. A pillar of the technical frameworks is that IHE-based architecture will continue to be supported even if the standard is no longer maintained, thus achieving long-term technological sustainability. This is a key point when software systems are based on a variety of different standards from different organizations, as the governance model over them still guarantees interoperability.

It is important to note here that our work does not seek to redefine existing standards in C-ITS or healthcare governance. Rather, we propose a methodological and architectural bridge between their respective domains adapting the IHE governance and profile-based validation process (originally designed for healthcare interoperability) to the C-ITS domain. This includes tailoring the profile structure, validation lifecycle (e.g., Connect-a-thons), and layered architectural mapping (via RAMI 4.0) to the security and interoperability challenges specific to C-ITS.

In the remainder of this work, we assume an IHE-based governance model to be in place, and reuse the concepts of *domain*, *profile*, *grouping* and *Connect-a-thon*, to benefit from a mature and well-known methodology employed in the design and maintenance of critical infrastructures.

4. Methodology

In this section, we outline the methodology intended to facilitate the design of sustainable, interoperable, and secure-by-design solution architectures for the C-ITS domain. Fig. 5 depicts the relationships between the concepts, integrating modular C-ITS profiles, each composed of actors and transactions, across the entire system stack (from physical assets to business governance).

The vertically spanning block named *Profiles (C-ITS)* represents the IHE-based integration profiles that define the *actors* participating in the profile and the *transactions*, i.e. message exchanges between the actors (like authentication, data delivery, and audit logging). These profiles are the architectural core, cutting across and linking components in all RAMI layers to ensure modularity, reusability, and governance-driven integration.

The Business Layer contains the Business Objectives (on the left side), representing strategic drivers like mobility efficiency and safety. In addition, the right side consists of the Risks & Goals (RMIAS), defining security and assurance objectives aligned with system-level business priorities. These elements influence which profiles are selected and how they are configured. In the Functional Layer, the C-ITS Control handles decision logic and process orchestration for service execution, like warning issuance and routing. The Audit Record Repository and Policy Server, on the other hand, are security enforcement endpoints, used in profiles like ATNA. Through the Information Layer, abstract data representations are governed by semantic consistency between message producers and consumers (CAM, DENM formats), but are not explicitly named here to preserve the general character of the methodology. Furthermore, the Communication Layer defines the protocols (e.g., DSRC, 5G) used by profiles to facilitate real-time message delivery, whereas the Integration Layer bridges physical assets with the digital logic (for example, encoding data from sensors or packaging control logic into actionable flows). Finally, the Asset Layer contains the RSU (ITS-S) and Data Center (on the left), with all hardware and infrastructure roles; on the right, the OBU (Vehicle) represents the mobile asset communicating with the road infrastructure. These are the endpoints that instantiate the transactions defined in the profiles.

Each entity is connected via dotted arrows to the Profile block, indicating that profiles unify and structure the interactions. Deployment-specific logic is determined by how profiles are grouped and configured for a particular use case (as shown in the next section). This results in the development of a *target solution architecture* as an enhanced and expanded set of grouped profiles fortified with the necessary security measures to address the initial use case. This architecture not only anchors the security goals (via RMIAS) to system design at all levels, but promotes modular reuse of the profile specifications across deployments. Moreover, it ensures consistency between the business objectives, policy enforcement, communication mechanisms, and the physical systems.

By relying on IHE-based profiles, our methodology provides the technical capabilities needed to address the complex demands of diverse use cases. These profiles can be of different types: *content* profiles address semantic interoperability challenges; *infrastructural* profiles target syntactic hurdles; and *security* profiles are specifically tailored to address cyber-physical security and safety concerns. Security profiles are often integral components of mandatory groupings designed to combat infrastructural issues, with the general objective of establishing security-by-design. Within this framework, it falls upon the architect to define the content profiles tailored to address the precise requirements of each use case, thus paving the way for the (semi)automated emergence of security profiles during the system design phase.

4.1. Introducing C-ITS as a new IHE-based domain

Domains serve as structured communities where technical and administrative users convene to exchange insights and prioritize information sharing, as presented in Section 3.4. At the core of our methodology is the establishment of a new domain, which is critical for fostering INTEGRATION PROFILES and eliciting interoperability.[8]

To create a new domain, the initial step involves defining a set of profiles encapsulating specific functionalities pertinent to Vehicle-to-Infrastructure (V2I) and Infrastructure-to-Vehicle (I2V) communication. These profiles encompass various communication protocols already established within the C-ITS. Subsequently, a set of TEST ASSERTIONS is formulated to facilitate the creation of hypothetical CONNECT-A-THON events, pivotal for establishing the necessary quality assurance measures.

To implement an effective governance of C-ITS domains, the establishment of TECHNICAL and PLANNING COMMITTEES is of critical importance. The technical committee is tasked with developing and documenting solutions, primarily integration profiles. Conversely, the planning committee is responsible for long-term strategic planning, sustainability initiatives, and overseeing deployment activities, such as testing and educational events [47].

To bootstrap the process, an artificial *C-ITS domain* is initially forged. This enables individuals with operational and traffic management expertise to discern authentic integration profiles. Consequently, C-ITS equipment VENDORS can converge on consensus regarding the development of standards-based solutions that address information sharing priorities.

4.2. Profile governance

In IHE, developing a profile is a year-long process with multiple refinement cycles [46]. However, while profiles evolve over time, the governance model remains unchanged, as it is already mature and immediately applicable. This paper's methodology follows an established governance model, ensuring feasibility and reliability. Similar profile-based approaches in IHE (healthcare interoperability) and Smart Grids have successfully standardized interoperability and security without long delays.

The introduction of a new profile in the C-ITS domain follows a systematic and iterative (CONTINUOUS DEVELOPMENT) process [46]. Initially, a proposed use case is presented to the *planning committee*, which convenes quarterly to evaluate new work items. Following a voting process by eligible organizations, the work item is then forwarded to the *technical committee* for a thorough review of the proposed technical solution. Upon completion of a rigorous process to select the standards,

[8] We use IHE original concepts in SMALL CAPS typeface.

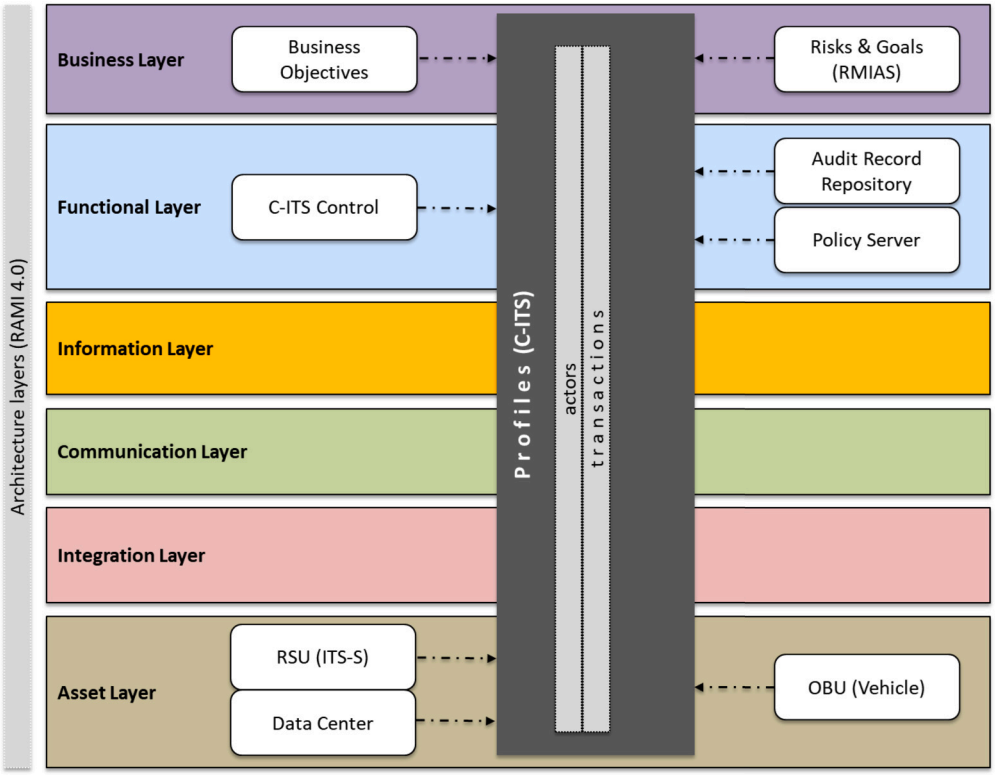

Fig. 5. Conceptual diagram of the methodology.

the profile is drafted in two volumes for public consultation, containing respectively:

1) A comprehensive overview of the profile, including the specific use cases addressed by the profile, the involved actors, and references to transactions and content modules.

2) In-depth technical descriptions of the individual transactions.

By successful participation in two consecutive testing events, the profile advances to its *final text* and becomes integrated into the domain *technical framework*. The development is primarily guided by the submission of use cases to the planning committee for evaluation during PROFILE DEVELOPMENT CYCLE, as outlined in Section 3.4.

Interoperability is formally evaluated at Connect-a-thons using semi-automatic tools and human intervention. These events, held annually for each continent, use *test assertions* [54]: *for each profile requirement, following the keyword organization set in [61], create an assertion, that is, a statement containing information that can be used to create reproducible* ***test chains***. The System Under Test (SUT) is tested for compliance with a specific normative source, for a prescription level (mandatory = SHALL, optional = SHOULD), in a specific context. For instance, a test assertion may stress the following requirement of the ATNA profile[9]: *"when used for I2V and V2I communications, messages shall be signed according to ETSI TS 102 940 v1.3.1"*. In this case, the mandatory source becomes the ATNA profile, the prescription level is mandatory, and the context is V2I and I2V communications.

By adopting the IHE development process, our methodology does not introduce any additional overhead. This holds both with regards to the original IHE process, as well as when compared to other standardization tracks (e.g. those governed by ISO), which typically require an average of 24 months to reach publication stages.[10] This is due to the fact that the IHE process enables parallel workstreams: while the Technical Committee drafts the integration profile, testing tools can be developed simultaneously. This coordination enables the delivery of a "trial implementation" profile, tested and validated by at least three vendors during the Connect-a-thon, within approximately 9 months. Such trial implementations are eligible for use in public procurement, allowing vendors to claim conformance early in the lifecycle.

In addition, the adoption of the IHE framework ensures technological sustainability with no extra overhead both during profile creation and countermeasures definition. Profiles function as architecture building blocks, encapsulating functionality independently from the evolution of underlying standards. Thus, when a referenced standard evolves, the IHE Technical Committee evaluates the changes and determines whether the integration profile should be updated – effectively decoupling system architecture stability from standard volatility and preventing lock-in.

4.3. Profile specifications

The C-ITS domain operates within a structured TECHNICAL FRAMEWORK, consisting of two volumes: VOLUME 1 offers comprehensive overviews of each profile, including the specific PROFILE USE CASE(s) they address, the involved ACTORS, and references to TRANSACTIONS and CONTENT MODULES. VOLUME 2, on the other hand, provides in-depth technical descriptions of the individual transactions [45].

To bootstrap the C-ITS domain, we introduce a set of five IHE-based profiles for architects to select from and design their solution architectures: Audit Trail and Node Authentication (ATNA), Exchange of ITS-S Messages (EIM), Road Works Warning (RWW), Share Kinematic Data (SKD) and RSU-to-Backend (R2B) communication. These integration profiles were chosen to represent a balanced cross-section of the most pressing challenges in current C-ITS deployments. They were not selected arbitrarily; instead, each addresses a distinct layer of interoperability and security concern that is common across national and cross-border initiatives:

[9] Audit Trail and Node Authentication, an original IHE profile that we reuse in our use case, as explained further.

[10] See, e.g., https://www.iso.org/stages-and-resources-for-standards-development.html.

- ATNA and SKD target foundational security challenges such as identity, trust establishment, and secure communication, which are critical regardless of the specific C-ITS application domain.
- EIM addresses cross-organizational identity management, relevant especially in international roaming scenarios, where vehicles may interact with infrastructure located in different jurisdictions.
- RWW reflects one of the core safety-related Day 1 services promoted in both the C-Roads platform and ITS-G5 rollouts, thus grounding the profiles in a widely supported operational use case.
- R2B addresses the backend integration challenge, often overlooked, but essential for ensuring coherent data flow from edge infrastructure (e.g., RSUs) to traffic control centers.

Together, these profiles span the content, infrastructure, and security views defined by our methodology, while also mapping to real-world interoperability pain points observed in EU projects such as C-Roads, InterCor,[11] and NordicWay.[12] The structure and lifecycle management proposed for these profiles can be generalized to support other use cases such as in-vehicle signage (IVS), cooperative adaptive cruise control (C-ACC), or vulnerable road user (VRU) protection services, by following the same architectural layering and governance approach.

The respective specifications of each profile, in accordance to Volumes 1 and 2 of the Technical Framework, are provided in the following subsections.

4.3.1. Volume 1 - Integration Profiles

In this section, we present excerpts from the specifications contained in Volume 1 of the Profiles in the C-ITS domain. Each profile follows a specific template, consisting of: i) introduction and motivation, ii) actors and transactions diagram, iii) use cases, and iv) grouping rules.

Audit Trail and Node Authentication (ATNA)

Introduction to the profile: The ATNA profile defines how secure, authenticated communication channels are established between different components of a C-ITS platform. This profile is essential for ensuring that sensitive data shared between components remains protected. Its use is mandatory because key security functions, such as authentication and accountability, are critical in C-ITS environments.

Actors: ATNA involves four main types of system actors: The *Audit Record Repository* (ARR) secure, tamper-proof storage system that collects and stores audit logs. These records are accessed by: *Audit Consumers* (AC) - systems or tools that analyze audit trails to detect or investigate security-related events; *Secure Nodes* (SN) - devices, typically hardware components like roadside units (RSUs), that can only be accessed through authenticated communications; and *Secure Applications* (SA) - software-based systems such as backend servers. Unlike SNs, these may have privileged access (e.g., admin/root accounts) and additional security controls.

Transactions: ATNA specifies two transactions: *Record Audit Event [C-ITS-01]*, which defines a standard log message format, typically using syslog, which is sent to the ARR to document security-relevant events; and *Node Authentication [C-ITS-02]*, which requires that communication channels between nodes are secured using encryption and integrity-protection methods (e.g., TLS, digital signatures). All system vendors must support both transactions to ensure compatibility and compliance. An illustration of these interactions is provided in Fig. 6.

Use Cases: *Normal node process flow*. When one Secure Node (e.g., a vehicle or RSU) needs to exchange data with another, it first initiates a secure channel based on agreed security measures such as encryption or digital signatures. After establishing this connection, the initiating node logs the transaction by sending an audit record to the ARR. When the receiving node completes the data exchange, it also sends an audit entry, ensuring full traceability on both ends.

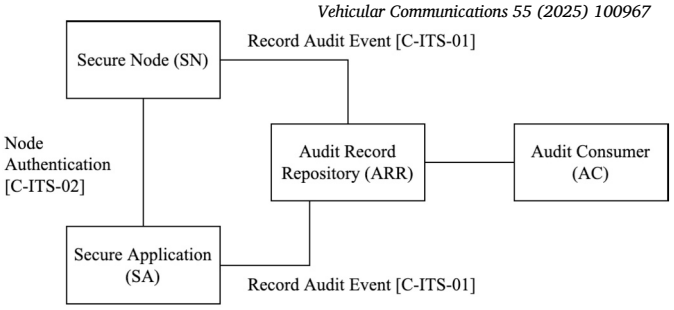

Fig. 6. ATNA: actors and transactions.

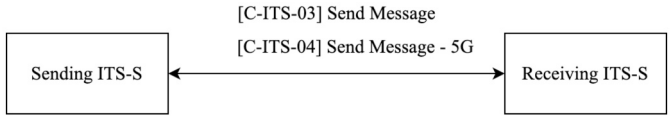

Fig. 7. EIM: actors and transactions.

Grouping Rules: Every system that incorporates the ATNA profile must specify: What details are included in the audit logs, and what encryption methods are used to protect communication channels. These requirements help ensure that all implementations meet a consistent standard of security while remaining adaptable to different deployment scenarios.

Exchange of ITS-S Messages (EIM)

Introduction to the profile: The EIM profile facilitates data exchange between the RSUs and the OBUs. The architecture is defined in [27], specifying the communication framework used by the Cooperative Awareness Message (CAM) [28] and Decentralized Environmental Notification Message (DENM) [30] services. While EIM does not alter the structure or content of these messages, it requires full compliance with the relevant standards. The actual values transmitted (e.g., types of alerts or statuses) are defined in coordination with specific content-oriented profiles like RWW and SKD.

Actors: EIM involves two primary actors: *Sending ITS-S* (SI), which is typically an RSU or OBU responsible for generating and sending CAM or DENM messages, and *Receiving ITS-S* (RI), which represents the counterpart system that receives and processes these messages, enabling appropriate C-ITS responses. These systems are expected to operate over Dedicated Short Range Communications (DSRC) and, optionally, 5G networks.

Transactions: EIM has two transactions: *Send Message [C-ITS-03]*, defining how standardized messages (e.g., CAM, DENM) are transmitted over DSRC, and *Send Message - 5G [C-ITS-04]*, which enables message transmission using 5G. This transaction is optional and reflects the architectural flexibility of the profile.[13] Fig. 7 illustrates these transactions and their interaction.

Use Cases:(1) *Vehicle data sharing.* When a vehicle needs to transmit sensor information (e.g., speed, direction, or position), it uses the communication format defined by the EIM profile. (2) *Infrastructure data sharing.* Similarly, when infrastructure systems (e.g., highway management, or smart city platforms) need to broadcast information, they also follow the EIM-defined message structure.

Grouping Rules: EIM is designed to work in conjunction with content-specific profiles, such as RWW and SKD, and cannot operate independently. Its role is comparable to the IHE XDS/BPPC relationship

[11] https://c-its.developpement-durable.gouv.fr/en/projects/intercor/.
[12] https://www.nordicway.net/.

[13] This example illustrates how IHE architectures can accommodate future technologies by using optional components for standards that may not yet exist.

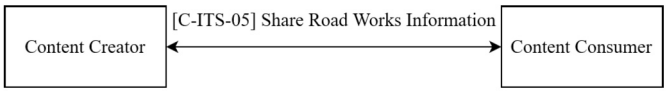

Fig. 8. RWW: actors and transactions.

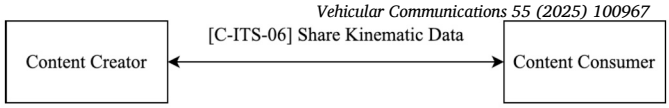

Fig. 9. SKD: actors and transactions.

in healthcare systems: EIM manages how data is exchanged (the transport layer), while the content profiles determine what data is exchanged and how it should be handled [47]. Unlike generic transport protocols, EIM is specialized for use with DSRC and optionally 5G.

When grouped with the ATNA profile, both the Sending ITS Station (ITS-S) and the Receiving ITS-S are treated as Secure Nodes. This ensures that messages are protected for integrity, authenticated, and authorized according to the ETSI security architecture [31]. Both sending and receiving actions must generate audit logs, which are defined by the following fields:

- *Who:* identity based on the subject in the ITS-S's enrollment certificate
- *What:* the string "C-ITS-03" indicating the transaction type
- *When:* the timestamp of the transaction
- *Resource:* the value of the (Provider Service Identifier) (PSID) from the Authorization Certificate
- *Server:* the StationID of the ITS-S

Road Works Warning (RWW)

Introduction to the profile: The RWW profile, based on the ISO 21219 standard [50], defines how road infrastructure systems should send notification messages to alert vehicles and drivers about upcoming road works. Its goal is to reduce traffic disruptions and enhance safety near construction zones.

Actors: RWW is composed of two actors: Content Creator (CC) and Content Consumer (CCons). Content Creators are typically a road authority system or infrastructure operator that generates road works information by filling in predefined fields within a DENM message. Content Consumers are systems (such as an on-board vehicle unit) that receive the DENM message and interpret it using the same standardized vocabulary to take appropriate action (e.g., alerting the driver or adapting route).

Transactions: RWW defines one main transaction: *[C-ITS-05] Share Road Works Information*, which uses ETSI's DENM format to deliver structured road works data between the infrastructure and vehicles [30]. The message structure and protocol for this transaction are illustrated in Fig. 8.

Use Cases: *Road Works Ahead Notification.* When the infrastructure operator is aware of ongoing or planned roadworks, details such as the location, affected lane(s), and expected duration are encoded using the C-ITS-05 transaction. This message is broadcast to nearby vehicles, allowing them to take preventive measures (e.g., reduce speed or change lanes).

Grouping Rules: must be used in conjunction with a transport profile such as EIM to ensure the proper transmission of messages. As part of the security and accountability process, both the sender and receiver generate an audit trail each time a message is sent or received. The audit trail includes the following information:

- *Who:* identifies the ITS station using the subject of its enrollment certificate.
- *What:* specifies the transaction type, labeled as "C-ITS-05."
- *When:* records the exact date and time the message was sent or received.
- *Resource:* contains the unique identifier for the road works event being reported.
- *Server:* indicates the StationID of the ITS station involved in the communication.

This type of logging ensures traceability, accountability, and regulatory compliance within the C-ITS environment.

Share Kinematic Data (SKD)

Introduction to the profile: The SKD profile is designed to transmit key movement-related data from vehicles, such as speed, turning angle, and acceleration, to roadside infrastructure. This data helps enhance real-time traffic monitoring and safety decisions. The SKD builds on existing standards like ETSI CAM and ISO/TS 18234 [28]. Typically, each vehicle sends this information 10 times per second (10 Hz).

Actors: SKD is composed of two actors: Content Creator (CC) and Content Consumer (CCons). Content Creators are software systems that within vehicles that generate and package movement data into the CAM message. Content Consumers are infrastructure-side systems (e.g., traffic controllers) that receive and interpret this data using the same format and definitions to ensure consistent understanding and reliable decision-making.

Transactions: SKD has one transaction: *[C-ITS-06] Share Kinematic Data*, which is based on the ETSI CAM standard and is responsible for transmitting the vehicle's movement information [28]. It is illustrated in Fig. 9.

Use Cases: *Real-Time Traffic Management:* Road operators use the movement data provided by vehicles to assess traffic conditions, predict congestion, and dynamically adjust traffic signals or routing suggestions. By having access to precise, real-time vehicle data, infrastructure can respond more intelligently to road conditions and enhance safety.

Grouping Rules: Although the SKD profile does not mandate a specific grouping with other profiles, it still includes a standardized audit mechanism to ensure traceability and accountability for each data exchange. Both the sender and receiver must generate an audit log containing the following information:

- *Who:* identifies the entity using the subject field from the Authorization Certificate of the ITS-S.
- *What:* the operation performed, marked by the string "C-ITS-06".
- *When:* the exact timestamp of when the transaction occurred.
- *Resource:* identifier of the specific data stream, using the PSID from the Authorization Certificate.
- *Server:* the StationID of the ITS-S involved in the transaction.

This audit trail ensures transparency and compliance by tracking each exchange of kinematic data, even in the absence of strict grouping requirements.

RSU-to-Backend communication (R2B)

Introduction to the profile: The R2B profile addresses a key interoperability challenge: how to reliably and efficiently transmit high-frequency data streams between RSUs and backend data centers. This is particularly relevant for profiles like SKD, which generate data at rates of 10 Hz per vehicle. Ensuring that this data reaches the backend without loss and in near real-time is crucial for system performance and traffic management. To handle the volume and reliability demands of this communication, several technologies were considered, such as Apache Kafka, JMS queuing systems, and Datex II. However, in this work, we demonstrate the use of the Connecting Europe Facility (CEF) eDelivery

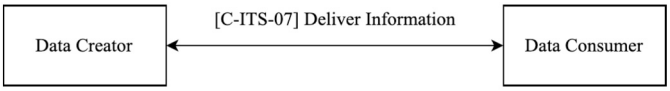

Fig. 10. R2B: actors and transactions.

building block as a standards-based, secure, and scalable messaging solution [7].

Actors: R2B is composed of two actors: the Data Creator (DC), which initiates the transmission of data (typically the RSU sending vehicle data to the backend), and the Data Consumer (DCons), which receives the incoming data and processes it according to its defined semantics (such as a traffic control center or data analytics service).

Transactions: R2B has one transaction: *[C-ITS-07] Deliver Information*, which facilitates the secure and reliable transmission of data from the RSU to the backend data center, or vice versa. It is based on the specifications defined in the ebMS 3.0 protocol, as outlined in [7]. Fig. 10 visually represents the flow of this transaction.

Use Cases: *Communicate data with the data center* Motorway operator needs to deploy RSUs that can both send and receive real-time traffic information to and from the backend infrastructure in order to fully participate in C-ITS data sharing.

Grouping Rules: R2B must be grouped with the ATNA profile to ensure secure communications. Each data exchange, whether sending or receiving, is logged through an audit trail with the following fields:

- *Who:* identifier from the Authorization Certificate of the ITS-S.
- *What:* fixed string "C-ITS-07" representing the transaction type.
- *When:* the timestamp of the transaction.
- *Resource:* the PSID value from the Authorization Certificate
- *Server:* the StationID of the ITS-S

4.3.2. Volume 2 - Transactions

Here, we present the specifications of transactions according to Volume 2 for the profiles defined in the previous section. Similarly to Volume 1, Volume 2 also follows a template, containing: i) underlying standards and, where applicable, ii) transactions definition.

ATNA **Underlying standards.** The channel is established either using TLSv1.2 or higher (such as ISO 21177), while message signature can be in XML or using ETSI TS 102 940 v.1.3.1. Although there is not yet a defined standard format for storing audit trail, one inspired by rfc3881 will be defined. **C-ITS-01** is based on the Syslog protocol [36,18] whose payload shall be defined as per rfc 3881. For each log entry, the following information is reported: "*who* did *what*, and *when* on which *resource*, *using* which server". **C-ITS-02** requires either the use of TLSv1.2 with a strong cipher-suite (to be constrained by local project policies), or, when used for I2V and V2I communications, messages shall be signed according to ETSI TS 102 940 v1.3.1.

EIM **Underlying standards.** The access layer is specified by ETSI EN 302 6635 [29] for the **C-ITS-03**. The **C-ITS-04** provisions the use of standards not-yet delivered by associations, such as 5GAA [1].

RWW **Underlying standards.** The format for the messages for the **C-ITS-05** is defined by the DENM basic service in [30], and is further addressed by [50].

SKD **Underlying standards.** The access layer is specified by ETSI TS 102 637-2 [28] for the **C-ITS-06**.

R2B **Underlying standards.** The access layer for the **C-ITS-07** is specified by the CEF building block eDelivery [7].

It is worth emphasizing here that the specification of the C-ITS message structure is maintained, but the architecture provides a governance through integration profiles that ensure consistency, interoperability,

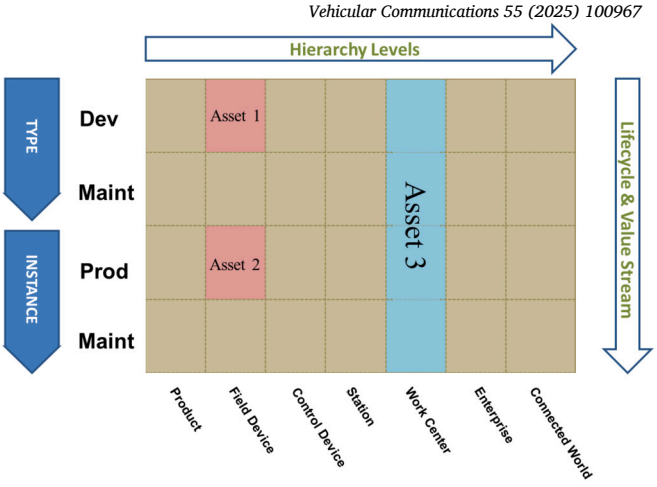

Fig. 11. Dissecting over a RAMI 4.0 architecture layer.

and compliance across different deployments. The novelty of our approach lies in the following key aspects:

- *Structuring the use of ITS-S messages* within a broader, architecture-based interoperability model aligned with standardized architectural frameworks. While our reference framework is RAMI 4.0, the approach remains flexible and can be readily adapted to other established models with minimal adjustment.
- *Mapping ITS-S message flows* to specific architectural layers and security policies through the use of proposed integration profiles, thereby clarifying their role within the system architecture.
- *Supporting governance bodies* in managing changes to message implementation and usage contexts over time, via a defined profile lifecycle and validation process.

Thus, although ITS-S message formats are pre-defined, our framework provides the architectural and governance scaffolding needed to integrate them into C-ITS deployments in a manner that ensures secure-by-design engineering and cross-vendor interoperability. This governance-driven approach to standardized content forms the core contribution of our work, as elaborated in the following subsections.

4.4. Architecture-based profile dissection

The dissection of profiles starts with a comprehensive analysis of the actors, transactions, and underlying standards, referred to as *technology*, associated with each profile. As Fig. 11 shows, it is a bottom-up procedure traversing though the RAMI 4.0 layers (Fig. 1), ultimately yielding the following constructs:

- **Asset** and **Integration** layers: As IHE does not mandate the use of specific products, these layers are deferred for subsequent iteration.
- **Communication** layer, which has as its target constructs Infrastructure and Security profiles (e.g., HTTP, TLS). Profile specifications are mapped into the Type/Development row of the RAMI's Lifecycle & Value Stream dimension. In the Instance/Production row, vendors' implementations of these specifications are placed. Each *actor* defined in the profiles is part of the Type/Maintenance, accompanied by their technical representations and associated informative assets (e.g., manuals) within the Instance/Maintenance.
- **Information** layer includes Content Profiles as target technologies, undergoing a similar dissection process. Their definition materializes within the Type/Development, transitioning into instantiation within the Instance/Production.
- **Functional** layer encapsulates Profile use cases within its Type/Dev, describing the functionalities offered by each profile.

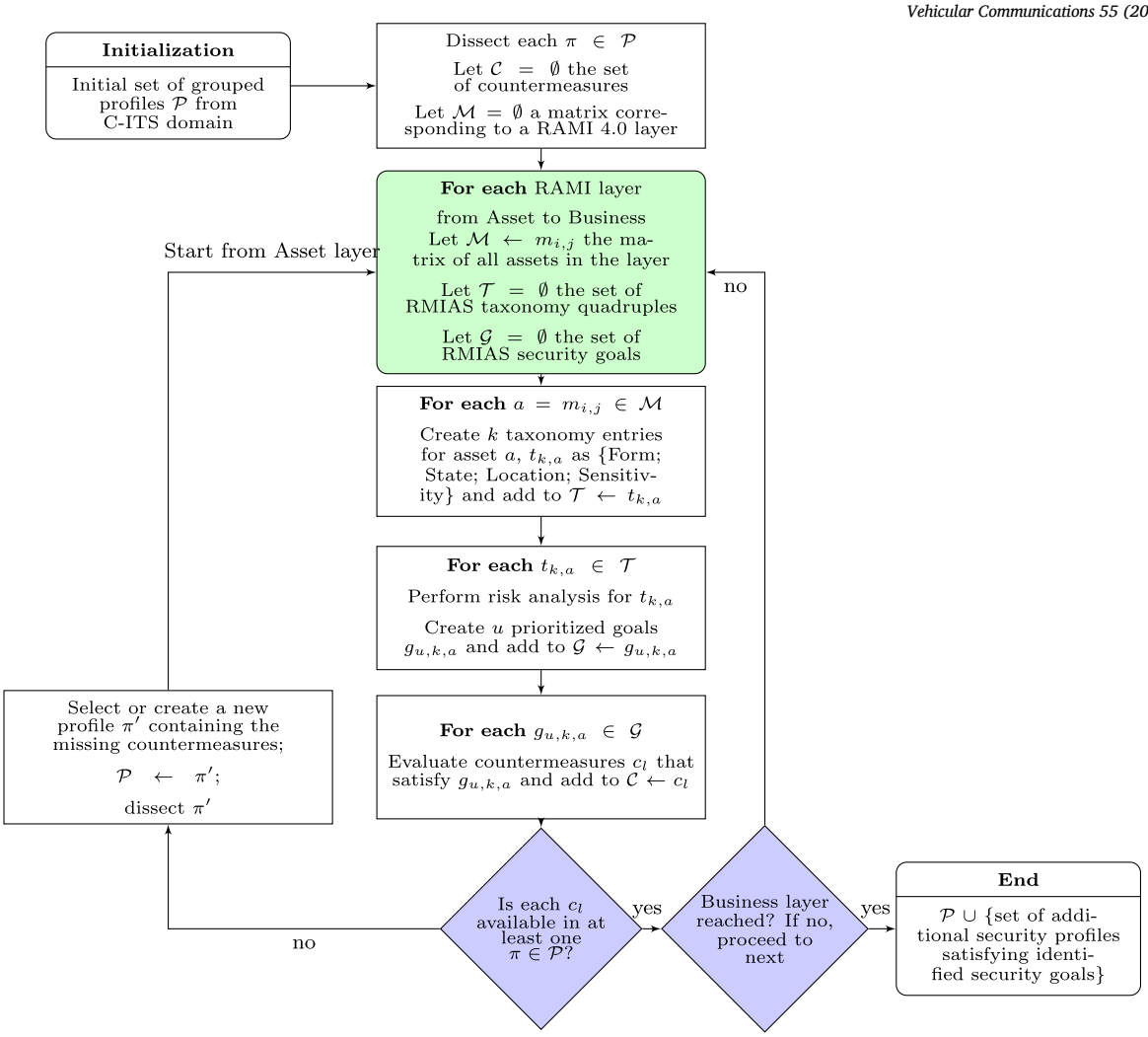

Fig. 12. The integrated model. Assets to protect are identified via RAMI 4.0 and security countermeasures are elicited with RMIAS, having architecture building blocks as input and output.

- **Business** layer incorporates pertinent information such as budgetary considerations, along with political and legal interoperability aspects.

Each architectural layer is populated with the contents of the profiles and remains amenable to further updates as the architecture evolves.

4.5. Eliciting security countermeasures

As a preliminary step before implementing the Reference Model for Information Assurance and Security (RMIAS), it is important to select an appropriate Software Development Life Cycle (SDLC). The RMIAS process starts from the initial stage of the SDLC, which involves the identification of the information assets requiring protection and their categorization, based on the RMIAS information taxonomy. The procedure is outlined in Fig. 12. The same asset may fall into different categories depending on its lifecycle phase, such as during creation and transmission. For each asset category, one or more security goals are prioritized in alignment with the assessment of business risks. Subsequently, cost-effective countermeasures are identified to fulfill the selected security goals for each asset category. This process is iterated across all stages of the SDLC, with ongoing monitoring of the effectiveness of implemented measures.

From a formal standpoint, each of the resultant architecture layers derived from the dissection process, can be represented as a matrix $\mathcal{M} := 4 \times 7$, where each element $m_{i,j}$ represents an asset to be protected, with i and j being the coordinates in the Hierarchy and Lifecycle & Value Stream axes (see Fig. 11). These assets can range from protocols and servers to devices and contracts. Protection considerations extend across all stages of the asset lifecycle, (creation, processing, transmission, persistence and destruction). The methodology accommodates this multifaceted perspective by eliciting security countermeasures for each asset at every stage of its lifecycle in a semi-automatic manner. This iteration follows the RMIAS model (as outlined in Section 3.3) to derive a comprehensive set of countermeasures aligned with business-oriented security goals. The identified countermeasures are then matched to security profiles within the domain, leading to the respective inclusion or creation of new profiles, thereby enriching and fortifying the solution architecture.

After identifying the lifecycle of the assets, the next iteration produces a taxonomy of quadruples structured as {Form; State; Location; Sensitivity}. “Form” denotes the medium of the asset, which could be *verbal, electronic, or paper-based*. “State” reflects the specific lifecycle stage of the asset, encompassing *creation*, *transmission*, *storage*, *processing*, and *destruction*. “Location” pertains to the physical location of the asset at a given moment or a categorization thereof that conveys the degree of organization control over the asset (e.g., *Restricted, Unrestricted*).

Lastly, "Sensitivity" denotes the security classification of the data.[14] For example, two entries within the taxonomy can be as follows:

1. <Form: Electronic, State: Creation, Sensitivity: top secret, Location: restricted >
2. <Form: Electronic, State: Transmission, Sensitivity: top secret, Location: restricted >

The first entry pertains to the data creation process, such as in the healthcare sector, where confidentiality and authentication are pivotal security goals. For instance, C-ITS data may require top-secret classification to safeguard critical infrastructure assets, while also being restricted to specific locations, such as within a constrained road infrastructure area. Likewise, the second entry addresses data transmission considerations. Each entry is designated as $t_{k,a}$, indicating the k-th taxonomy entry for the asset a, stored in a dedicated set $\mathcal{T}$.

Following the identification of taxonomy entries, the methodology proceeds with risk analysis. This analysis can be conducted either for an operational system or through abstract asset reasoning [57]. The outcome is a set of desired (i.e., prioritized) security goals tailored to the system of interest, encompassing all its assets. These security goals serve as high-level benchmarks, facilitating discussions with non-security experts [4].

Once security goals (referred to as $g_{u,k,a}$) are established for each asset category $t_{k,a}$ within the set $\mathcal{G}$, the security experts assess the required countermeasures to achieve these goals, often employing cost-effectiveness analysis. These countermeasures are then cross-referenced with the profiles defined for the relevant domain. If a match is identified, the process proceeds to the next asset; otherwise, the countermeasures are identified as new and used to formulate new profiles that meet the specific requirements of the use case.

4.6. Real-world application

The proposed approach is designed to be incrementally deployed using a combination of existing infrastructure, standardization initiatives, and governance structures. Its real-world implementation would follow a phased adoption strategy to ensure minimal disruption and resource efficiency.

Establishment of a governance framework. The governance model follows a federated approach rather than relying on a single central entity. Inspired by IHE governance in healthcare, the deployment would be community-driven, where key stakeholders (e.g., public authorities, road operators, OEMs, and technology providers) participate in a profile development process. While a technical C-ITS Coordination Body (which can be an extension of existing regulatory agencies like ETSI, ISO, C-Roads, or the existing C-ITS Point of Contact - CPOC[15]) can oversee compliance, implementation remains distributed among various industry players.

Adoption of interoperability profiles in existing systems. Profiles do not replace existing C-ITS systems; instead, they serve as an added layer that enhances their functionality. Each profile defines a set of requirements that vendors and operators can implement in their systems without requiring a centralized controller. Profiles such as RWW, SKD, and EIM integrate into existing V2X and RSU infrastructure without necessitating a large-scale overhaul. Since the approach is based on Enterprise Architecture principles, it allows for gradual adoption through modular implementation rather than a single large-scale deployment.

Leveraging existing standardization bodies and compliance processes. As reported above, the compliance process can leverage existing governance structures such as ETSI ITS, ISO, IEEE, and the EU C-Roads Platform, reducing the need for new regulatory bodies. It also integrates with national and regional mobility strategies (e.g., EU Cooperative, Connected, and Automated Mobility (CCAM) initiatives) to ensure it aligns with ongoing legislative efforts.

Resource efficiency. The framework is designed to be scalable and self-sustaining, reducing the need for extensive overhead. Unlike traditional standardization efforts that require heavy regulatory oversight, the profile-based approach allows for independent, domain-specific groups to develop and manage their own interoperability standards. Connect-a-thons allow vendors to validate compliance without ongoing government intervention. Moreover, industry stakeholders self-certify their compliance with predefined C-ITS profiles, which reduces the need for a centralized enforcement agency. The governance model relies on automated compliance testing rather than manual inspections. Test assertions and automated conformance tools can be developed to validate C-ITS components at vendor and deployment levels. For example, when a new RSU is deployed, it runs a self-check validation against predefined security and interoperability profiles before being approved.

Finally, it is important to reiterate that the deployment model in this work follows a layered abstraction mapped to concrete system components. Thus, it consists of both directly implementable and abstract governance components. Directly implementable elements include RSUs and OBUs with ETSI-compliant DSRC/5G interfaces for real-time CAM and DENM message exchange; EIM, RWW, and SKD profiles that define runtime message structures and semantics based on ETSI and ISO standards; the ATNA profile, which enforces secure communication through mutual TLS and syslog-based audit logging (C-ITS-01, C-ITS-02); and R2B for secure back-end integration using ebMS3.0 over the CEF eDelivery stack (C-ITS-07). In contrast, abstract governance components, such as profile grouping and dependency logic, define how content, transport, and security profiles are composed and validated at design time. These include the policy server, which governs conformance and audit policies (optionally implemented for certification workflows), and the audit record repository, which, although deployable, is treated as a compliance anchor whose instantiation depends on jurisdictional needs. The following section sheds greater lights on the implementation details of the methodology, showcasing a real-world scenario for a V2I infrastructure.

5. Use Case: Deployment of a V2I Infrastructure

In this section, we put into practice the proposed methodology and use it for the secure deployment of V2I infrastructure, namely Road Side Units (RSUs), following each step outlined in the previous section. First, we define the specific profile use cases through which we instantiate the methodology. Then, we identify the profile dependencies and groupings to enable their mapping and integration into the RSU deployment as part of the overall C-ITS architecture. Finally, we elicit the specific security requirements essential for safeguarding the RSUs and the data they handle. By identifying and addressing these requirements, we strengthen the overall security posture of the RSU deployment.

A comprehensive implementation of the methodology providing a practical resource for secure deployment of RSUs is made openly available on Github [53]. It contains a formalization of the entire procedure and a step-by-step guide for its implementation.

5.1. Use case definition

Use cases within the C-ITS domain undergo extensive scrutiny [58, 21,26,62]. Fig. 13 illustrates a common deployment scenario for C-ITS stations: vehicles communicate with Road Side Units (RSUs) using the Exchange of ITS-S Messages (EIM) and Road Works Warning (RWW) or Sharing of Kinematic Data (SKD) profiles. In turn, RSUs relay this information to the backend systems using the RSU-to-Backend (R2B) protocols. To ensure the integrity and confidentiality of these communications, all interactions are secured through the implementation of the

[14] The actual categories in Location and Sensitivity are highly context-dependent.

[15] See, e.g., https://cpoc.jrc.ec.europa.eu/index.html.

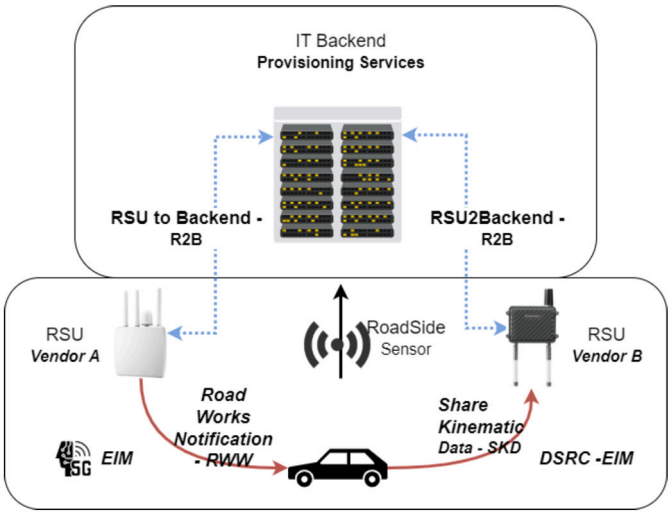

Fig. 13. The deployment of the C-ITS use case.

Audit Trail and Node Authentication (ATNA) profile. We focus on two profile-specific use cases: Road Works Warning (RWW) and Sharing of Kinematic Data (SKD). These profile use cases involve the exchange of data structures, facilitated either through Dedicated Short-Range Communication (DSRC) [29] or via 5G [29], as indicated by the red arrows in Fig. 13. However, this dual approach creates interoperability challenges, which our methodology aims to resolve.

An important aspect of interoperability we address is the lack of consistency in both syntactic and semantic communication with backend services, denoted by the blue arrows in Fig. 13. To ensure a comprehensive approach to security, we establish a baseline security profile that serves as a fundamental requirement for all subsequent profiles, aligning with the principle of security-by-design. The establishment of security-by-design precedes these operational procedures, facilitated by the provision of the newly created profiles (see section 4.3.1). The enabled interoperability and the established governance framework integrate existing ETSI standards and use cases with our methodology, ensuring compliance with established protocols, while incorporating security and governance into a standardized approach for solution architecture design.

5.2. Profile dependencies and grouping

Given that security-by-design is a legal requirement in critical infrastructures, within IHE security-related profiles are integral to any solution. This is achieved by grouping them with other functional profile, allowing these security profiles to be reused across different use cases without duplicating their definitions. This approach ensures that each profile can evolve independently while maintaining consistency. For example, the ATNA profile, which provides core security capabilities such as authentication and audit trails, must be grouped with any other operational profile. This makes ATNA a foundational building block across all configurations.

The profile dependencies and grouping rules are shown in Fig. 14. The diagram should be read from bottom to top, where the leaf nodes represent specific business use cases. For instance, if a project requires a motorway operator to handle only CAM messages related to vehicle movement, the architect would select the SKD profile. SDK requires the EIM profile for transport, which in turn depend on ATNA or secure communication and audit logging. These selected profiles collectively form the *solution architecture*.

The architect creates solution architectures using the IHE methodology by analyzing bottom-up the tree in Fig. 14 and matching the C-ITS use case with one or more content profiles (the leafs), following the

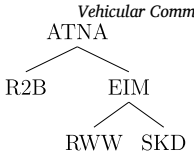

Fig. 14. Profile dependencies in the C-ITS domain.

grouping rules. In our specific C-ITS use case focused on issuing advance road works warnings, the architect would select the RWW profile, which is designed for that business function. However, RWW requires the EIM transport profile to define how messages are transmitted, and EIM, in turn, depends on the ATNA profile to provide baseline security. This dependency chain is clearly visualized in Fig. 15, illustrating how each layer builds upon the other to form a coherent, standards-based solution architecture. Each profile in the grouping adds specific capabilities to the final message format. In the CAM message example, EIM specifies the ITS PDU Header and key data fields such as Cooperative Awareness and Generation Time. SKD, which groups with EIM, enriches the message further by defining kinematic values in containers like SituationContainer. ATNA then secures the message by defining fields within the Security section. Similar logic applies to DENM messages. EIM sets the base structure including the header and general container, RWW defines the event-specific values (e.g., ManagementContainer), and ATNA ensures the message is protected through cryptographic and audit features.

5.3. Architecture-based profile dissection

In this section, the designed methodology is instantiated to facilitate secure deployment of the road side units (RSUs) supporting bidirectional Vehicle-to-Infrastructure (V2I) communications. We begin by defining the use case in Example 5.3:

Example 5.3 *(RSU deployment use case)*. A motorway operator aims to contribute to C-ITS by proactively transmitting information about road works to vehicles.

Fig. 12 outlines the methodology as a procedure that starts with a selection of grouping profiles out of those devised in Section 4.3.1. Initially, the architect identifies the content profiles that align with the defined use case. For example, the RWW profile encapsulates the use case: *"The road infrastructure operator is aware of road works on the motorway. The operator knows the lane, the geolocation, and the duration"*, which mirrors Example 5.3. According to RWW's grouping rules, the EIM profile is required, which in turn necessitates grouping with ATNA, as illustrated in Fig. 14. This forms the initial set $\mathcal{P}$ ={RWW,EIM,ATNA}

The next step involves dissecting each profile to pre-fill the RAMI 4.0 architecture layers. RWW primarily defines the semantics of the information exchanged by the RSU, targeting the Information layer (refer to Table 2). As it pertains solely to the RSU, the applicable column is *Field Device*. Since RWW offers no alternatives, the Type/Maintenance row does not present any variability points. Similarly, the dissection of EIM and ATNA follows the same principles set in Section 4.4, with options mapped in the Type/Maintenance row, inclusive of audits for each transaction, as mandated by the grouping rules of each profile. In essence, Table 2 represents two condensed $\mathcal{M}$ matrices, corresponding to the Communication and Information layers, respectively.

For each RAMI 4.0 layer, we first identify the assets and populate the $\mathcal{M}$ matrices accordingly. Each entry $m_{i,j}$ in the matrix $\mathcal{M}$ is then associated with a taxonomy $t_{k,a}$. For the sake of readability, we adopt the default SDLC outlined in the RMIAS specifications and provide the taxonomy for the RWW profile. Given that the road work messaging

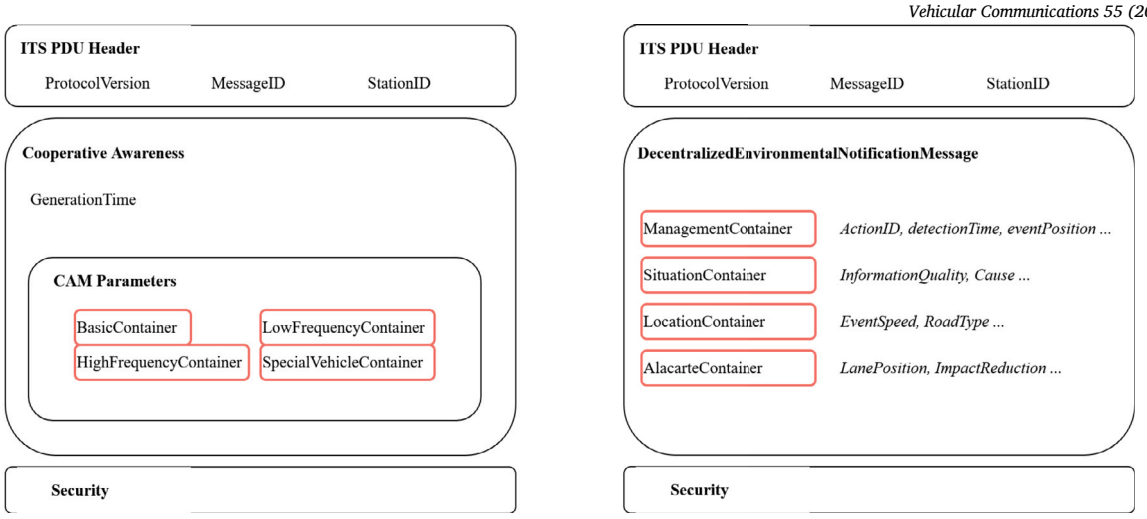

Fig. 15. How profile *grouping* works: Fig. 15a shows an excerpt of a CAM, as per [28]. The structure and the ITS PDU Header is defined by the EIM profile, the circled containers are defined by the content profiles, e.g., SKD, RWW, while the security box is provided by ATNA. Similarly, Fig. 15b shows another excerpt of the structure of a decentralized environmental notification message (DENM) and its groupings.

Table 2
Information and Communication layers superimposed after dissecting RWW, EIM and ATNA (empty Hierarchy columns are not shown).

Life Cycle & Value Stream	Field Device
Type/Development	(Information) RWW: Volume 1 and Volume 2 versioned C-ITS domain specifications. (Communication) EIM: Volume 1 and 2, ATNA Volume 1 and 2
Type/Maintenance	(Information) RWW: Further constraints and variability points. (Communication) EIM: C-ITS-04 is suppressed. ATNA: C-ITS-02 is suppressed, audit definitions per profile
Instance/Production	(Information, Communication) EIM, ATNA, RWW: Vendor A's product operational information
Instance/Maintenance	(Information, Communication) EIM, ATNA, RWW: Vendor A's product manual

specification is publicly available through ETSI, our focus lies on protecting information during the engineering phase, which may include sensitive infrastructural business details. As such, we establish the following taxonomy ($\mathcal{T}$ set):

1. $t_{1,\text{RWW}}$:=<`Form:` Electronic, `State:` Creation, `Sensitivity:` public, `Location:` restricted >
2. $t_{2,\text{RWW}}$:=<`Form:` Electronic, `State:` Transmission, `Sensitivity:` public, `Location:` unrestricted >

The process of message creation occurs within a restricted environment, typically the operator's internal IT data center. Conversely, during transmission, messages become publicly available as part of the DENM standard. Accordingly, we set the security goals as follows: $g_{1,1,\text{RWW}}$:=<Confidentiality> (during the creation phase) and $g_{2,2,\text{RWW}}$:=<Availability> (during the transmission to vehicles). These security goals collectively form the set $\mathcal{G}$.

5.4. Eliciting security requirements

Once the profiling and dissection stages are complete, the methodology proceeds to devise countermeasures that address the identified security goals. For instance, ensuring confidentiality involves adopting secure communication channels like Transport Layer Security (TLS), which prevents malicious interception of messages and their creation process. Achieving availability entails using reliable channels such as queuing mechanisms or reactive streams.

To determine the appropriate set of countermeasures, we assess their availability within the profiles in $\mathcal{P}$ or the IHE profiles in the technical framework. For instance, TLS is defined by the ATNA profile, while queuing mechanisms are not specified. In such scenarios, use cases identified by applying RMIAS are marked and incorporated into a profile, which is then submitted for consideration in the next standardization cycle. This iterative procedure continues according to the algorithm in Fig. 12.

Similarly, RMIAS is applied to the EIM and the ATNA profiles. Here, no additional security requirements are found, as the grouping rule EIM → ATNA already enforces the confidentiality requirement. Thus, the process continues with the designation c_1 :=< ETSI TS 102 940>.

Since queuing mechanisms are not included in any profile within the C-ITS domain, a new temporary profile, denoted as π', is created, and the dissection process is restarted. This adjustment does not impact any other layer ($m_{i,j}$) in the architecture. Consequently, all necessary countermeasures are now accounted for in all profiles, with TLS specified in the ATNA profile and queuing mechanisms included in π'. With this, the target solution architecture is defined as <RWW, EIM, ATNA, π' >, effectively concluding the process specified in the methodology.

Upon completing the methodology implementation, the RAMI 4.0 matrix is populated with the technical representation of the solution architecture, alongside the database of specifications overseen by the new IHE C-ITS domain. This first version of the solution architecture is refined by incorporating details about devices, RSUs, SCADA servers, and sensors into the *Asset* and *Integration* layers. The use case is integrated into the *Functional* layer for the respective assets, while the *Business* layer is enriched with legal and financial information. With this, security countermeasures are mapped to the asset lifecycle, security goals (e.g., confidentiality, integrity, availability) are aligned with the system components, whereas cryptographic and compliance measures (e.g., TLS,

audit trails) are automatically assigned to the appropriate architectural layers.

This proof-of-concept use case demonstrates that the methodology is feasible and scalable by: successfully deploying RSUs with predefined security and communication profiles; structuring governance around technical and planning committees, ensuring continuous adaptation to evolving standards and regulations; and reducing the risk of vendor and standards lock-in by maintaining an architecture that can integrate new security measures without breaking compatibility. The use case illustrates that the methodology supports both legacy (DSRC) and emerging communication protocols within the same security framework. Such adaptability is crucial in future-proofing the security model against evolving threats, facilitating cross-border interoperability through regulatory alignment, as well as supporting AI-driven security enhancements, such as automated threat detection and compliance monitoring.

5.5. Use-case discussion

The presented use case focused on a realistic C-ITS deployment where a motorway operator broadcasts road works warnings (RWW) to approaching vehicles via CAM/DENM messages. This scenario requires not only message transport and content standardization, but also secure back-end integration and automated compliance with audit and policy rules.

When analyzed against other architectural or non-architectural approaches, we note some important benefits of the proposed method. The integration of the ATNA profile ensures mutual authentication and audit trails between RSUs and back-end systems, fulfilling the legal mandates of security-by-design in critical infrastructure. *Traditional or ad-hoc approaches lack this preemptive security anchoring.* The use of EIM for message transport and RWW for content semantics ensures that both the sender (infrastructure) and the receiver (vehicle) interpret the message consistently. *Compared to non-profile-based systems, this eliminates discrepancies in data interpretation across vendors or national deployments.* Each profile in the architecture represents a loosely coupled building block, reusable across different C-ITS deployments (e.g., RWW can be replaced with SKD without disrupting the rest of the architecture). *Centralized orchestration or risk-based approaches lack this composability*. From a grouping logic perspective, the modular profile structure means that if a new technology solution is to be introduced in the architecture (for example, if DSRC is replaced by 5G), only the transport profile (EIM) needs updating, without affecting the content profile (RWW) or the security layer (ATNA). *Ad-hoc or standard-only systems would require manual re-integration across all layers.* Finally, all transactions in the use case (e.g., C-ITS-01 to C-ITS-07) are predefined, logged, and validated through policy servers and the Audit Record Repository. This enables hands-off regulatory compliance and simplifies procurement. *Traditional approaches would require periodic manual reviews or custom-made validation tooling.*

Thus, the proposed architecture is not just theoretically robust, but is demonstrably superior in a practical deployment scenario. It enables the motorway operator to deploy scalable, secure, and interoperable V2I infrastructure with significantly reduced overhead, faster vendor onboarding, and long-term sustainability.

6. Discussion

6.1. Overview of contributions

A key novelty of the proposed methodology is its structured and iterative approach to profile selection, where use cases undergo rigorous evaluation by planning and technical committees before adoption. The implementation of the methodology highlighted several critical insights. First, the integration of an enterprise architecture framework significantly enhances the ability to maintain security-by-design throughout the lifecycle of C-ITS deployments. Second, fostering collaboration between standardization bodies, infrastructure providers, and technology vendors is essential to ensure interoperability while minimizing risks associated with standards lock-in. The approach also demonstrated that leveraging well-established security frameworks from other domains, such as the IHE's ATNA profile, provides a solid foundation for securing V2I communications.

In C-ITS, data plays a central role. Components like RSUs exchange messages with vehicles and, indirectly, with other components of the broader infrastructure. These data exchanges support a wide range of public services: smart cities can adjust traffic flows in real time; hospitals can coordinate emergency response; and fire brigades can optimize routing based on live road conditions. This high level of interdependence among infrastructures speaks of the importance of a coordinated and secure data-sharing framework. Our methodology directly supports these needs by integrating with diverse data sources, such as real-time traffic monitoring systems, V2X networks, road maintenance schedules, and cybersecurity tools like audit logs and anomaly detectors. The governance mechanism defines how the systems interoperate efficiently and without redundancy, and the use of standardized profiles acts as a unifying interface, encapsulating vendor-specific data-sharing models. This not only ensures interoperability, but also mitigates the risk of vendor or standards lock-in—facilitating scalable, future-proof infrastructure management.

Another important trait of the proposed governance model is that it is inherently adaptable to emerging C-ITS technologies and evolving security paradigms due to its architectural layering, modularity, and profile-based lifecycle management. As new technologies like 5G-V2X, AI-driven intrusion detection, or quantum-safe cryptography become relevant, the modular profiles can be extended or versioned to integrate new standards, interfaces, or security controls without disrupting the overall system architecture. For instance, a profile focused on RSU-to-Vehicle communication can be updated to support 5G NR sidelink modes while maintaining existing infrastructure elements. Moreover, the use of a reference architecture like RAMI 4.0 ensures that any new component, regardless of whether it emerges in the connectivity, processing, or application layer, can be consistently classified, governed, and validated. The governance model can also accommodate paradigm shifts such as zero-trust architectures or decentralized identity frameworks by embedding them into future profiles and aligning them with security goals defined through RMIAS. This extensibility positions the framework to act as a durable foundation for long-term C-ITS evolution.

While the methodology is inspired by structured, centralized coordination models such as IHE, we recognize that the C-ITS ecosystem is highly fragmented, encompassing diverse stakeholders across industry, governments, and regions. To address this, the proposed governance framework supports both centralized and federated operational modes. In federated mode, regional or national committees can assume the roles of the Planning and Technical Committees, managing integration profiles within their domains. Cross-domain interoperability can then be coordinated through minimal harmonization mechanisms, such as profile registries or peer-reviewed validation events, reducing the need for full-scale alignment. Additionally, Connect-a-thon-style events can be conducted as voluntary or bilateral validation exercises rather than mandatory industry-wide checkpoints. These adaptations enable phased adoption, encourage incremental buy-in from vendors, and lower the barrier to participation in interoperability governance. Future implementations may also explore decentralized governance models, leveraging, for e.g., blockchain-based audit trails or smart contracts to automate profile validation and update propagation, further reducing reliance on centralized oversight.

While not the primary focus, the proposed approach helps reduce the workload of experts and the need for expert oversight, lowering maintenance costs. The EA-based approach enhances expert collaboration by reducing unnecessary system-level discussions and abstracting technical dependencies, minimizing manual updates as standards evolve. By using

modular building blocks, it ensures that the system components adhere to predefined structures and best practices without the need to redefine security policies from scratch each time. This streamlines the design of security policy, promoting consistency across components and eliminating redundant efforts. Furthermore, it enables a seamless integration of emerging technologies like 5G and AI-driven security without requiring fundamental architectural changes. Finally, IHE compliance validation through Connect-a-thons ensures that security policies and interoperability requirements are met before deployment, shifting the focus from post-deployment troubleshooting to proactive security enforcement.

6.2. Limitations and future work

Despite the introduced novelties and contributions, certain limitations in our approach still persist. One major constraint comes from the lack of a universally accepted regulatory framework for C-ITS security in Europe, which complicates efforts to standardize security requirements. Furthermore, reliance on existing standards meant that some aspects of interoperability had to be addressed through domain-specific adaptations, which may pose additional requirements for applicability in heterogeneous C-ITS ecosystems. Finally, while security-by-design principles were embedded throughout the methodology, additional processing overhead introduced by cryptographic mechanisms and audit trails may affect system performance. Thus, further research is needed on optimizing security measures without compromising real-time communication efficiency.

To validate the real impact of our work, we envisage validation through pilot deployments with a real-world C-ITS system, as well as simulation-based tests to quantify the actual security, interoperability, and efficiency gains. Future research will refine the governance model to better align with international regulations. As connected vehicle technologies evolve, adaptive security models shall dynamically address emerging threats while ensuring interoperability. In this context, the long-term viability of standards-based security frameworks requires investigation, especially with advancements in communication infrastructures like 6G and edge computing. Future iterations of the methodology will explore hybrid security approaches, integrating traditional cryptographic mechanisms with decentralized trust models, such as blockchain-based identity verification for C-ITS components. Additionally, AI and ML will be used to detect compliance violations and predict security breaches before they occur [3].

Governance and interoperability in C-ITS extend beyond technical and regulatory concerns. Economic-based mechanisms, such as auctions, have been successfully applied in other domains to allocate and manage shared resources efficiently [40,66]. The Federal Communications Commission (FCC) spectrum auctions, for example, enforce interoperability by compelling service providers with differing standards to conform to common operational frameworks [17]. In the context of C-ITS, similar auction-based mechanisms have been proposed for flexible route planning [63]. It would be worthwhile investigating the potential of such mechanisms for enhancing security, interoperability, and sustainability. For example, auctions could be designed to encourage standard-compliant implementations, where vendors that adhere to strict interoperability standards could gain preferential access to public procurement contracts, fostering wider adoption of secure-by-design architectures. Furthermore, an auction-based approach could regulate the allocation of communication channels in V2X interactions, preventing interference, and ensuring fair distribution among service providers. Thus, the system could balance economic incentives with interoperability requirements, promoting both competition and adherence to security-by-design principles.

7. Conclusions

In this paper, we have presented a governance-driven methodology for securing Cooperative Intelligent Transport Systems (C-ITS) through an enterprise architecture-based approach. Given the complex landscape of C-ITS, where multiple standards, organizations, and regulatory frameworks converge, ensuring security-by-design while maintaining interoperability remains a significant challenge. Our proposed framework leverages methodologies established in other critical sectors, such as healthcare and energy, to provide a structured and adaptable solution that aligns with existing governance models while addressing security concerns.

A central contribution of this work is the combination of modular, standards-based profiling with an architecture-driven approach to security. Drawing on well-established enterprise architectures principles, particularly the Reference Model for Information Assurance and Security (RMIAS) and the RAMI 4.0 framework, we have demonstrated how security countermeasures can be systematically embedded at design time. This proactive strategy allows architects and security professionals to define and apply consistent security policies early in the development lifecycle, rather than retrofitting them later. Beyond enhancing resilience against evolving threats, our methodology contributes to the reduction of expert workload, promotes long-term interoperability, and mitigates standard lock-in, enabling sustainable, scalable, and secure deployments of C-ITS infrastructures.

CRediT authorship contribution statement

Tanja Pavleska: Writing – review & editing, Writing – original draft, Validation, Supervision, Resources, Methodology, Investigation, Funding acquisition, Conceptualization. **Massimiliano Masi:** Writing – review & editing, Visualization, Software, Project administration, Methodology, Investigation, Formal analysis, Data curation. **Giovanni Paolo Sellitto:** Writing – review & editing, Writing – original draft, Visualization, Supervision, Methodology, Conceptualization. **Helder Aranha:** Writing – review & editing, Visualization, Validation, Supervision, Methodology.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This work was supported by the Slovenian Research Agency, Grant No. P2-0037.

Data availability

Data will be made available on request.

References

[1] 5GAA, MEC for automotive in multi-operator scenarios, Technical report, 5GAA, https://5gaa.org/content/uploads/2021/03/5GAA_A-200150_MEC4AUTO_Task2_TR_MEC-for-Automotive-in-Multi-Operator-Scenarios.pdf, 2021.

[2] Hezam Akram Abdulghani, Niels Alexander Nijdam, Anastasija Collen, Dimitri Konstantas, A study on security and privacy guidelines, countermeasures, threats: IoT data at rest perspective, Multidisciplinary Digital Publishing Institute, 2019.

[3] Lampis Alevizos, Automated cybersecurity compliance and threat response using AI, blockchain and smart contracts, Int. J. Inf. Technol. 17 (2) (2025) 767–781, https://doi.org/10.1007/s41870-024-02324-9.

[4] Helder Aranha, Massimiliano Masi, Tanja Pavleska, Giovanni Paolo Sellitto, Enabling security-by-design in smart grids: an architecture-based approach, in: 15th European Dependable Computing Conference, EDCC 2019, Naples, Italy, September 17-20, 2019 Naples, 2019, pp. 177–179, IEEE.

[5] Helder Aranha, Massimiliano Masi, Tanja Pavleska, Giovanni Paolo Sellitto, Securing mobile e-health environments by design: a holistic architectural approach, in: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2019, Barcelona, Spain, October 21-23, 2019 Barcelona, IEEE, 2019, pp. 1–6.

[6] Meriem Benyahya, Anastasija Collen, Sotiria Kechagia, Niels Alexander Nijdam, Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments, Elsevier BV, 2022.
[7] CEF, Edelivery - exchange data and documents securely and reliably, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery, 2020.
[8] A. Chattopadhyay, K. Lam, Y. Tavva, Autonomous vehicle: security by design, IEEE Trans. Intell. Transp. Syst. 1 (1) (2020) 1–15.
[9] Yulia Cherdantseva, Jeremy Hilton, Omer F. Rana, Wendy Ivins, A multifaceted evaluation of the reference model of information assurance & security, Comput. Secur. 63 (2016) 45–66, https://doi.org/10.1016/j.cose.2016.09.007.
[10] E.U. Commission, Cooperative, connected and automated mobility (ccam), https://ec.europa.eu/transport/themes/its/c-its_en, 2020.
[11] European Commission, Commission staff working document: Eu road safety policy framework 2021-2030 - next steps towards vision zero, Technical report, European Commission, Jun 2019.
[12] The European Commission, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the union, https://eur-lex.europa.eu/eli/dir/2016/1148/oj, 2016.
[13] A.I. Elkhawas, M.A. Azer, Security perspective in rami 4.0, in: 2018 13th International Conference on Computer Engineering and Systems (ICCES), IEEE, Cairo, 2018, pp. 151–156.
[14] Adriano Koshiyama, et al., Towards algorithm auditing: managing legal, ethical and technological risks of AI, ml and associated algorithms, R. Soc. (2024), https://doi.org/10.1098/rsos.230859.
[15] Checkoway Stephen, et al., Comprehensive experimental analyses of automotive attack surfaces, in: Proceedings of the 20th USENIX Conference on Security, SEC'11, USENIX Association, USA, 2011, p. 6.
[16] Christian Vitale, et al., Caramel: results on a secure architecture for connected and autonomous vehicles detecting GPS spoofing attacks, EURASIP J. Wirel. Commun. Netw. (2021), https://doi.org/10.1186/s13638-021-01971-x, Springer Nature.
[17] Evan Kwerel, et al., Economics at the fcc, 2016–2017: auction designs for spectrum repurposing and universal service subsidies, Rev. Ind. Organ. 51 (4)) (2017) 451–486, https://www.jstor.org/stable/48722400.
[18] F. Miao, et al., Transport layer security (tls) transport mapping for syslog, https://tools.ietf.org/html/rfc5425, 2009.
[19] G. Raja, et al., Energy-efficient end-to-end security for software-defined vehicular networks, IEEE Trans. Ind. Inform. (2021), https://doi.org/10.1109/TII.2020.3012166, https://www.semanticscholar.org/paper/2b6a9447f9ee13b71508d45caaee82cedd4d5d7a.
[20] Marion Gottschalk, et al., From integration profiles to interoperability testing for smart energy systems at connectathon energy, https://doi.org/10.3390/en11123375, 2018.
[21] Lu Meng, et al., C-its (cooperative intelligent transport systems) deployment in Europe-challenges and key findings, in: 25th ITS World Congress, 2018.
[22] P. Adolphs, et al., Reference architecture model industrie 4.0 din spec 91345:2016–04, Technical report, DIN, 2016.
[23] Takahito Yoshizawa, et al., A survey of security and privacy issues in v2x communication systems, ACM Comput. Surv. (2022), https://doi.org/10.1145/3558052, Association for Computing Machinery.
[24] Tanja Pavleska, et al., Cybersecurity evaluation of enterprise architectures: the e-SENS case, in: PoEM 2019, Proceedings, Luxembourg, November 27-29, 2019, in: Lecture Notes in Business Information Processing, vol. 369, Springer, Cham, 2019, pp. 226–241.
[25] Zeinab El-Rewini, et al., Cybersecurity challenges in vehicular communications, Veh. Commun. 23 (2020) 100214, https://doi.org/10.1016/j.vehcom.2019.100214, http://www.sciencedirect.com/science/article/pii/S221420961930261X.
[26] ETSI, ETSI TR 102 638 - v1.1.1, intelligent transport systems (its); vehicular communications; basic set of applications; definitions, Technical report, 2009, https://www.etsi.org/deliver/etsi_tr/102600_102699/102638/01.01.01_60/tr_102638v010101p.pdf.
[27] ETSI, ETSI EN 392 665 V1.1.1, intelligent transport systems (its); security; communications architecture, Technical report, ETSI, 2010.
[28] ETSI, ETSI TS 102 637-2, intelligent transport systems (its); vehicular communications; basic set of applications; part 2: Specifications of cooeprative awareness basic service, Technical report, ETSI, 2011.
[29] ETSI, ETSI EN 302 663, intelligent transport systems (its); access layer specification for intelligent transport systems operating in the 5 GHz frequency band, Technical report, ETSI, 2012.
[30] ETSI, ETSI EN 302 637-3, intelligent transport systems (its); vehicular communications; basic set of applications; part 3: Specifications of decentralized environmental notification basic service, Technical report, ETSI, 2014.
[31] ETSI, ETSI TS 102 940 V1.3.1, intelligent transport systems (its); security; its communications security architecture and security management, Technical report, ETSI, 2018, https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf.
[32] Brian F.G. Fabrgue, Andrea Bogoni, Privacy and security concerns in the smart city, Multidisciplinary Digital Publishing Institute, 2023.
[33] German Federal Ministry for Economic Affairs and Standardization Administration of the P.R.C., Alignment report for reference architectural model for industrie 4.0/intelligent manufacturing system architecture Sino-German industrie 4.0/intelligent manufacturing standardisation sub-working group, Technical report, Apr 2018.
[34] Gerald Franzl, Marion Gottschalk, Richard Pasteka, The IES cookbook - enabling interoperability the IES way, Technical report, edition 0.8, IES Austria, 2019.
[35] Aurona Gerber, Pierre le Roux, Carike Kearney, Alta van der Merwe, The Zachman framework for enterprise architecture: an explanatory is theory, in: Marié Hattingh, et al. (Eds.), Responsible Design, Implementation and Use of Information and Communication Technology, Springer International Publishing, Cham, 2020, pp. 383–396.
[36] Rainer Gerhards, Rfc: the syslog protocol, Technical report, IETF, 2009, https://tools.ietf.org/html/rfc5424.
[37] Marion Gottschalk, Mathias Uslar, Christina Delfs, The Use Case and Smart Grid Architecture Model Approach the IEC 62559-2 Use Case Template and the SGAM Applied in Various Domains, Springer, Cham, 2017.
[38] Smart Grid Coordination Group, Smart grid information security, Technical report, CEN/CENELEC/ETSI, November 2012.
[39] The Open Group, The TOGAF® Standard, Version 9.2, The Open Group, 2020, https://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html.
[40] Francesco Guala, Building economic machines: the fcc auctions, Stud. Hist. Phil. Sci. A 32 (3) (2001) 453–477, https://doi.org/10.1016/S0039-3681(01)00008-5.
[41] WHO Guideline, Recommendations on digital interventions for health system strengthening, Technical report, World Health Organization, Jan 2019.
[42] Roland Heidel, Michael Hoffmeister, Martin Hankel, Udo Döbrich, The Reference Architecture Model RAMI 4.0 and the Industrie 4.0 Component, VDE Verlag, Berlin, Germany, 2019.
[43] HIMSS, What is interoperability, https://www.himss.org/previous-himss-interoperability-definitions, 2020.
[44] HL7, Saif architecture program, https://wiki.hl7.org/SAIF_Architecture_Program, 2020.
[45] IHE, IHE technical frameworks general introduction, Technical report, IHE, October 2019.
[46] IHE, Continuous development process, https://wiki.ihe.net/index.php/Continuous_Development_Process, 2020.
[47] IHE, Domains, https://www.ihe.net/ihe_domains/, Sep 2020.
[48] IHE, IHE it infrastructure technical framework, https://www.ihe.net/resources/technical_frameworks/#IT, Aug 2020.
[49] ITS International, Australia moves towards C-its systems, https://www.itsinternational.com/its10/news/australia-moves-towards-c-its-systems, 2020.
[50] ISO, SO/TS 21219-15:2016, intelligent transport systems — traffic and travel information (tti) via transport protocol experts group, generation 2 (tpeg2) — part 15: Traffic event compact (tpeg2-tec), Technical report, ISO, 2016, https://www.iso.org/standard/63116.html.
[51] P. Karkhanis, M.G.J.v.d. Brand, S. Rajkarnikar, Defining the C-its reference architecture, in: 2018 IEEE International Conference on Software Architecture Companion (ICSA-C), IEEE, Seattle, 2018, pp. 148–151.
[52] Brooke Lampe, Weizhi Meng, Intrusion detection in the automotive domain: a comprehensive review, IEEE Commun. Surv. Tutor. (2023), https://doi.org/10.1109/comst.2023.3309864, Institute of Electrical and Electronics Engineers.
[53] Massimiliano Masi, A formalisation of the IHE process - an open source implementation, 2020–2024, https://github.com/mascanc/MOSA2.
[54] OASIS, OASIS test assertions guidelines, Technical report, OASIS, 2013, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tag.
[55] Office of the Assistant Secretary for Research and Technology, Intelligent transportation systems, Joint Program Office, 2020, https://www.its.dot.gov/.
[56] Office of the National Coordinator HealthIT, Appendix i – sources of security standards and security patterns, https://www.healthit.gov/isa/appendix-i-sources-security-standards-and-security-patterns, 2020.
[57] Tanja Pavleska, Helder Aranha, Massimiliano Masi, Giovanni Paolo Sellitto, Drafting a cybersecurity framework profile for smart grids in EU: a goal-based methodology, in: Simona Bernardi, et al. (Eds.), Dependable Computing - EDCC 2020 Workshops, Springer International Publishing, Cham, 2020, pp. 143–155.
[58] C-ITS Platform, Final report, Technical report, 2016, https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf.
[59] Pasika Ranaweera, Anca Delia Jurcut, Madhusanka Liyanage, Mec-enabled 5G use cases: a survey on security vulnerabilities and countermeasures, ACM (2021), https://doi.org/10.1145/3474552.
[60] Ramin Ranjbar Motlagh, Omid Ameri Sianaki, Himanshu Shee, A survey on cooperative intelligent transportation systems (C-its): opportunities and challenges, in: Leonard Barolli (Ed.), Complex, Intelligent and Software Intensive Systems, Springer Nature Switzerland, Cham, 2024, pp. 253–260.
[61] S. Bradner, Key words for use in rfcs to indicate requirement levels, Technical report, IETF, 1997, https://tools.ietf.org/html/rfc2119.
[62] José Santa, Fernando Pereniguez-Garcia, Antonio Moragón, Antonio Skarmeta, Experimental evaluation of cam and denm messaging services in vehicular communications, Transp. Res., Part C, Emerg. Technol. 46 (2014) 98–120, https://doi.org/10.1016/j.trc.2014.05.006.
[63] Sergey Satunin, Eduard Babkin, A multi-agent approach to intelligent transportation systems modeling with combinatorial auctions, Expert Syst. Appl. 41 (15) (2014) 6622–6633, https://doi.org/10.1016/j.eswa.2014.05.015.

[64] Ovidiu Vermesan, Jol Bacquet, Distributed intelligence at the edge and human machine-to-machine cooperation, in: Next Generation Internet of Things, 2018.

[65] Y. Dajsuren, Defining architecture framework for automotive systems, in: Y. Dajsuren, M. van den Brand (Eds.), Automotive Systems and Software Engineering, vol. 1, 2019, pp. 141–168.

[66] Sharrukh Zaman, Daniel Grosu, A combinatorial auction-based mechanism for dynamic vm provisioning and allocation in clouds, IEEE Trans. Cloud Comput. 1 (2) (2013) 129–141, https://doi.org/10.1109/TCC.2013.9.