TÜV AUSTRIA

WhitePaper

Figure: Shutterstock, © Yaran

New Approaches for Intelligent Transport Systems Security

Cyber-Security Reference Architecture

T · · Systems ·

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY

NOKIA

ASFINAG

universität wien

swarco

New Approaches for Intelligent Transport Systems Security

Cyber-Security Reference Architecture

Vienna, 12/03/2020

CySiVuS Consortium

Arndt Bonitz
Thomas Doms
Markus Hofer
Carina Kloibhofer
Martin Latzenhofer
Klaus Pollhammer
Thomas Raab
Stefan Ruehrup
Erich Schweighofer
Edvin Spahovic
Tom Vogt
Heinz Weiskirchner
Jakob Zanol

TÜV AUSTRIA Group, AIT Austrian Institute of Technology GmbH, T-Systems Austria GmbH, Swarco Futurit Verkehrssignalsysteme GmbH, ASFINAG Maut Service GmbH, Universität Wien - Arbeitsgruppe Rechtsinformatik, Nokia Solutions and Networks Österreich GmbH

Imprint

Abstract

ITS, connected automated driving require a cyber-secure digital information exchange

Intelligent Transport Systems (ITS) are an increasingly important factor for future mobility, especially in combination with automated driving. The increase of automated driving functions implies that more decisions are made by machines instead of human drivers. Driving decisions will rely on machine perception of the environment and digital information. This digitalisation transformation also involves infrastructure in the form of digital maps, digital road signs, information about environmental situations, traffic information and so on. Information is conveyed from the infrastructure to vehicles via communication interfaces, leading to a complex and interconnected system. As an unwanted side-effect, these new interfaces carry the risk of cyber-attacks, the effects of which cannot be neglected.

A reference architecture captures all stakeholders, components, data flows, and service requirements

In order to approach cyber-security in the complex environment of Intelligent Transport Systems, we propose a reference architecture that captures all the stakeholders involved, the corresponding data exchange, as well as the cyber-security requirements. We also consider legal implications, reflecting societal and governmental principles. The objective of this white paper is to present this reference architecture and provide a modelling methodology for the identification of important ITS elements as a fundamental basis for further security analyses. The modelling process is based on ArchiMate, a suitable architecture modelling language, where implications of decisions and changes can be evaluated from a stakeholder perspective. ArchiMate contains an extensive vocabulary that covers most areas of an enterprise architecture, i.e., strategy, motivation, business, application and technology.

This reference architecture for cyber-secure road and traffic infrastructure has been developed in the CySiVuS project (Cyber-Security for Transport Infrastructure- and Road Operators) of the Austrian security research program KIRAS, funded by the Austrian Research Promotion Agency (FFG). The CySiVuS project was carried out with the participation of the practitioners Austrian Federal Ministry of the Interior (BMI) and Austrian Federal Ministry of Defence (BMLV).

Content

1 Introduction

An interconnected transport system requires digitalisation

In the future, our transport systems will provide mobility as a service, with different choices for personal mobility, offering seamless and intermodal transport. Road transport and especially connected and automated driving is seen as an important part of this mobility concept. In this context, connected and automated vehicles are embedded into an overarching transport system which is characterized by an interconnection of intelligent and semi-automated or fully automated vehicles with a digital road infrastructure. Since vehicles are becoming increasingly automated, traffic management and control are also using more and more digital elements that can be understood by machines, such as digital road works warnings. In the future, all visual traffic signs could be complemented by their digital equivalents, such as digital traffic messages or speed limits transmitted via communication technologies. While the automated vehicle perceives its environment (including lane markings) via on-board sensors, it may in the future rely fully on digital information about hazardous locations or regulations on the road network.

Safety and Security are essential

Connected and automated vehicles as well as infrastructure elements have several interfaces where cyber-security is an issue that needs to be addressed. Manipulation, access to sensitive information, as well as focused and highly specialized cyber-attacks are just some of the threats that require increasing attention to maintain IT security, functional safety of vehicles, and the availability of infrastructure. Therefore, reliability and legal assurance of systems are becoming a key challenge for society and the economy.

Moreover, cyber-security, data protection and privacy are creating new challenges for connected and automated vehicles, as well as for cooperative roadside infrastructure. In order to operate safely, vehicles have to be able to obtain an accurate picture of their environment. This assessment of the environment relies on sensor input and information provided by roadside infrastructure or backend systems. As an example, road lane markings and obstacles are detected by on-board sensors, while road works warnings and speed limits might be received by communication technologies. The integrity of this data exchange by roadside infrastructure and vehicles is an essential prerequisite for automated driving, since driving decisions are made solely or partially by a machine. Cyber-security is crucial to make these technologies safe, secure and readily available to society.

Cyber-security reference architecture addresses a cyber-secure ITS

Based on forecasts of the future relevance of cooperative roadside infrastructures for automated driving, the CySiVuS project (Cyber-Security for Transport Infrastructure- and Road Operators) of the Austrian security research program KIRAS focused in particular on the identification of functional and structural requirements that are necessary for the cyber-secure operation of the infrastructure. In addition to the identification of potential threats and attack vectors, two key issues are of particular interest: First, a reference architecture has been developed, which helps to structure the relevant elements of use cases for connected and automated driving. Second, initiatives for further development in the future have been considered. This white paper is intended to provide a first insight into the solutions and the thinking behind them.

1.1 State of the art

ITS and its characteristics

Intelligent Transport Systems integrate telecommunications, electronics and information technologies with transport engineering, in order to plan, design, operate, maintain and manage transport systems [15]. ITSs are characterised by an interconnection of several systems using several information and communication technologies. Therefore, a unified model for ITS does not exist so far. However, the components that can make up an Intelligent Transport System are well known [1]. An exemplary overview of these components and their communication paths is given in Figure 1. The following infrastructure components are the main ones used for road traffic control and traffic information:

- All essential data collected by road operators converges in traffic control centres. Here, it is also possible for operators to intervene manually in traffic control.
- Sensors provide traffic and environmental data. This data is used to determine the traffic situation and environmental conditions (e.g., traffic volumes, speed averages, road surface temperature, fog).
- Visual displays are used to inform road users and to announce speed limits and other regulations.
- Roadside ITS Stations (R-ITS-S) are used to exchange data with vehicles. Road works warnings and other events, in-vehicle signage, etc. are transmitted to vehicles via short range communication technology.
- External interfaces are used for data exchange with other traffic centres or other service providers such as navigation services, weather services, etc. Data is both received (e.g., weather data) and transmitted (e.g., traffic messages, road works warnings).

In addition, there are other infrastructure components that are used for tunnel control (e.g., ventilation, control technology).

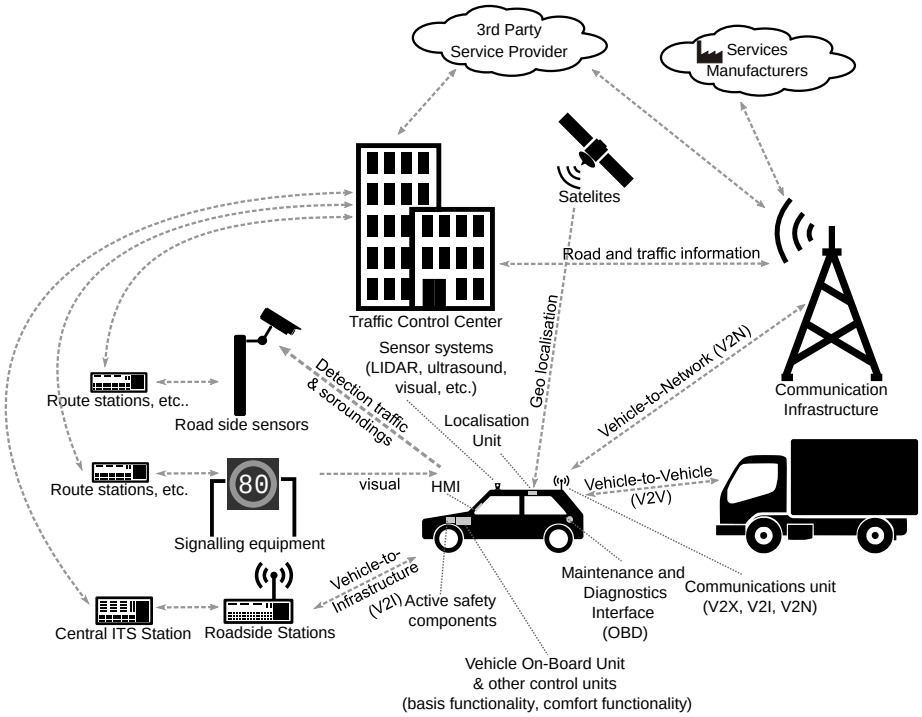


Figure 1: Overview of typical ITS components in road transport

Data flows and communication patterns

Data processed in this ecosystem can be divided into vehicles' on-board sensor data and communicated data. Sensors such as camera systems, RADAR (radio detection and ranging) or LiDAR (light detection and ranging) provide the vehicle with information about its immediate surroundings. Additional information can be exchanged through dedicated short-range communication (e.g., ITS-G5) or via a mobile communication network. Overall, one can differentiate the following major communication patterns [13]:

- V2V (Vehicle-to-Vehicle): Direct communication between two vehicles.
- V2I (Vehicle-to-Infrastructure): Communication between vehicles and the roadside infrastructure.
- V2P (Vehicle-to-Person): Both communication between a vehicle and a person's smartphone and pedestrian collision warning systems. Such systems currently exist as prototypes.
- V2N: Vehicle-to-Network: Broadcast and unicast communications between vehicles and some backend or central component in the network. This term is often used for the connection between vehicles and cloud services using mobile internet.

1.2 Scope and Definitions

The present document considers the modelling and assessment of cyber-security in ITS with a special focus on the interaction of connected and automated vehicles with the road infrastructure. The goal is to provide modelling tools to identify central elements of an ITS in order to perform security analyses.

Autonomous vs. automated driving

In the context of automated vehicles, the two terms "autonomous driving" and "automated driving" are often used synonymously, but there is a subtle difference: When driving autonomously, the vehicle has all the necessary information to perform a driving task while in the context of automated driving external data is needed. An autonomous vehicle can rely on its on-board sensors and no further information exchange necessary. In this mode, visual road signs can be perceived by image recognition and no digital map, in which road signs are registered in a digital form, is necessary. Autonomous vehicles have been featured in the DARPA (Defense Advanced Research Projects Agency) Challenges, last held in 2007 [14]. The term "automated driving" refers to the automation of driving functions such as lane keeping, distance control, speed control, or obstacle avoidance being performed by the vehicle. Depending on which functions the vehicle is able to perform automatically and under which conditions, different levels of automation have been classified: the so-called SAE levels [2].

ITS vs. C-ITS

A distinction needs to be made between the terms "Intelligent Transport System" and "Cooperative Intelligent Transport Systems" (C-ITS). Cooperative ITS is a subset of ITS that is characterised by V2V/V2I communication in a trusted domain. Thus, the term "C-ITS" is related to connected vehicles but not necessarily to automated vehicles. As an example, road works warnings transmitted via C-ITS to approaching vehicles can be made available to the driver, who reacts manually. Automated vehicles benefit even more from such digital data, because it can be a basis for driving functions that decelerate and change lanes to avoid closed lanes in the road works zone. For that reason, C-ITS is often considered in conjunction with automated driving.

Safety vs. security

In order to increase traffic safety and traffic efficiency, it is highly beneficial that automated vehicles exchange status data (e.g., position, speed and planned trajectory) reliably and cyber-securely. The susceptibility to cyber-attacks is increased by communication interfaces, data exchange and coordination between the elements in the traffic system, and there is thus also an increased need for comprehensive risk analyses and preventive protective measures. Therefore, the focus is on reliable communication between the components for the provision and use of traffic services. Particular attention should be paid to cyber-security for safety, i.e., the protection against targeted attacks on the "safety" of the system, as well as to the "security" for reliable operation, i.e., protection against attacks that disrupt or negatively influence the proper functioning of the system.

Methodology to describe an ITS cyber-security reference architecture

The core objective of the CySiVuS project was the creation of a reference architecture for the entire road transport system. Because of the multitude of ongoing parallel initiatives, and the technical, legal and social developments at different levels (vehicles, infrastructure, transport system) this is equivalent to a Sisyphean ("CySiVuS") task. A generally applicable methodological approach was chosen, which enables other projects or persons to integrate their own findings later after a certain familiarization with the syntax and semantics of the elements. The focus of this white paper is to present the methodology and - as exemplary use cases and as a form of verification - the application of this methodology for the use cases defined in the project. These use cases may not be complete per se but offer a sufficient representation of possible implementations. These should motivate other projects, groups or persons to formulate their use cases in the same way and thus successively expand the content of the reference architecture. Other architectures from other ongoing initiatives (e.g., ALP.Lab, DigiTrans) can be a further source for verifying the sustainability of the architecture if they are transferred to the reference architecture - i.e., if they are described by the architectural elements presented here.

1.3 Research Questions and Goals

The overriding problem comprises the following:

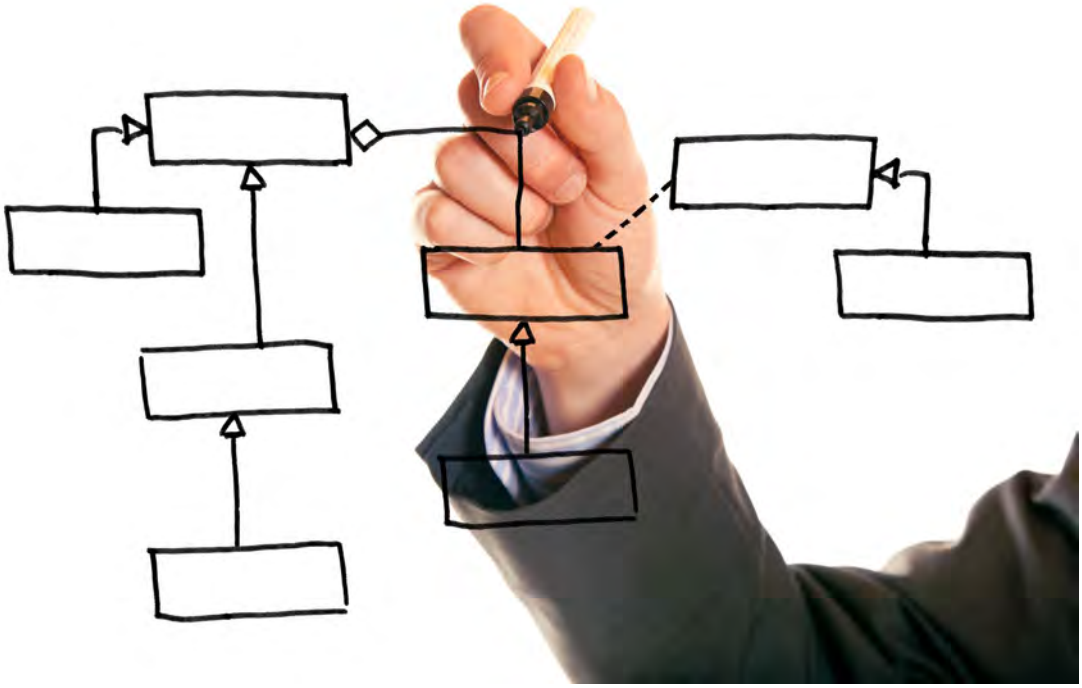
1. Development of a comprehensive reference architecture for the entire road transport system, primarily from a level that includes infrastructure components but abstracts from a detailed model of in-vehicle components.
2. Reduction of the inherent system complexity by an innovative architectural design and the un-bundling of this complexity into manageable parts.
3. Dealing with different perspectives such as technology, functionality, stakeholder's interests, etc.
4. Application of recognized and generally applicable methodical structures in order to later formulate new ideas, use cases and developments and integrate them into the reference architecture.
5. Creation of an open and extensible structure of the reference architecture.
6. Elaboration of explicit cyber-security measures and their interaction in the overall context for the automotive sector or for a C-ITS.

2 Methodology

2.1 ArchiMate

Cyber-security reference architecture is modelled in ArchiMate

The architecture is modelled in the open standard ArchiMate. It is a modelling language for the description of enterprise architectures. ArchiMate is used by many organizations in different industries worldwide. It is a sophisticated and complete architecture description standard that is aligned with the Open Group Architecture Framework (TOGAF) and is based on a grammar similar to natural language to describe what people or "things" do, and adds an external, service-oriented view of these activities [3].



2.2 Elements of the ArchiMate Meta-Model

In ArchiMate a model consists of elements and their relationships. Elements can be structural elements (the business actors, application components, and devices that display actual behavior; i.e., the “subjects” of activity), representing static aspects, as well as behavior elements (processes, functions, events, and services), which model dynamic aspect. The connections between these elements are modelled by relationship elements.

2.2.1 Structural Elements

ArchiMate active and passive structure elements and behavior elements

Figure 2 shows the meta-model, which lists the main types of structural and behavior elements available in ArchiMate. Active structure elements can be subdivided into internal active structure elements that realize behavior (e.g., the business etc.) and external active structure elements that expose this behavior to the environment (e.g., the interfaces). An interface provides an external view of the service provider and hides its internal structure.

Behavior elements represent the dynamic aspects of the enterprise. Like active structure elements, behavior elements can be subdivided into internal behavior elements and external behavior elements; e.g., the services that are exposed to the environment.

Passive structure elements can be accessed by elements which display behavior.

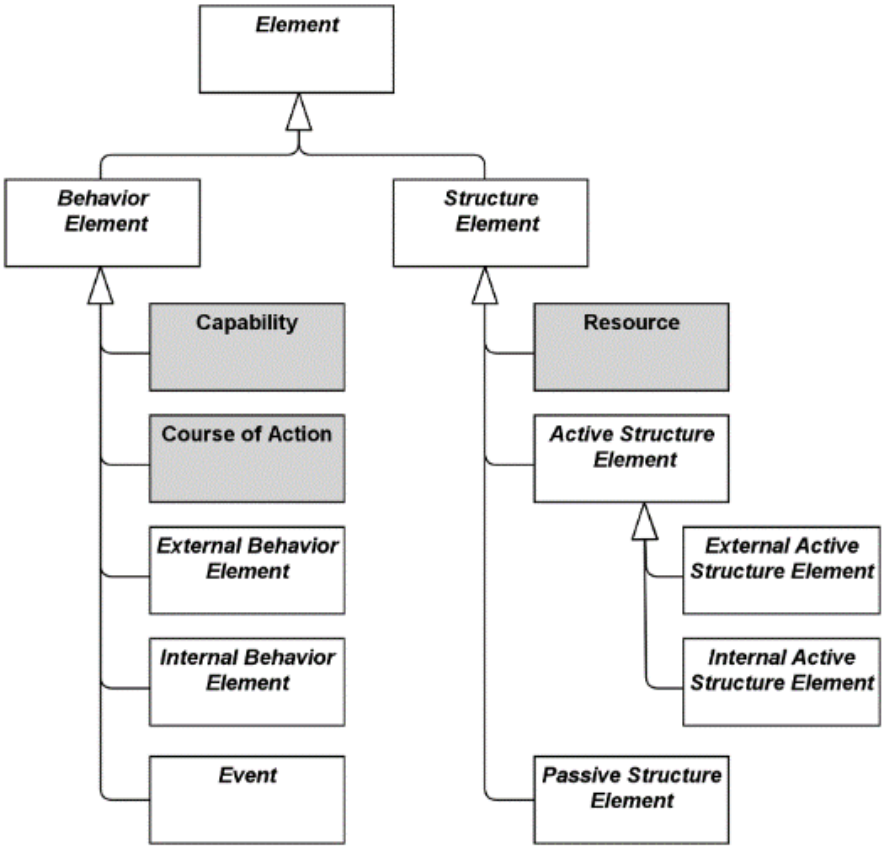


Figure 2: Structural meta-model

2.2.2 Relationships

Relationship types

ArchiMate allows elements to be connected in different ways. The type of these connections depends on the relationship of the respective interconnected architecture elements. ArchiMate divides communication elements into the following relationship types:

- **Structural relationships**: model the static construction or composition of concepts of the same or different types. These are divided into composition relationships, which indicate that an element consists of one or more other concepts and aggregation relationships that indicate that an element groups several other concepts. The assignment relationship expresses the allocation of responsibility, performance of behavior, or execution. The realization relationship indicates that an entity plays a critical role in the creation, achievement, sustenance, or operation of a more abstract entity [4].

- **Dependency relationships**: These relationships model how elements are used to support other elements. The serving relationship models that an element provides its functionality to another element. The access relationship models the ability of behavior and active structure elements to observe or act upon passive structure elements. The influence relationship models that an element affects the implementation or achievement of some motivation element.

- **Dynamic relationships**: Dynamic relationships are used to model behavioral dependencies between elements. The triggering relationship describes a temporal or causal relationship between elements. The flow relationship represents transfer from one element to another.

- **Other relationships**: The specialization relationship, association relationship and junction are relationships that do not fall into one of the above categories.

The graphical representation of these relations is shown in the meta-model in Figure 3.

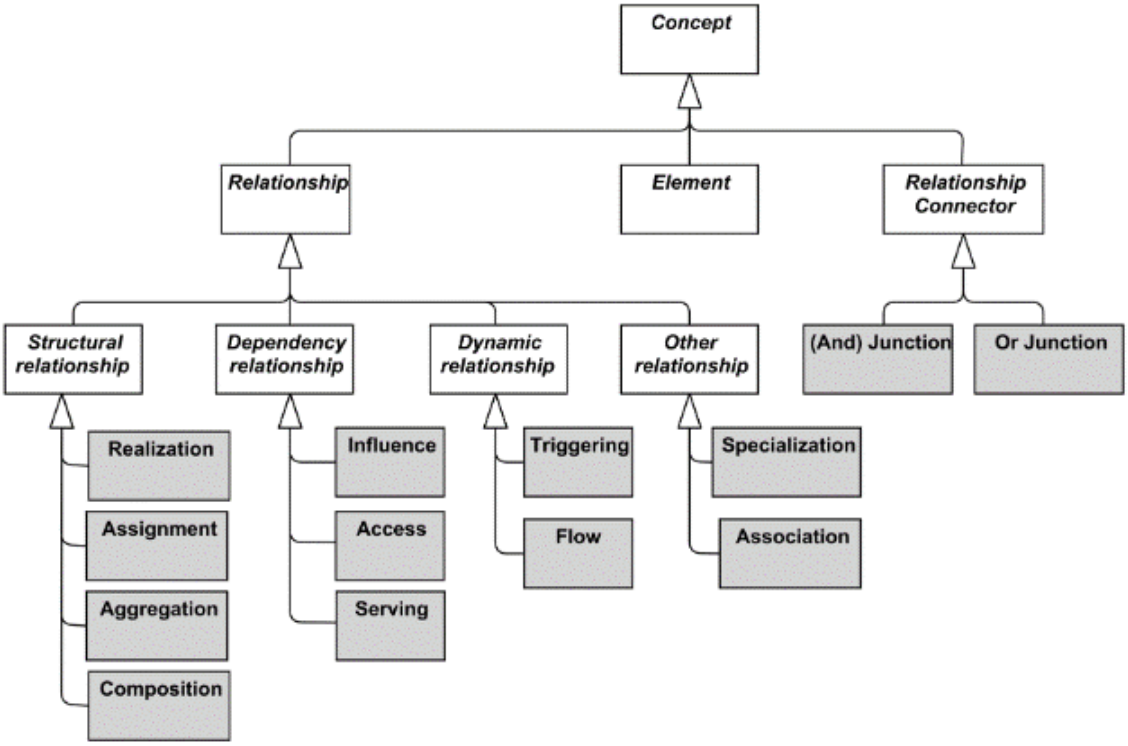


Figure 3: Communication Meta-Model

2.3 Threat Analysis

Security attributes

At the most abstract level, cyber-security has a small set of security targets or security attributes. The acronym CIA, which stands for the three terms **confidentiality** (access to information), **integrity** (trustworthiness and accurateness of information) and **availability** (reliable and constant access to information) is familiar to anyone in the field of cybersecurity. Furthermore, there are numerous extensions to it such as the Parkerian Hexad [3] which defines the additional three attributes **possession or control**, **authenticity** and **utility**, all three of which are relevant in the context of this Whitepaper.

- **Possession/Control** refers to loss of control over an asset which can not only enable other risks as the attacker has time to stage more attacks, but can also be a risk by itself, such as the misuse of resources even if no data is breached or service affected.
- **Authenticity** refers to the fact that the origin of data can be verified, such as authorship of documents or sender of messages.
- **Utility** refers to the use of an asset. Data scrambled or encrypted (e.g., ransomware) is still available, confidential and integral, but no longer useful. It is distinct from availability in the Parkerian Hexad while in standard CIA it is often expressed as an availability issue.

Security overlay in the cyber-security reference architecture

We add these security targets into the reference architecture as requirements using the security overlay convention of adding a «Sec» prefix, shown in Figure 4.

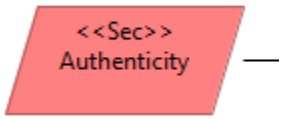


Figure 4: Security overlay example

The logic to identify applicable elements follows the method outlined in [11]:

- For every node or edge in the architecture model
- Identify the functionality of that element within the architecture
- Apply an FMEA [10] or a SWIFT [12] analysis to identify possible failures of that functionality
- Add the appropriate security requirement to the architecture, depending on the security requirement or requirements violated by the failure or failures.

Depending on the security level of the entity under consideration, every relevant or only the essential security attributes can be added to the model. Security attributes added consist of the prefix "«Sec»" and the name of the security attribute, such as "Authenticity" or "Confidentiality".

3 Scenarios

Diamond model structurally describes a possible scenario

In this chapter, two scenarios developed within the CySiVuS project are presented. These scenarios are modelled in detail in chapter 4. Both scenarios assume a cyber-attack on the intelligent transportation infrastructure. Both scenarios are described in a diagram, using the Diamond model [9] for intrusion analysis. This method shows in a concise way the core elements of an intrusion event: victim, adversary, infrastructure and capability of the adversary. In short, a Diamond expresses that an "adversary deploys a capability over some infrastructure against a victim" [9]. The relationship between the four elements forms a diamond, as depicted in Figure 5.

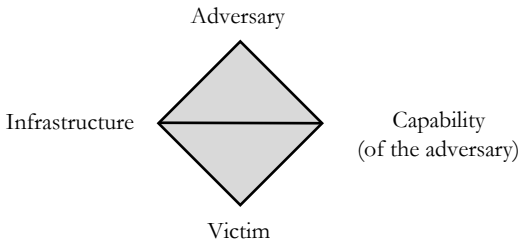


Figure 5: Diamond model

3.1 Scenario I

Scenario I: Malware infection of an ITS

In this scenario I we assume that components of an Intelligent Transport System are infected by malware, which leads to severe restriction or loss of system functionality. The infection is not targeted at the ITS; the damage occurs as collateral damage. An example is ransomware or crypto-mining malware, shown in Figure 6.

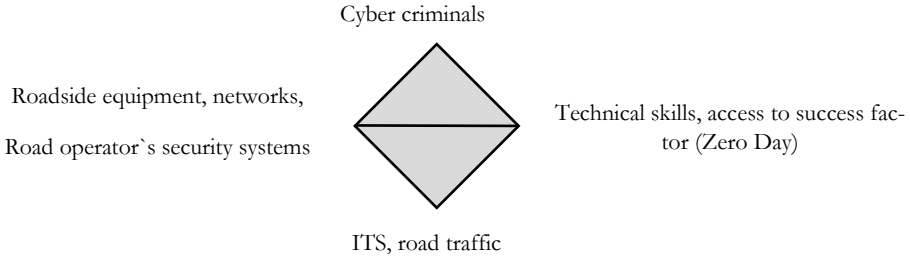


Figure 6: Diamond model for scenario I

Cyber criminals use malware (e.g., ransomware or crypto mining) to acquire money maliciously. If a component of an ITS is affected, it could have implications for further connected components. The malware is typically created by cyber criminals and provided with the appropriate capability. No malware is considered that is likely to be detected and removed by standard antivirus software.

3.2 Scenario II

In scenario II we assume that cyber terrorists or vandals use their detailed system knowledge to compromise the network that connects the variable message signs to the central controller. The respective diamond model is shown in Figure 7.

Scenario II: cyber terrorists compromise the network

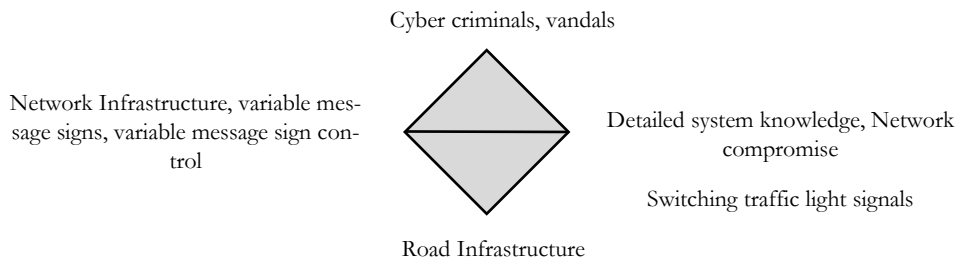


Figure 7: Diamond model for scenario II

4 Results

This chapter provides an overview of the reference architecture developed in the CySiVuS project. Due to its complexity, not all services can be shown in detail (see abstract for Gitlab repository for detailed information). Here the motivation layer of the considered stakeholders is described, the security overlay is explained, and two scenarios are shown in ArchiMate.

4.1 Reference Architecture

4.1.1 Motivation Layer

Motivation layer reflects the stakeholder's goals

The *motivation layer* is the basis for the development of the communication-specific architectural models. Different fundamental stakeholders can be identified. Each stakeholder has certain goals, which lead to certain requirements. The goals, drivers, results and requirements are relevant to our use cases and infrastructure considerations. Stakeholders may well have additional motivations beyond these.

Road User

Motivation of the road user

The *road user* is part of the society and has six main drivers as illustrated in Figure 8:

1. **Comfort**: An enhancement of comfort leads to a better satisfaction of the customer. In order to achieve this goal, easy and convenient access to the vehicle must be ensured.
2. **Privacy**: The road user is interested in maintaining and securing his privacy. In order to do this, it must be ensured that personal data is stored confidentially. Non-disclosure of personal data is ensured among other things by protection against unauthorized access.

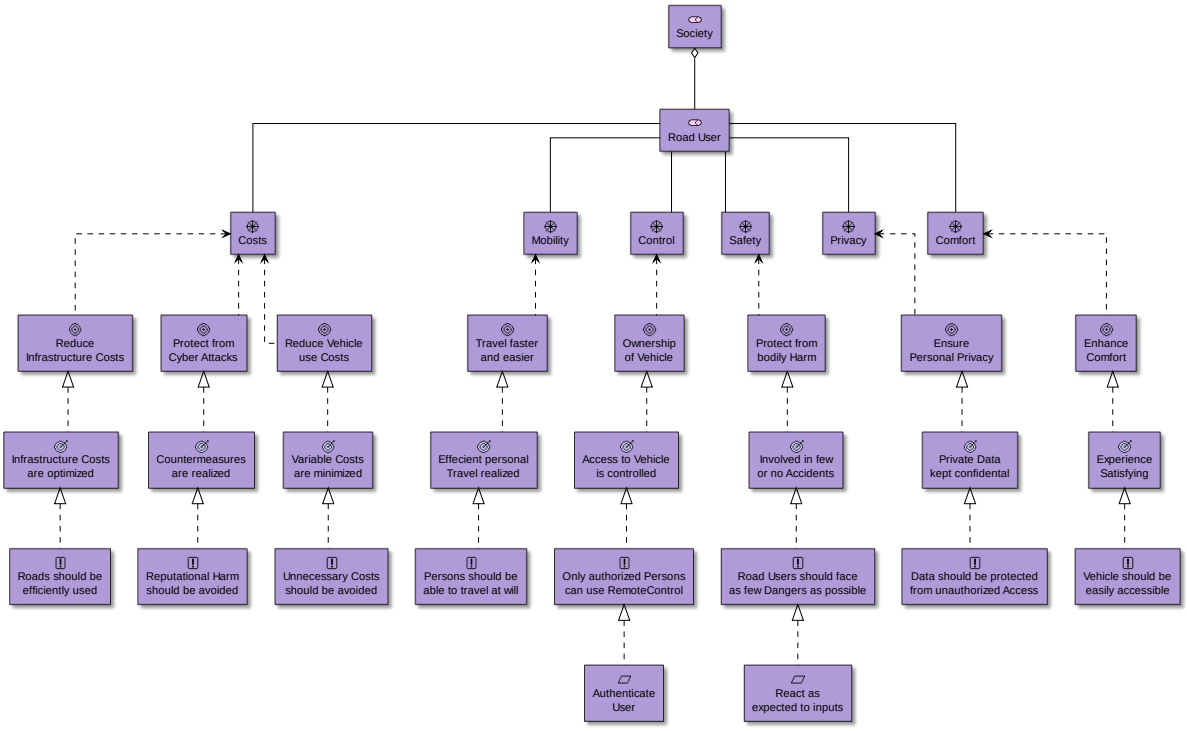


Figure 8: ArchiMate motivation layer – road user

3. **Safety**: One of the most important factors for road users is safety. This ensures the physical well-being of the road user in road traffic. It means that the road user is involved in fewer or no accidents. As a general rule, the road user should be exposed to as few hazards as possible, which is achieved by, among other things, the conformity of the vehicle with the assumed response to input.
4. **Control**: The road users demand control over their vehicles. This is achieved by controlling the access to the vehicle, which is done by authorizing the persons who want to access the vehicle.
5. **Mobility**: In addition to safety, the mobility of road users is a major criterion. Efficient and fast transport must be possible at all times to satisfy this need.
6. **Costs**: Road users want to keep the variable costs for the use of their vehicle as low as possible and reduce them if possible. This requires avoiding unnecessary costs.

Vehicle Manufacturer

Motivation of the vehicle manufacturer

In this model, the interests of the *vehicle manufacturer* are confined to economic and legal motives depicted in Figure 9 and described below:

1. **Market share**: Vehicle manufacturers want to increase their market share. They achieve this through the satisfaction of their customers, which is necessary for the continued existence of the company.
2. **Legal regulations:** In order to avoid any penalties, the vehicle manufacturer must comply with the legal requirements to ensure the continued existence of the company.

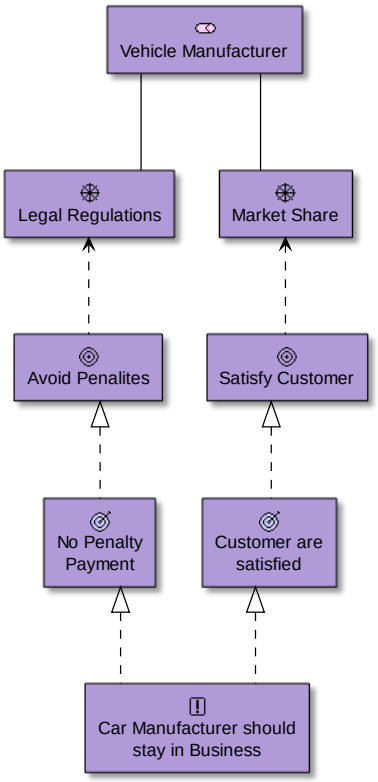


Figure 9: ArchiMate motivation layer - vehicle manufacturer

Third Party Service Provider

Motivation of the third party service provider

Third party service providers provide services and products that are not necessarily required to operate an ITS, but that provide the road user with additional comfort and safety features. The motivations of the providers are solely in the economic sector and are shown in Figure 10:

1. **Profit**: The main motivation of the third-party service provider is the profit, which is generated with the offered services.
2. **Reputation**: In order to increase the provider's profit, customers must be acquired, serviced and satisfied. A main prerequisite is a good reputation of the company.

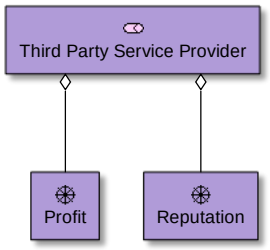


Figure 10: ArchiMate Motivational Layer - Third Party Service Provider

Security Authorities

Motivation of the security authorities

Security authorities are responsible for enforcing the legal framework in which transport systems operate. This includes all activities which the executive must carry out within the framework of its traffic police activities, as well as the protection of members of society from damage. Figure 11 illustrates the motives of the security authorities, which are described in the following:

1. **Protection**: A very central task of the public security agency is "danger prevention". It includes the defence against dangerous attacks, which includes the prevention of intentional offences according to the criminal code.
2. **Legal obligation**: The Security Police Act (SPG), the State Security Police Act (PStSG) and the Code of Criminal Procedure (StPO) define the statutory duties, responsibilities and measures of the police, the Federal Office for the Protection of the Constitution and in general the fight against terrorism, the criminal investigation department and the Public Prosecutor's Office.
3. **Crisis management**: Security organizations protect the health of the population in natural disasters such as floods and fires as well as in human-made crises, either by directly intervening in the situation or by coordinating other organizations.

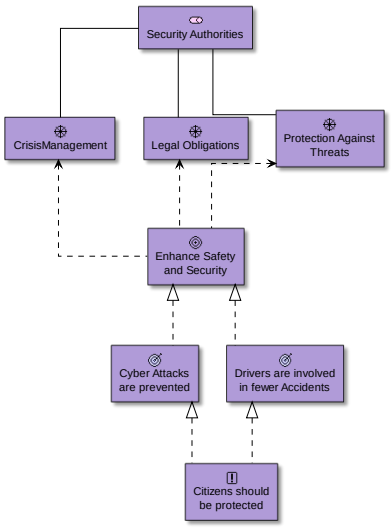


Figure 11: ArchiMate motivation layer - security authorities

Standards Organisations

Motivation of the standards organisations

The principal activity of a standards organisation is the development, dissemination, publication and coordination of standards required by a group of affected stakeholders [5]. According to the International Organization for Standardization (ISO), a standard "provides rules, guidelines or characteristics for activities or for their results, aimed at achieving the optimum degree of order in a given context" [6]. The motivations of *standards organizations* are illustrated in Figure 12.

1. **Harmonization**: Due to the various stakeholder interests and development cycles, several standards can evolve on the same subject. This redundancy shall be reduced in the course of harmonization and ideally a uniform standard shall be created.
2. **Interoperability**: Interoperability describes the property of a product whose interfaces are fully understood so that other products or systems can work with it. This interoperability is ensured, among other things, by the coordination and standards of the standard organisations.
3. **Influence** and lobbying: Industry stakeholders, who are also members of the standardisation committees, have an interest in adapting the standard to be established to fit their product portfolios or to obtain other possible benefits.

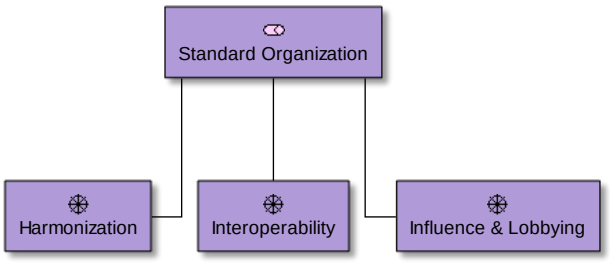


Figure 13: ArchiMate motivation layer - standard organization

Logistics Service Providers

Motivation of the logistics service providers

The interests and motivations of the *logistics service providers* are primarily in the reduction of costs (e.g., through platooning), as well as in a properly regulated and efficient road traffic. These two aspects coincide with the interests of the road user and the infrastructure operator.

4.1.2 Legal Compliance

Legal compliance is an inherent aspect of the motivation layer

For a well-functioning intelligent transport infrastructure, the legal structure must be considered, reflecting societal and governmental principles. Measures like prohibitions, penalties and claims for damages guide stakeholders to comply with European and national regulations. Non-compliance with societal values is always a strong challenge for new products and services. European regulation follows a liberal approach with a strong emphasis on safety and security. It is necessary to consider the "state of the art" or to take "appropriate and proportionate technical and organisational safety precautions". Additional risks may occur due to rules on liability. In certain areas there is also a self-regulatory approach based on a risk-based approach. Despite it is no explicit layer in the reference architecture, the motivation layer should reflect legal compliance as well.

In a fast-developing environment, it is necessary to use an architecture that does not provide static specifications for today's legal situation but can also take future developments into account. Thus, technical, legal and societal developments have to be considered. The reference architecture offers the possibility of showing connections and determining which critical points can be protected and how.

Due to the diverse actors and their interactions within the scope of connected and automated driving, there is inevitably a multitude of different interests that complement or contradict each other. Here it is helpful to draw on an all-embracing picture, which can also support a legislator in weighing the interests involved in the legal policy process, as well as in determining whether a self-regulatory approach is possible.

4.1.3 Strategy Layer

Strategy layer captures the approach, resources and skills

The *strategy layer* is used to elaborate the overall strategy of reference architecture. The strategy is determined by the planned approach, the available resources and skills. Within this model, proper communication services are crucial. Therefore, a know-how in the development of communication services is a necessary capability used by the resources in form of the employees, partners and the development infrastructure.

4.1.4 Business Layer

Business layer represents the business actors, objects and services

The *business layer* is used to represent the business architecture of a company as a description of the structures and interactions between strategy, organization, functions, processes and information. As such, it identifies the concepts and relationships of business actors inside and outside the organisation, business objects, as well as business services. The idea of this layer is to describe products or services, their values, contracts, and the meaning of business objects. This layer is often used in conjunction with the strategy layer.

4.1.5 Application Layer

Application layer focusses on IS and applications

The *application layer* in ArchiMate is used to represent the architecture of a company's information systems and applications. Wherever possible, the analogy with the business layer is respected.

4.1.6 Technology Layer

Technology layer includes technical implementations (n/a)

The *technology layer*, shown in green in Figure 15, describes the applications in terms of software and hardware technology elements such as physical devices, networks, or system software (such as operating system, databases, and middle-ware). This layer is mentioned for the sake of completeness but is not in the scope of this project due to open architectural design.

4.2 Security Measures

Security measures are tagged to elements on all layers

After properly modelling the architecture and adding the security requirements, as outlined in chapter 2.3, we can further detail the security aspects of the model and include specific threats and countermeasures as well as failure states and other elements with a security impact. With additional security requirements on the business layer, known or expected vulnerabilities at the application and technology layer can also be tagged. The assessment element specifies these threats as shown in Figure 14:

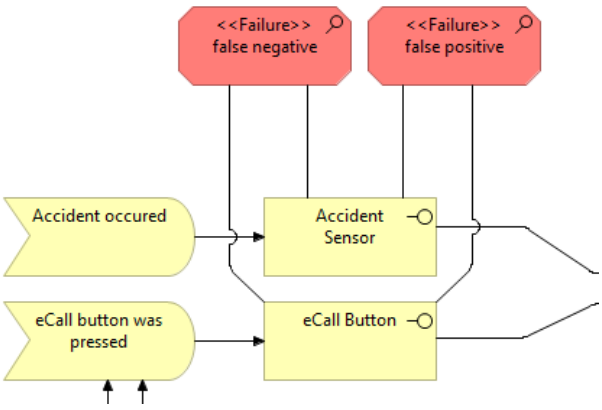


Figure 14: Example of an assessment element used to outline possible failure states

The threat influences security requirements and elements in the application or technology layer to mitigate those threats.

With threats connected to security requirements and security requirements linked into the motivation layer, every element of the model can be reasoned about, and its necessity evaluated. Security measures are no longer an extra add-on, but an integral part of the architecture.

4.3 Example: Vehicle to Infrastructure

Example model for the infrastructure-to-vehicle business model and the two attack scenarios.

In order to demonstrate the feasibility of modelling the infrastructure including necessary security measures, an example with two attack scenarios has been selected. The outcome of this work is shown in Figure 15, which is a representation of the infrastructure-to-vehicle business model, including two distinct attack scenarios with their subsequent security requirements.

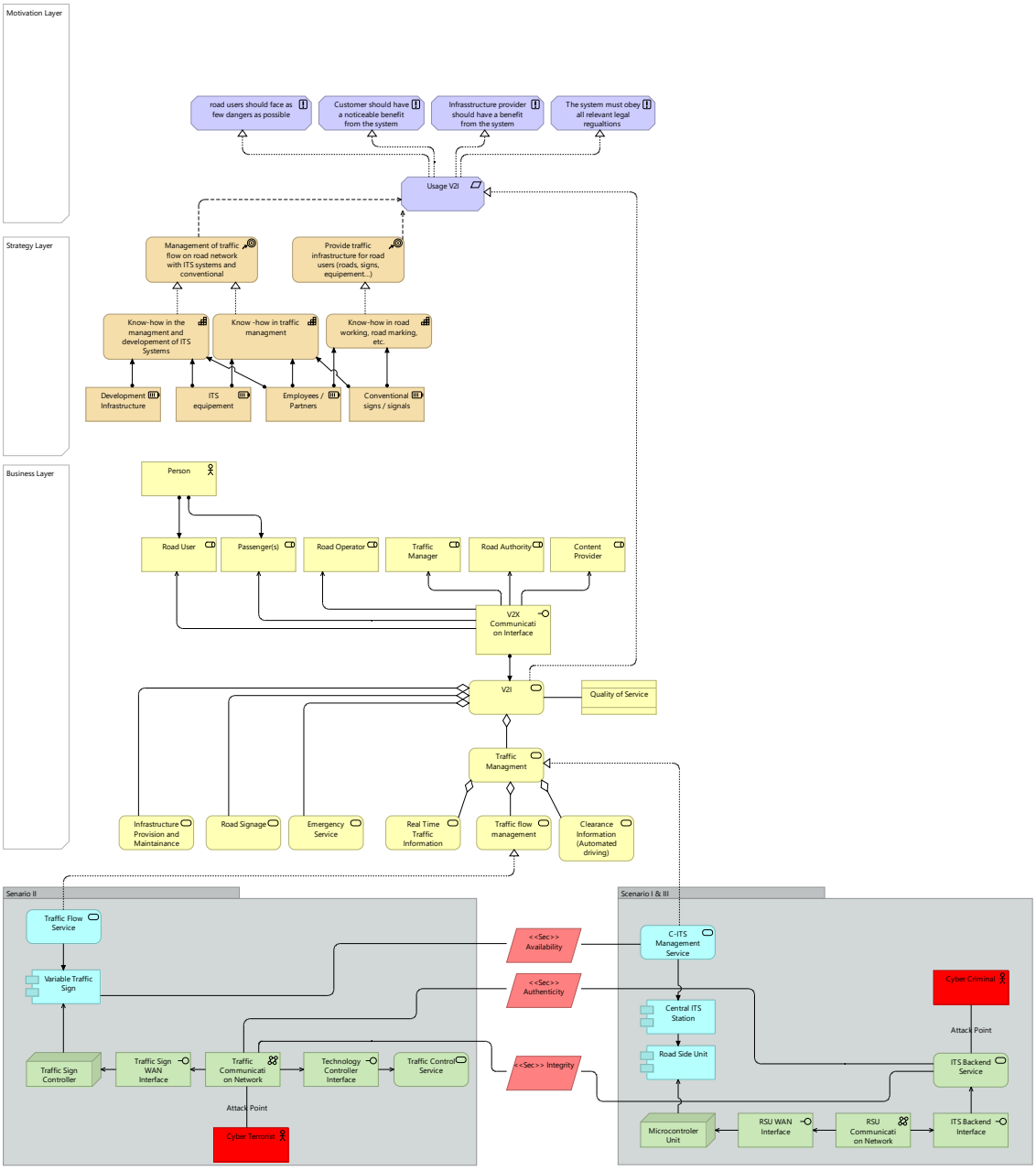


Figure 15: Vehicle to infrastructure example

As Figure 15 shows, the business service V2I consists of a set of sub-services, namely for providing infrastructure provisioning and maintenance, road authorities, emergency services, clearance information (for automated driving purposes), as well as traffic management. Latter service is composed of real time traffic information and traffic flow management. This view is the basis for our following considerations regarding integrating security requirements for countering specific attacks with the infrastructure-to-vehicle services.

4.3.1 Scenario I: Impact of collateral damage by malware

Model of scenario I

Scenario I in Figure 15 consists of mapping of the attack scenario from chapter 3.1 to our V2I model. It includes elements from the *application layer*, that is the *application service* "C-ITS management service", which controls *application component* "central ITS station" and in subsequent fashion the underlying road side units and realizes the *traffic management service*, as well es elements from the *technology layer*. Here, we can see the *technology service* "ITS backend service", which communicates via its *technology interface* (the ITS backend interface) over the *communication network* "RSU communication network" with the *node* "microcontroller unit" of an RSU. Attack point of the *business actor* "cybercriminal" is the ITS backend service. Therefore, this service needs to implement the three security requirements **availability**, **authenticity** and **integrity** in order to withstand attacks from a cybercriminal.

4.3.2 Scenario II: Manipulation of variable message sign control system

Model of scenario II

Analogously to the fist scenario, the second scenario is marked as scenario II in Figure 15. Here, the *application service* "traffic flow service" realizes the traffic flow management service of the V2I model. This service controls the underlying *application component* "variable traffic sign". On the *technology layer*, we have the *technology service* "traffic control service" which communicates via *technology interfaces* and the *communication network* "traffic communication network" with the *node* "traffic sign controller". In this example, our malicious actor, the *business actor* „cyber-terrorist", chooses to attack the traffic communication network. Therefore, this *communication network* must provide its users with **authenticity** and **integrity**. At a higher level, the *application component* "variable traffic sign" must guarantee **availability** to the V2I services and users.

5 Analysis

The proposed reference architecture is critically assessed in the following and viewed from the perspective of strengths, weaknesses, opportunities and threats applying a SWOT structure.

5.1 SWOT Analysis

Discussion of the CySiVuS cyber-security reference architecture approach

Strengths

The important characteristic of the architecture framework we have employed is the division of a system into different perspective levels. Due to the technology-neutral and restrictive focus on individual viewing levels – e.g., services, motivations, technical applications – the modelling tasks are separated from their complexity and thus simplified. After several iterations and inclusion of different stakeholder perspectives, this ultimately leads to a holistic view of information processing and helps to better understand inherent relationships and dependencies. The uniform vocabulary of the elements of the reference architecture allows new elements to be easily added, integrating them into the existing representation, thus successively building up the ICT architecture.

The modelling tool ArchiMate offers the possibility to apply consistency checks to the model over several levels. Through this formal verification, open or contradictory relations can be uncovered and corrected. For content verification, various concrete scenarios are then mapped to the reference architecture that has been created, and they are checked for representability in the model. The uniform notation and the compatibility with machine-readable process descriptions enable the execution and machine validation of the entire process model.

The choice of this generally applicable methodical approach according to an open standard enables other projects or persons to integrate their own findings at a later point in time after a certain familiarization with the syntax and semantics of the elements used.

The complexity reduction by the consideration of six levels is essential for the successful employment of the modelling tool. However, the technology level has been omitted, since different technologies can implement the applications and are thus not crucial for a reference architecture.

Weaknesses

The ArchiMate modelling tool has many usable elements, the actual purpose of which only becomes apparent when used for the first time. Firstly, the modellers must deal with the intention and logic of the given granularity, which takes a certain amount of time for newcomers. In addition, the level of detail from the use cases to be mapped is not defined at the beginning and must be worked out during modelling. Ultimately, these weaknesses are a question of skill.

During the modelling of the use cases there can be duplication of content in the modelling, which are uncovered only at a late stage. In practice, the question also arises as to the level at which an aspect can be modelled.

The reference architecture and the modelling language do not provide a rigid procedure model, although modelling practice at least suggests the order of the modelling levels. However, this can lead to gaps between the levels, which are only recognized in the overall view.

Opportunities

A definite possibility for the application of the reference architecture is the creation of perspective changes. This was also visible when the security overlays were considered. By tailoring security aspect to the metamodel it can be determined, where the implementation of security measures is appropriate, where these are missing or possibly detect redundant or conflicting measures. The chain of successive activities is decisive here, since potential attack paths can be based on both the elements and their relationships.

Another aspect is the creation of a unified view across multiple use cases, projects or focal points. Since this white paper is addressed to an interested audience of professionals and invites them to contribute their own views, projects, emphases, architectures, processes, activities, and relationships by modelling them in ArchiMate, over time an overarching reference architecture can be created to ensure its consistency with other content.

Threats

From the threat perspective it can be stated that too few iterations lead to a lack of quality in the modelling and its balanced level of detail are discovered very late. This means that models created with less effort, which may not be thought through in every detail, can find their way into the reference architecture. The value of the model critically depends on the correct use of the tool.

The application of a standard distinct from the reference model itself is profitable for the user on the one hand, but the question of assured downward compatibility arises on the other. The security overlay is a good example of this. Their combination with the overall model is given at this point; if the architecture tool is reformulated, it can endanger the content substance of the reference model.

5.2 Cyber-Security Implications

How to analyse security requirements in the cyber-security reference architecture

If we view the architecture model as a network of nodes and edges, we can apply an automated logic to it to identify possible security issues. Any security requirement or assessment that is not addressed by an appropriate incoming edge (typically of the "influences" type) is a security issue that has not been addressed. While a model cannot identify the quality of security measures taken, it can ensure that no potential security issues have been entirely overlooked.

The approach also allows statistical applications to the model. A simple count will advise us to the primary security concerns throughout the entity under consideration. An entity primarily concerned with confidentiality of data will show a higher count of such relations than a model primarily concerned with performance and availability. This gives additional information about the focus of security efforts and their relative importance. While not a replacement for a proper risk analysis, the model itself allows for a big-picture view of the security requirements.

Finally, if modelled properly we can see relations throughout the model and identify common features easily. A principle of architecture is re-use; while an element can appear in multiple views in different ways, the underlying model only has one representation of this element. For our security overlay models, this means that selecting the "<<Sec>> Integrity" element, e.g., will show us all related elements for which integrity is a security requirement, seen in Figure 16.

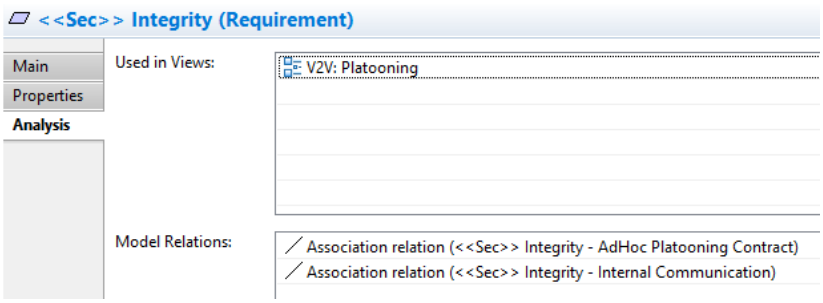


Figure 16: Security analysis example

This view on the model makes it easier to identify possible countermeasures that can address multiple security requirements, because it is likely that a countermeasure that increases the integrity for one node can also be applied to other nodes. Edges, representing data or control flows, often share a medium such as a network, a bus system or a data store. Again, it is likely that a single security measure can address similar security requirements in multiple places.

5.2.1 Analysing Legal Aspects

The reference model also allows requirements of the legal system to be included. The main principles and standards result, e.g., from safety and security (e.g., security of network and information systems – NIS - rules, road safety), liability and responsibility (compensation for damages and criminal law) data protection law (e.g., General Data Protection Regulation - GDPR) etc. Furthermore, the future role of robots and AI must be considered. The reference architecture can be extended to cover detailed legal requirements, which vary from country to country. The reference architecture can be used to show which measures must be taken by individual actors to comply with legal standards. For example, which measures must be taken regarding data protection and security regulations, in order to minimise the risk of prohibitions, penalties and claims for damages and to act in compliance with the law. The relationships presented in the reference architecture can be used to analyse efficient measures within the framework of risk analysis. The fact that cyber-security and data protection measures are already considered in the development process and in the technical design (security-by-design; privacy-by-design) enables a type of compliance that goes beyond the mere fulfilment of legal requirements and shows good practice.

How to analyse legal aspects

The reference architecture also offers the possibility of forming an overall picture of the complementary or conflicting interests within the framework of the intelligent transport infrastructure. The interaction between the interests of those subject to the law (including fundamental rights) and social (public) interests can be represented, which can initiate a political debate. The reference architecture can also help to decide how regulation should take place - e.g., by self-regulation or legislation.

6 Conclusion

6.1 Summary

How to get the cyber-security reference architecture

The proposed reference architecture allows modelling and structuring various traffic infrastructure elements, communication services needed, as well as security requirements. In order to structure the architecture, off-the-shelf tools are used to split the traffic infrastructure system and all relevant players and stake holders into different layers. Attributing, interfaces, relationships and communication links can be assigned within the different layers to support the architecture definition.

The architecture is available as Gitlab repository under the following link:

https://gitlab.com/CySiVuSConsortium/cyber-security-reference-architecture

6.2 Outlook

How to develop the cyber-security reference architecture – bring in your scenarios or use cases to contribute!

Based on its modularity the reference architecture has the potential to find various future applications. The reference architecture starts from a holistic perspective, but it can be extended and further specified by every stakeholder to meet his or her requirements. Thus, the reference architecture can be employed by (among others): society (road users, motoring organizations), infrastructure operators, logistics service providers, vehicle manufacturers, third party service providers, administration, standardization companies, countries, and maintenance providers.

The modelling language ArchiMate offers the possibility to apply consistency checks over several levels to the model. This formal verification allows uncovering and correcting of open or contradictory relations. For content verification, various scenarios are checked for representability in the model. A final verification of the reference architecture can be done by different showcases and demonstrators.

The results obtained in the final verification and by the application of the stakeholders can in turn be used to extend the reference architecture in iterative steps.

7 Partners

TÜV AUSTRIA Group

TÜV AUSTRIA is an international company with branches in more than 20 countries of the world. TÜV AUSTRIA employs about 2.000 people. The service competencies of the four business areas „Industry & Energy", „Infrastructure & Transportation", „Business Assurance " and „Digital Services" encompass the areas of testing, monitoring, certification, education and training consulting.

From its offices in Cologne and Vienna, TÜV AUSTRIA Group Member TÜV TRUST IT is the neutral, objective and independent partner for consulting and certification services related to information security and data protection. The goal is to help companies protect information assets that are necessary for proper business operations and that are made available through infrastructures and processes. The services of TÜV TRUST IT are based on recognized standards and proven methods.

Contact partner for Architecture Modelling:

Tom Vogt – tom.vogt@tuv.at

AIT Austrian Institute of Technology

The Austrian Institute of Technology (AIT) is the largest Research and Technology Organisation (RTO) in Austria. AIT provides a major contribution to strengthen the technological knowledge base of the Austrian economy and to maintain Austria's position as a business location in international competition. The Center for Digital Safety and Security (DSS) is a high-tech organisation in the field of applied research. In partnerships with industry, universities and other research partners, DSS builds bridges between ideas, design and development, test and implementation to leading, innovative and intelligent system solutions in selected market areas. Areas of competence are computer vision, video surveillance, high performance image processing, intelligent sensor systems and IT security.

Contact partner:

Martin Latzenhofer - martin.latzenhofer@ait.ac.at

T-Systems

T-Systems is one of the five leading ICT service providers in Austria. The company uses its bundled know-how to support its customers along their entire value chain in all phases of complex system implementation: From infrastructure through consulting, development, implementation and integration to the operation of the solutions. T-Systems operates its own competence centre for cyber-security and offers a range of security solutions.

Contact partner:

Thomas Raab - thomas.raab@t-systems.com

SWARCO

SWARCO Group is a growing international group providing the complete range of road marking, signalling and traffic management products, services and solutions. The focus of SWARCO's business is to keep traffic in motion, inform, and guide the traveller with innovative products and services in order to support the growing mobility needs of society. Our mission is to help our customers manage mobility and increase road safety with high quality and environmentally friendly solutions while providing a sustainable return to our stakeholders.

As the world's largest traffic light producer, SWARCO has comprehensive expertise in traffic signalling. For more than seven years, SWARCO is working on solutions for connected and recently automated driving. The solutions comprise roadside equipment for V2X communication, either via ITS-G5 or via 3G/4G. Moreover, a backend system

as interface to a traffic management system is also part of the solution. Numerous cities and highway operators in Europe and beyond trust SWARCO's future-proven signalling solutions in order to reduce emissions and save money.

Contact partner:

Klaus Pollhammer - klaus.pollhammer@swarco.com

ASFINAG

ASFINAG is the Austrian motorway and expressway operator with a network length of over 2200 km. ASFINAG plans, finances, builds, maintains and collects tolls on the entire primary road network in Austria.

Contact partner:

Stefan Ruehrup - stefan.ruehrup@asfinag.at

Universität Wien - Arbeitsgruppe Rechtsinformatik

The Faculty of Law of the University of Vienna is the oldest and largest law faculty in the German-speaking area. Law has been researched and taught here for over six centuries. Today, more than 10,000 students are supervised by around 600 staff members. Law is at home here - from the basics of law to its application in daily practice, it is the subject of our research and teaching.

The interdisciplinary Centre for Computers and Law of the University of Vienna (ARI, Arbeitsgruppe Rechtsinformatik) is situated at the Faculty of Law of the University of Vienna and looks back at more than 25 years of teaching and research and is considered as one of the top 10 centres worldwide in this field. It is one of the few centres of computers and law with a strong focus in the technology of legal applications (e.g., legal information systems, automation of law, legal ontologies, etc.) and maintains one of the strongest interdisciplinary networks in Vienna and world-wide. Its co-organised conference IRIS (Internationales Rechtsinformatik Symposion) is the largest event in Europe in legal informatics with an interdisciplinary focus on theory, practice & ideas.

Contact partner for legal issues:

Erich Schweighofer – erich.schweighofer@univie.ac.at

Nokia Solutions and Networks GmbH

We create the technology to connect the world. We develop and deliver the industry's only end-to-end portfolio of network equipment, software, services and licensing that is available globally. Our customers include communications service providers whose combined networks support 6.1 billion subscriptions, as well as enterprises in the private and public sector that use our network portfolio to increase productivity and enrich lives.

Through our research teams, including the world-renowned Nokia Bell Labs, we are leading the world to adopt end-to-end 5G networks that are faster, more secure and capable of revolutionizing lives, economies and societies. Nokia adheres to the highest ethical business standards as we create technology with social purpose, quality and integrity. www.nokia.com

Contact partner:

Christian Watzinger – christian.watzinger@nokia.com

8 Bibliography

Sources

[1] E. ETSI, "302 665", Intelligent transport systems (ITS), pp. 1–44, 2010.

[2] SAE, "taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems J3016_201401", 2014. [Online]. Available: https://www.sae.org/standards/content/j3016_201401/. [Accessed 20 6 2018].

[3] Parker, Donn B. (2002). "Toward a New Framework for Information Security". In Bosworth, Seymour; Kabay, M. E. (eds.). The Computer Security Handbook (4th ed.). New York, NY: JohnWiley & Sons. ISBN 0-471-41258-9.

[4] The Open Group, „ArchiMate® 3.0.1 Specification, an Open Group Standard", The Open Group, 2017-2012.

[5] W. Ping, "A Brief History of Standards and Standardization Organizations: A Chinese Perspective,"no. 117, p.28, 2011.

[6] International Organization for Standardization, "Deliverables." [Online]. Available: http://www.iso.org/cms/render/live/en/sites/isoorg/home/developing-standards/deliverables-all.html

[7] STRIDE, Microsoft, https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)

[8] Demarco, Tom. *Structured Analysis and System Specification*. New York: Yourdon Press, 1979. ISBN 978-0138543808. P. 352.

[9] Caltagirone et al. T*he Diamond Model of Intrusion Analysis*

[10] IEC, *IEC 60812 Failure modes and effects analysis (FMEA and FMECA)*. 2018.

[11] Vogt T., A Comprehensive Risk Management Approach to Information Security in Intelligent Transport Systems

[12] Alan J. Card et al.: Beyond FMEA: the structured what-if technique (SWIFT). In: Journal of healthcare risk management: the journal of the American Society for Healthcare Risk Management

[13] C-V2X ebnet den Weg hin zu 5G für autonomes Fahren, https://www.all-electronics.de/c-v2x-5g-autonomes-fahren/

[14] Defense Advanced Research Projects Agency, https://www.darpa.mil/

[15] Directive 2010/40/EU, framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32010L0040

Figures

Shutterstock (cover photo) CySiVuS Consortium (Figures 1 - 14)

WhitePaper

TÜV AUSTRIA Group

DI Edvin Spahovic
TÜV AUSTRIA-Platz 1
2345 Brunn am Gebirge
Mail: *edvin.spahovic@tuv.at*

tuvaustria.com

Figure: Shutterstock, © Yaran