Position paper

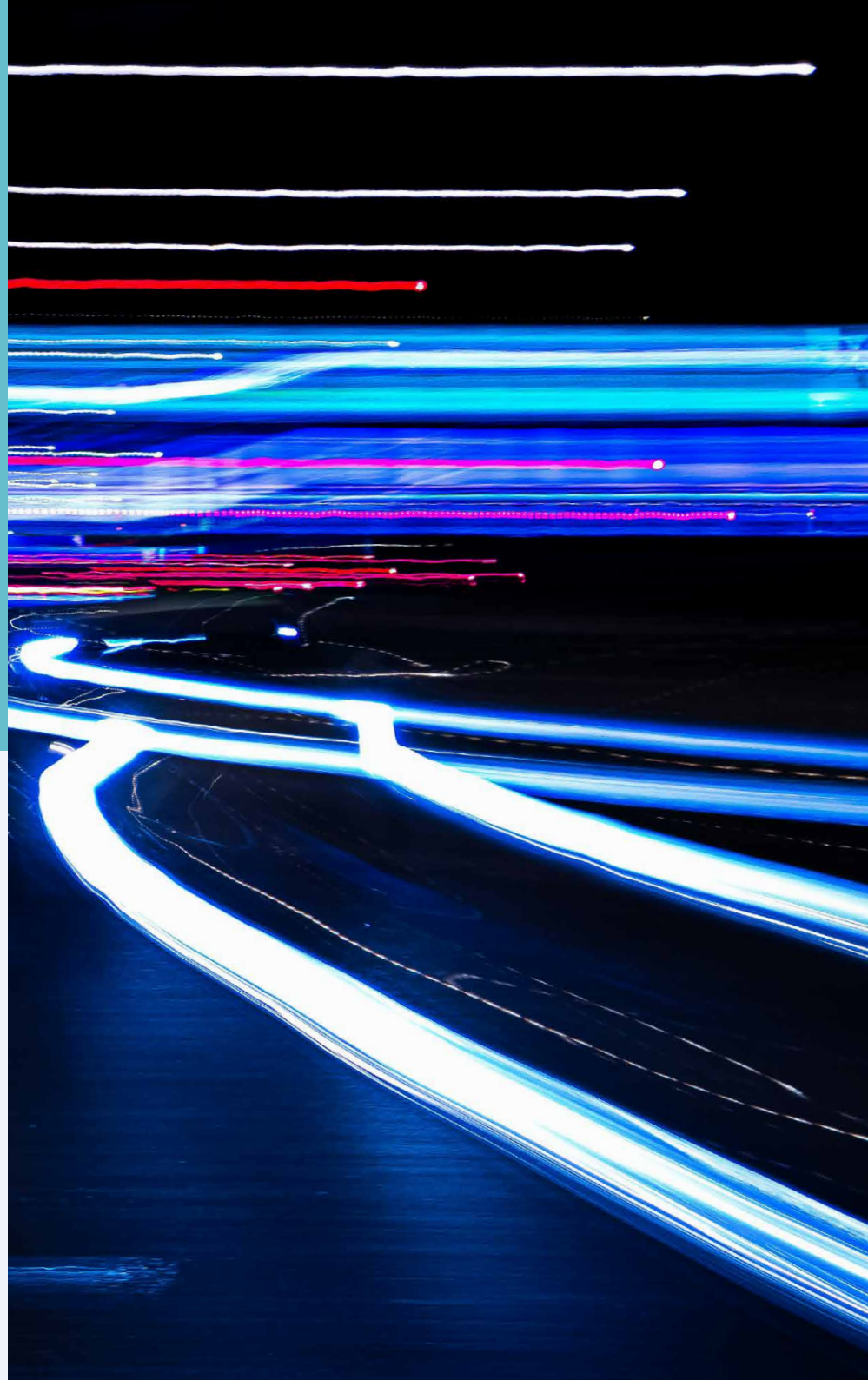
Cybersecurity in the Automotive Domain

Authors
Yoram Meijaard
André Smulders
Frank Benders
Jacco van de Sluis
Peter-Paul Schackmann
Bastiaan Wissingh
Shari Finner
Joëlle van den Broek

October 2023

TNO innovation for life

The window of opportunity to tackle cybersecurity aspects on a system level is now



Cybersecurity in the Automotive Domain

Modern smart mobility concepts are increasingly relying on data and connectivity, and cybersecurity is becoming an essential precondition for their uptake and success.

In fact, a lack of cybersecurity can be a complete showstopper for the further introduction of new smart mobility systems, especially in cases where road safety – and therefore human lives – may be endangered. With the fast digitization of the mobility domain, the risk is that mobility systems are being developed without security in mind, even if connected vehicles recently following the United Nations Regulation no. 155 (R155) and no. 156 (R156), this could lead to suboptimal and potentially blocking solutions. The window of opportunity to tackle cybersecurity aspects on a system level is now. For this, action is needed both by governments and private parties.

This TNO position paper provides an analysis of the most important organizational and technical challenges of cybersecurity aspects in the automotive domain. With a generic risk analysis method and model for cyber threats in mobility services, we perform a threat and gap analysis for three selected connected mobility system services. Our analysis leads to recommendations on how to tackle the challenge of cybersecurity in new mobility concepts and gives recommendations for starting points, both from an organizational and technical point of view.

Cybersecurity maturity

Our analysis reveals that several cyber security measures are in place in the mobility system domain such as defined in R155 and R156. Although these security initiatives seem to solve everything, both market and governmental parties show a different level of cybersecurity maturity, which hinders the integration of existing (connected) mobility system concepts and solutions. We therefore pose that clear actions from the Dutch and European governments are needed to streamline these efforts: The first step is to clarify ownership of the problem and the distribution of responsibilities, before taking the initiative to streamline efforts in the entire ecosystem by structurally setting up incentives and mechanisms for collaboration, standardization and information sharing. In our view, the role of governments, OEMs, road operators and service providers is to facilitate the transition by connecting to other public and private stakeholders, pursuing interoperability for their own services and products, and making information sharing and collaboration feasible from their own organizational perspective.

Building knowledge

From a broad mobility system solution perspective, TNO is in a promising position to facilitate the digitization transition towards connected mobility systems by helping companies and governments identify design and implementation requirements for future applications regarding cybersecurity logging and management systems, as well as detection, prevention & safe mitigation measures. As an independent research organization, TNO is suited to analyse different concept implementations, explore attack tooling to assess the resilience of automotive systems, and support governments and OEMs in building knowledge on the safety and cybersecurity case of novel AD/ADAS and connected applications in the automotive domain.

Contents

1. Introduction and motivation

Recent years have shown that, due to digitization, mobility is increasingly dependent on data and connectivity.

In short: this is a call-to-action for **security by design** at system level across the mobility domain!

This is a system transition, a transition that is required to combine society's future mobility needs with the simultaneous desire for zero casualties, zero emissions and zero efficiency loss. After all, the current available mobility and logistics systems are reaching their limits.

Within this system transition, it is increasingly clear that the development of cybersecurity is a precondition for the success of mobility of the future. In particular, this is evident in cases where information- and cybersecurity have an effect on physical traffic safety, although in the long-term, privacy and data integrity may become just as critical. Cybersecurity as a precondition makes it inevitable for the mobility industry to move to future-proof concepts like an integrated system approach and security by design, that take into account the complexity of the entire value chain and the scalability of new mobility concepts. Our analysis reveals that several cyber security measures are in place in the mobility system domain such as defined in United Nations Regulation no. 155 (R155)[1] and no. 156 (R156)[2]. Although these security initiatives seem to solve everything, both market and governmental parties show a different level of cybersecurity maturity, which hinders the integration of existing (connected) mobility system concepts and solutions.

With an integrated system approach, cybersecurity challenges are addressed at system level instead of only at parts of the product- or value chain. An integrated systems approach requires the alignment of the R&D agendas of the cybersecurity, ICT and mobility sector. Security by design means that hard- and software for new mobility concepts are developed with cybersecurity in mind. More specifically, it means that cybersecurity is already considered during the design phase, instead of retrofitted after the product development has been finished. This way, security-by-design leads to more secure and more scalable system solutions.

At the moment, in the newly evolving digitized mobility situation, no single party is fully responsible for end-to-end security, and the current and future attribution of responsibilities in the value chain is unclear. The imminent risk is therefore that products are being developed without security in mind. As a result, only a restricted set of security mitigations will be possible after the product design and development phase, resulting in sub-optimal solutions that could be showstoppers for promising new and innovative mobility concepts.

The new mobility systems must be formed by combining domain knowledge, key methodologies and key technologies from automotive, mobility, logistics and ICT. To this end, cross-sector solutions are needed in which economic interests as well as social interests must be weighed up. The Netherlands employs a dense infrastructure of roads and cities, and therefore has an intrinsic motivation to address and solve this challenging task. It is also well-suited to take crucial steps in solving this complex problem due to its excellent physical and evolving digital infrastructure, strong research, High-Tech and ICT industry, and strong economy with regard to logistics.
At the same time, it should be noted that a definitive solution requires dedicated efforts at European tables to foster standardization and strong international collaborations.

Call-to-action

At this point in time, Dutch and European public and private parties alike seems to find it difficult to take the first step. The goal of this position paper is to cultivate awareness and create clarity in an uncertain situation.

We aim to break the waiting cycle by showcasing a concrete step-by-step analysis of cybersecurity risks in the mobility domain, highlighting the main security bottlenecks and proposing concrete and tangible approaches with first steps. In short: this is a call-to-action for security by design at system level across the mobility domain!

2. The challenge: cybersecurity in the connected mobility system

Cybersecurity involves all measures for information systems and computers required to prevent, limit and recover from damage, disruption or misuse[3]. Traditionally, cybersecurity is concerned with so-called information systems, whose main purpose is to store, process and use data. Information systems consist of information and communication technology (ICT), such as computers, networks and servers. Nowadays, cybersecurity is also becoming more and more concerned with the emergence of cyber-physical systems, whose additional purpose is to have ICT directly interact with the physical world. Next to ICT components, cyber-physical systems include operational technology (OT) such as sensors, actuators and (hardware-) controllers.

Information systems and cyber-physical systems have different cybersecurity properties to be preserved. For pure information systems, the relevant properties are[4]:

Confidentiality
The property that information is not made available or disclosed to unauthorized individuals, entities, or processes (also called secrecy);

Integrity
The property of accuracy and completeness;

Availability
The property of being accessible and usable on demand by an authorized entity;

Authenticity
The property that an entity (e.g. a data set or data source) is what it claims to be;

Non-repudiation
The ability to prove or disprove the occurrence of a claimed event or action and its origins*.

*The objective of non-repudiation is to be able to resolve disputes about the occurrence or non-occurrence or an event or action by generating, collecting, maintaining, making available and verifying suitable evidence. This includes non-repudiation of origin, delivery, submission, transport, creation, receipt, knowledge, sending, ...

While these cybersecurity properties are defined in terms of their effect on information/data, they extend to the physical system in which this information is contained. For example, the integrity of medical records depends on the integrity of the computer on which they are stored. For cyber-physical systems, there are therefore additional cyber-physical properties to be preserved[5]:

Reliability
The system can perform its functions under stated conditions for a specified period of time;

Availability
The system can perform its functions when required;

Maintainability
The system can be easily repaired, adapted or improved;

Safety
The system cannot harm people, environment or other assets during operation.

Note that these properties are traditionally associated with any type of systems engineering, and hold irrespectively of the amount of 'ICT' or 'cyber' in the system. A purely mechanical gearbox, for instance, needs to be reliable, available, maintainable and safe for use. However, modern automatic gearboxes are completely digitalized and shift gear based on sensor-information. Faulty information, e.g. a reported rpm very different to the actual rpm may cause physical damage if causing a delayed gear shift. It becomes clear that the gearbox depends on the integrity of the digital information it receives in order to preserve reliability. More generally, an increasingly digitalized cyber-physical system becomes increasingly depended on cybersecurity properties in order to preserve its physical and cyber-physical properties.

The connected mobility system domain is a unique setting for cybersecurity. Mobility increasingly depends on a mix of information systems and cyber-physical systems. The mobility system is more than connected vehicles: Vehicles and road-side units feature a dynamic array of sensors that monitors the environment dynamically and accurately. All these systems cooperate to form a highly connected and dynamic environment that simultaneously needs to be safe and secure to be used. These dynamics, where information exchange is organized ad-hoc across many equipment manufacturers, is quite different to other domains using cyber-physical systems, which are typically much more static.

There is an ingrained safety culture shared across the entire mobility domain.

A vehicle produced by a manufacturer, for instance, is not allowed on the road unless it passes a series of standardised tests set by the legislator. This safety culture exists to make roads and general traffic as safe as possible and is strongly adhered to. In order to legislate and guarantee safe roads, the automotive industry is subject to a large number of norms and standards. Standardization in particular has led to much safer vehicles in traffic and drastically fewer traffic deaths and casualties. Following the idea of the ingrained safety culture in a more and more digitized domain, this position paper concerns the cybersecurity aspects of the connected mobility domain. In particular, cybersecurity aspects that may lead to unsafe road situations are taken into account. The scope of this paper thus does include tampering with road operator vehicles to induce collisions but excludes attacks on car-keys to steal vehicles or tampering with parking advice. While cybersecurity aspects such as privacy risks, societal impact and business impact are highly relevant for society, they do not impact physical traffic safety and are therefore not treated in this document.

Cyberattacks on the (connected) mobility system pose a varied collection of risks that require management. In general, cyber risk management is the process of reducing or limiting negative effects to a system by implementing the ability to identify threats, protect the system, detect attacks when they occur and adequately respond to and recover from the attack. As such, every attack will cause an organisation to go through the following cycle:

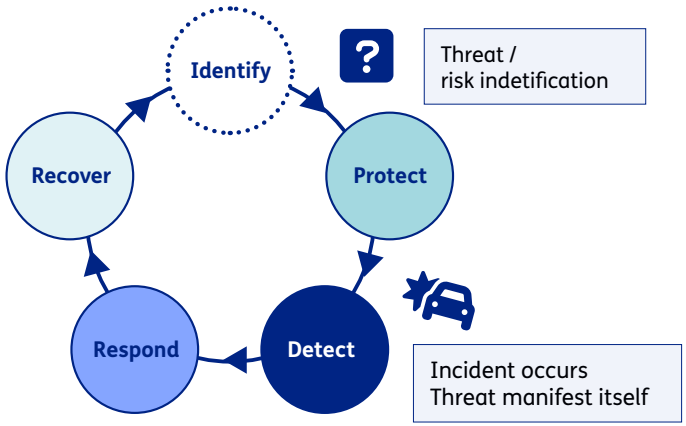


Figure 1. NIST Cybersecurity Framework, showing all five basic steps in cyber risk management.

Each of these steps may require one or more mitigating measures to be taken. Which measures to consider is a fundamental challenge in cybersecurity: applying too few (or worse: the wrong) measures will leave the system vulnerable, while too many or too strong measures can have a severe impact on the performance of the system and the organisations at large. A balanced and acceptable decision should be made between acceptable cybersecurity risk, physical safety risk, and impact on the applicable use cases.

There are various organisational and technical measures that can and should be taken, which will be elaborated in this paper in the context of connected mobility.

A final note on cybersecurity in new mobility system concepts vs. traditional physical traffic safety: Historically, the physical safety of a vehicle used to be determined at the time of development and construction: a vehicle adhering to the standard was considered safe for use. Standards for physical safety did change, but slowly. In contrast, cybersecurity is a continuous process over the entire lifetime of a product, which can change due to, for instance, software updates, communication or artificial intelligence. No predetermined tests derived at design-time can guarantee a cybersecure vehicle for decades. While from a safety perspective a vehicle used to be ‘done’ once it left the factory, new future-proof mobility concepts require vehicles to undergo continuous re-evaluation. As a result, in the coming years the existing norms and standards will be subject to change, with monitoring deployment processes and cybersecurity being crucial elements to check and prove safety of a car and larger mobility concepts.

3. Communication systems for the connected mobility system

In the connected mobility system, information is automatically transferred to a vehicle and/or its users to increase safety and/or traffic efficiency.

Examples include advisory systems on speed limits, lane closures, green light waves, etc. Note that current and future automated driving systems taking (semi-) automated actions also highly depend on information communication systems.

Information may be transferred to the vehicle or driver in several ways. In our analysis, we make a distinction between the following three mechanisms:

1.
Advice on a user device
The user has a device containing a smart advice system, e.g. an app on their smartphone or a smart GPS device; the information is obtained solely through communication channels provided by the device;

2.
Advice in vehicle
The vehicle itself collects information and communicates advice to the user. This information is obtained by integrated sensors and/or via additional communication channels with roadside units, other vehicles or via a cellular connection;

3.
Automated Driving System (ADS)
The vehicles cyber-physical systems use data to perform (semi-) automated actions like braking or steering. They may integrate information from different sources e.g. the vehicles own physical sensors and other communication channels.

The main differences between mechanisms 2 and 3 is the difference in SAE (Society of Automotive Engineers) automated driving levels*.

For mechanism 2 there are two options:
1. provide advice in the vehicle to the driver via the Human-Machine Interface or
2. the advice is interacting with the controls of the driver and displaying the advice on the Human-Machine Interface at the same time.

With both options the driver is in control and can overrule advice. Ergo, mechanism 2 is an SAE level 2 system. In contrast, mechanism 3 is an SAE level 3 system as the driver is not in the loop.

*The Society of Automotive Engineers (SAE) has defined several levels of increasingly automated driving [8]

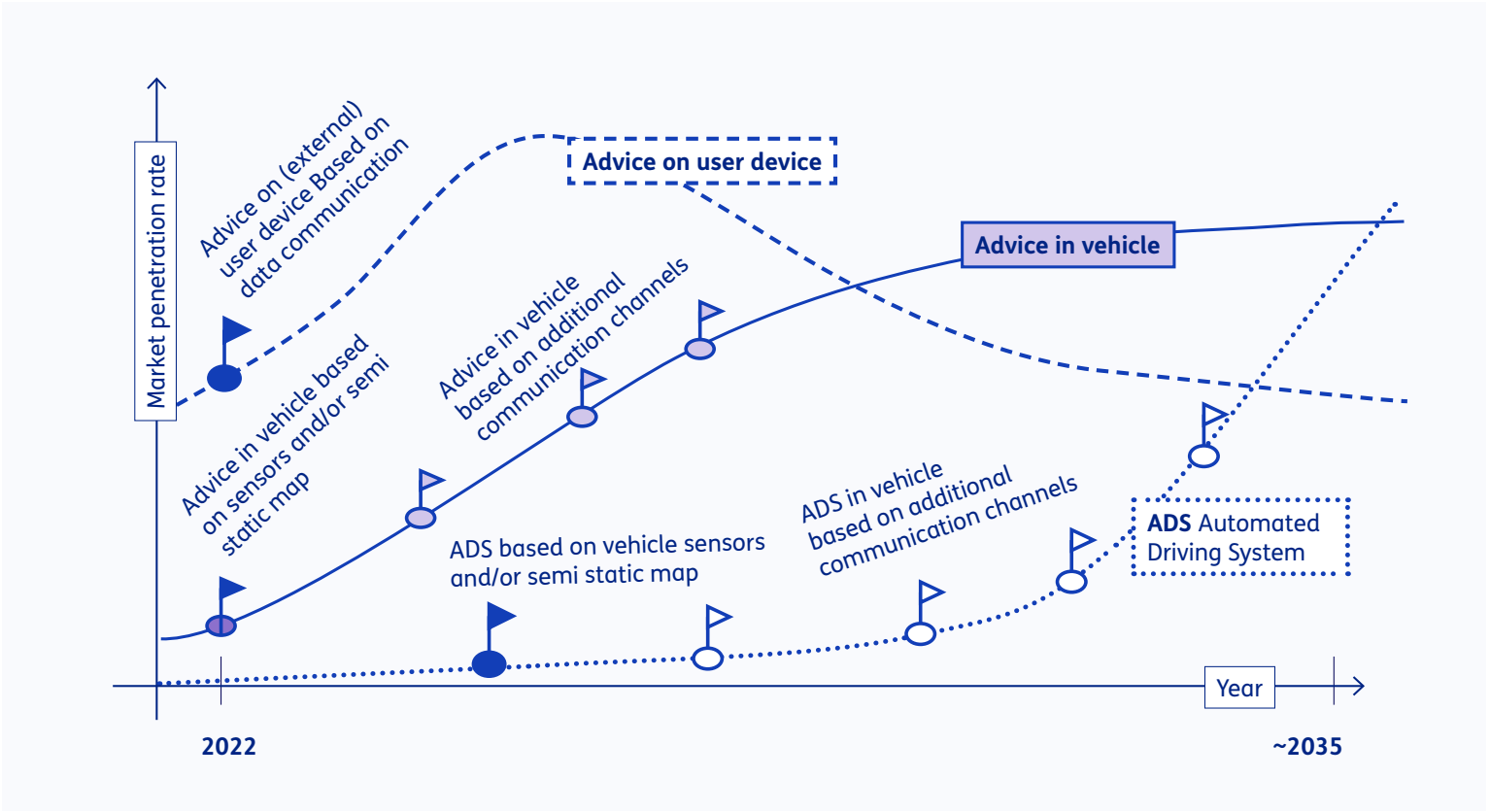


Figure 2. Expected timeline for market penetration rate of three information sharing systems in the automotive domain. Bron: TNO.

Figure 2 schematically shows the expected penetration rate of the three mechanisms over time. The dashed line is advice via the user's smartphone, while advice shown to the user by the vehicle itself is represented in solid line. Currently, the use of advanced advice systems on external devices is increasing, however it is expected to stall or even decline once vehicle-internal advice systems become more advanced and can integrate data from several sources. The dotted line represents automated driving systems. In the current situation, only advisory systems are being used, but in the future ADS systems are expected to be taken up widely, while the advice in vehicle usage is expected to level off.

These increasingly autonomous mechanisms require an increasing level of robustness and information security. The first two are pure information systems, where the final responsibility for taking action is assigned to the driver. However, users typically trust advice shown by the vehicle more (or more intuitively) than external devices, so there is a need for higher level of information quality for advise in vehicle compared to **advice on user device**.
The third mechanism, ADS, represents a cyber-physical system able to directly interact with its surroundings and therefore requires 100% trust in quality and integrity of the information.

4. Use cases in connected mobility system

Three specific connected mobility system services have been selected for this paper to serve as detailed exemplary use cases.

The intention for this approach is to give a representative – though not necessarily complete – picture of the cyber-automotive landscape and its main challenges. Our selected use cases are aimed to become relevant on different timelines as shown in Figure 2, for different stakeholders and with different communication technologies. Additional criteria for suitable use cases are:

- The use case involves security for physical traffic safety;
- the use case is urgent and crucial to be solved for future mobility concepts, but is not yet adequately addressed;
- the use case involves a high level of system-of-systems complexity;
- the use case is within the right-to-play of the Netherlands, that is, public and/or private parties are in a position to be able to solve (part of) the identified cybersecurity challenge.

A large collection of mobility services has been evaluated on these criteria and three services have been selected to give a representative view on cybersecurity challenges in the automotive sector:

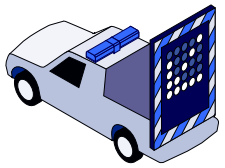
1. Early warning of ad-hoc lane-closure;
2. Intelligent Speed Assist (ISA);
3. Truck Platooning and Cooperative Adaptive Cruise Control (C-ACC).

Please note that this selection does not imply other services, such as traffic jam assist or priority at intersections to be less important. Our selection simply poses a starting point for a structured security analysis, which may later be extended to more services.

In the remainder of this section, the three selected use cases will be analysed. In particular, for each abovementioned service, our analysis includes:

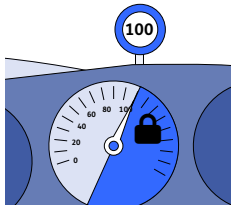
1. Technical description: what does the service do and what are the involved systems and stakeholders?

2. Communication analysis: what are and the communication and decision-making channels and where are the potential sensitivities?



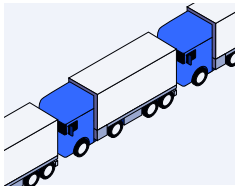
Lane Closure Warning

Timeline: Medium
Stakeholders: Mainly road authorities
Technology: Direct or cellular



Intelligent Speed Assist

Timeline: Now (Already there)
Stakeholders: Mainly OEMs, High in complexity and # stakeholders
Technology: Cellular or direct, several sources
Other: Indetification high due to well known ans widespead ISA tech



Truck Platooning and C-ACC

Timeline: Far, point on the horizon
Stakeholders:
Technology: Time-critical, sort range comm.
Other: Not clear yet whether, when and to which extent this service will become available

Figure 3. Selected mobility services for cybersecurity challenge analysis

Threat analysis reference model

For this analysis, we use a general reference model as shown in Figure 4. It is a layered model, in which each layer corresponds to an increasingly more specialised level of communication. For each layer the relevant systems are represented by coloured boxes, where different colours indicate that these systems are under control of different organisations.

The blue lines between coloured boxes represent the communication between systems. The purpose of using this reference model is to map the types of systems and the means of communication between those systems, in order to later identify attack vectors and their potential impacts.

In the model, a distinction is made between information systems and cyber-physical systems. This is because, due to differences in characteristics of these systems, the threats and impacts on these systems are also different.

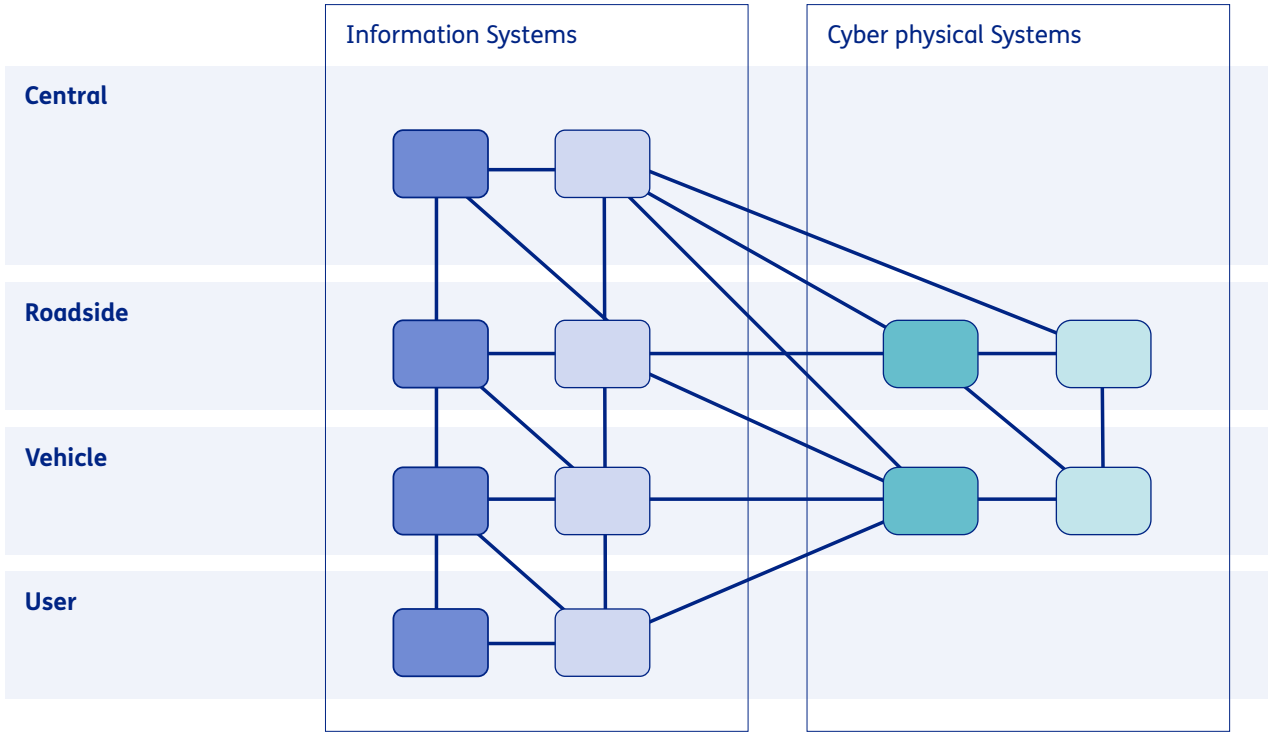


Figure 4. Threat analysis reference model.

Use case 1.
Early warning of ad-hoc lane-closure

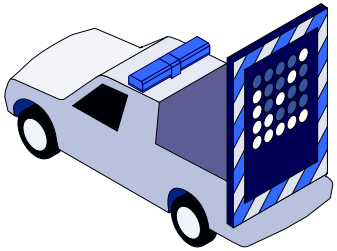


Figure 5. Stationary road operator vehicle near an accident / incident.

This use case concerns early warnings of ad-hoc lane-closure due to road operator vehicle in intervention (ROVI).

A ROVI is a vehicle from a road operator that stops near an accident to protect the site of the accident or is currently setting up equipment like lane delineation to protect the site. The road operator vehicle can be either on the hard shoulder or on the closed lane in front of the road works or accident, as shown in Figure 5. As traffic may approach the stationary ROVI with high speeds, this is a dangerous situation. It can result in near-misses and occasionally even collisions with the road works protection equipment or with the stationary vehicle, potentially causing human victims.

Sending an alert/warning to the approaching vehicles sufficiently in advance could prevent many dangerous situations. The approaching vehicles will be able to adapt their behaviour, e.g. by slowing down and / or changing lanes. Currently, this information can be used to inform the driver, such that the driver can adapt their behaviour based on the input. In the future, this information may also be shared to automatically adapt the speed and direction of a connected autonomous vehicle.

A warning will typically be generated at the incident site by equipment in the stationary ROVI. The warning can contain various information. This can be only a simple warning for a stationary ROVI, but also include more specific information, such as the exact location and lane of the road closure. Several communication channels, see also Figure 6, can be identified via which these warning messages are then delivered to the approaching vehicles:

1. The warning message is sent from the stationary ROVI to the back-office of the road operator using cellular communication. Once the warning arrives in the back-office, it can be further distributed in several ways:

A. To map providers and/or service providers, who forward these warnings to their customers using cellular communication* like LTE or 5G. For this set-up, both the road operator vehicles and the approaching vehicles would need to have cellular communication on board.

*Cellular communication, like LTE or 5G, typically can communicate over large distances.

B. To road users using shortrange communication** like ITS-G5 or C-V2X. For this, road side units (RSU) with shortrange communication capabilities will have to be used.

**Shortrange communication, like ITS-G5 or C-V2X, typically can communicate over shorter distances. Many connected mobility concepts, such as vehicle to vehicle (V2V) or infrastructure to vehicle (I2V), are based on shortrange communication.

C. To road users using cellular communication like LTE or 5G.

2. The warning message is sent from the stationary ROVI directly to the road users using short range communication, like ITS-G5 or C-V2X, between the road operator vehicle and the vehicles approaching.

In this case, both the road operator vehicles and the approaching vehicles would need to have on-board units (OBU) equipped with shortrange communication. It is also possible that combinations of these ways of communication will be used, resulting in multiple (similar/redundant) messages being received by the approaching vehicles. Please also note that, while not explicitly included in our analysis, there may also be physical tampering with RSU or ROVI equipment, or safety trailers from other parties instead of a ROVI.

Use case 1.
Early warning of ad-hoc lane-closure

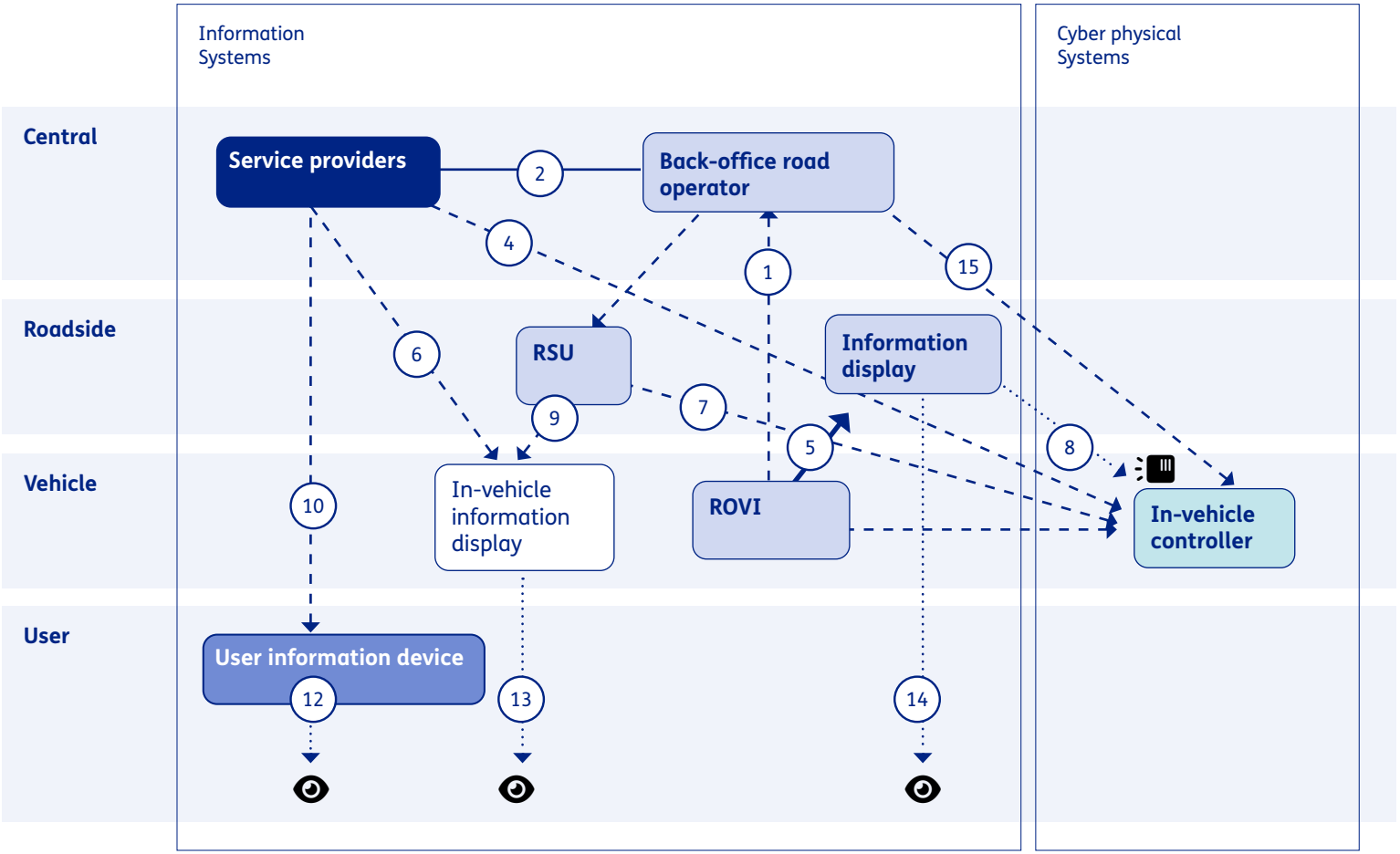


Figure 6. Overview of system elements and communication interactions for use case 1: Early warning of ad-hoc lane-closure

Use case 2.
Intelligent Speed Assist

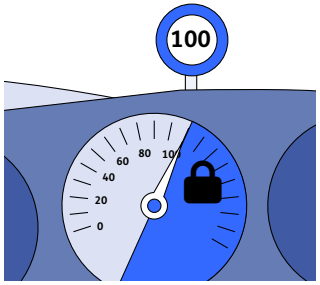


Figure 7. Schematic visualisation of Intelligent Speed Assist

Intelligent Speed Assist (ISA) can be defined as a smart system to assist the driver in maintaining the correct maximum speed of their vehicle at the current location.

The service informs the driver and/or the vehicle itself about the allowed maximum speed. This maximum speed can be time-dependent, type-of-vehicle dependent and/or location dependent.

ISA capability has become mandatory through the general vehicle safety regulation 2019/2144[6], though not yet for all vehicles. The following distinction has been made:

- From 6 July 2022 on for all new vehicle models and types introduced on the market;
- From July 2024 on for all new cars on the market;
- The ability to use ISA in the pre-existing vehicle fleet is not mandatory, but could be made available via after-market solutions.

It is left up to the vehicle manufacturer how to realize ISA. At the moment, ISA is typically implemented using traffic sign recognition in the vehicle itself by using cameras and/or by providing ISA information to the vehicle via input from map providers.

The map providers can use different sources to add the allowed maximum speed information to its maps. Two examples of an information source for map provides are:
1. Using traffic sign recognition information from vehicles and upload this towards map providers. Determining the allowed maximum speed using cameras and maps can be quite challenging, as the maximum speed can be time-dependent, type-of-vehicle dependent and/or location dependent. This is especially difficult considering that traffic signs can be unclear, missing, country-specific or even temporary.
2. Using (real-time) information from the road operator. The road operator has knowledge on the maximum allowed speed on its roads. This information can, if of sufficient quality, be included in the services of the map provider. Alternatively, the information from the road operators can be provided to the vehicle directly, without a map provider in between.

Several communication channels can be identified for how ISA information from the road operator could be delivered to the vehicle, complementing the information obtained by the vehicle sensors itself, see Figure 8. The information could be directly received from either the road operator, or from the service provider of the vehicle using the data of the road operator and/or the map provider.

The following communication channels exist for providing additional ISA information:
1. The ISA information is sent from the back-office of the service providers – using input from the road operator and/or the map provider – to their customers using cellular communication like LTE or 5G.
2. The ISA information is sent from the back-office of the road operator to road users using shortrange communication like ITS-G5 or C-V2X. For this setup, road side units (RSU) have to be used.
3. The ISA information is sent from the back-office of the road operator to road users using cellular communication like LTE or 5G, without a service provider in between.

It is also possible that combinations of these channels will be used, resulting in multiple similar or redundant messages being received by the vehicle. Authentication and authorization mechanisms may be used to determine which messages to use. These mechanisms can also filter out systems that should not be able to send messages in the first place.

Applying the same analysis methodology, we see several commonalities with the previous use case, especially the systems and communication lines. The effects of attacks will be somewhat different, due to the difference in objective for this use case. What remains more or less the same are the effects on user behaviour and general trust in the information provided by the individual systems and the use case as a whole.

Use case 2.
Intelligent Speed Assist

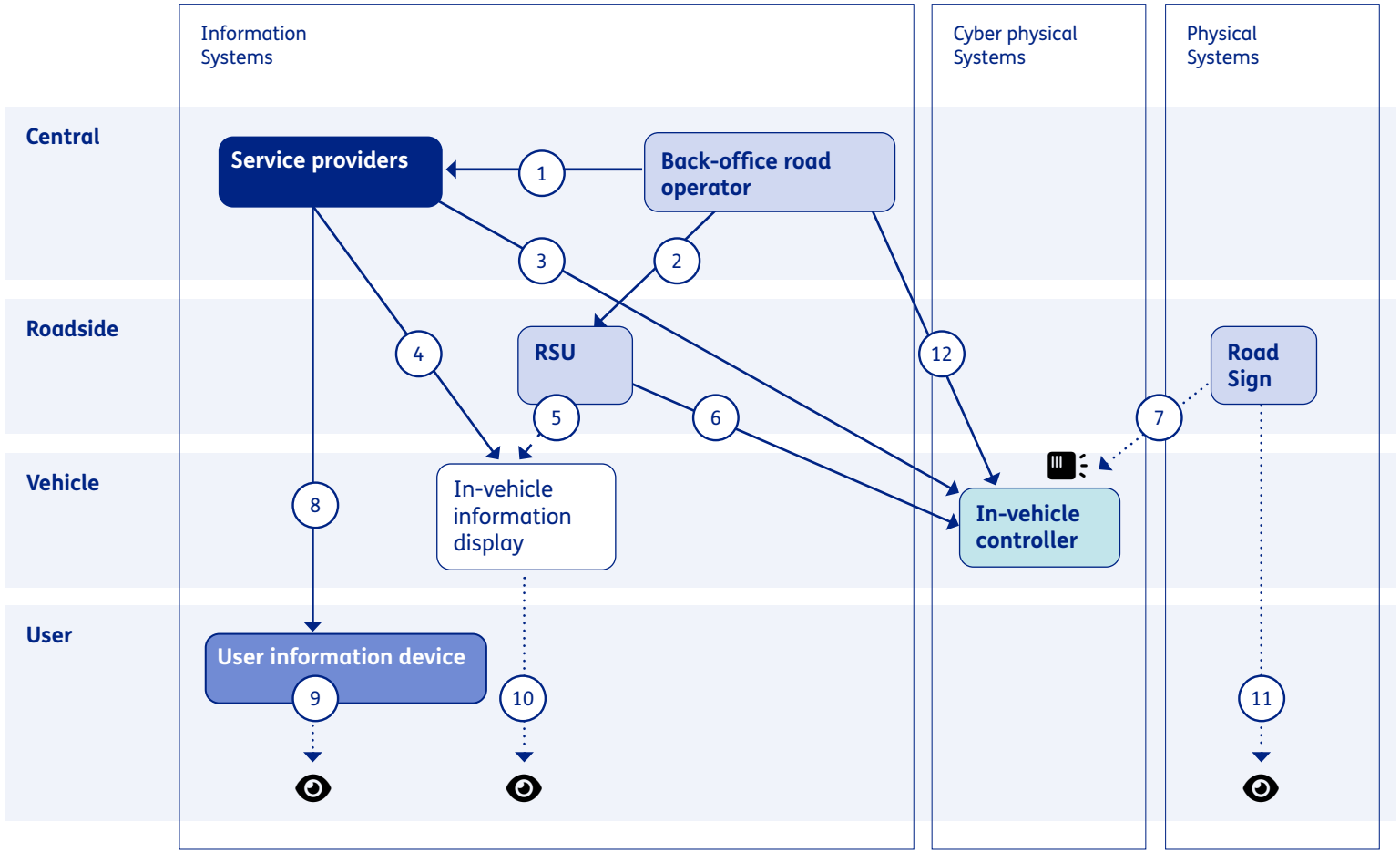


Figure 8. Overview of system elements and communication interactions for use case 2: Intelligent Speed Assist

Use case 3.
Truck Platooning and C-ACC

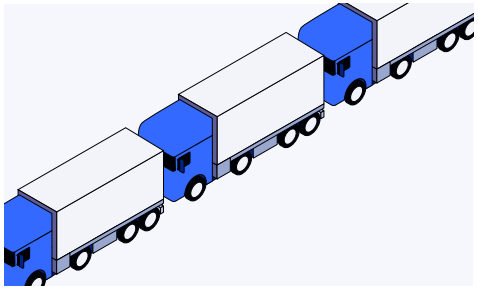


Figure 9. Visualisation of platooning trucks

Truck platooning is a cooperative application with trucks driving in a platoon at very short inter-truck distance.

The main goals for truck platooning are improved safety, cleaner and more efficient transport and increasing driver comfort. Truck platooning uses automated driving functions and vehicle to vehicle (V2V) communication to allow for very short following distances between the trucks, much closer then possible when manually driven, while respecting safety requirements. To support truck platooning, the V2V communication needs to be secure with a high level of assurance.

Comparable to platooning, but more often applied in passenger cars is cooperative adaptive cruise control (C-ACC). C-ACC is an extension of normal adaptive cruise control using V2V communication, in order to share vehicle control and state information in real-time. The C-ACC vehicle is “listening” to its preceding vehicle and using the received data for its own vehicle control. The received data can be combined with regular sensor information available from the vehicles own sensors and road infrastructure information via infrastructure to vehicle (I2V) communication.

Truck platooning and C-ACC are both cooperative road safety applications, as the vehicles are using and sharing real-time V2V data for vehicle control and decision-making functions. So, information technology and operational technology are converged. This use case highlights a significant transformation from driving computers to a network of driving computers. This transformation introduces complexity and new dependencies requiring new ICT solutions such as fast, cybersecure communications. As cooperative road safety applications are currently still in research, it is not yet clear whether and in which way exactly their deployment will take place.

I2V communication can also be used to connect additional platooning related services, for example priority services at signalized intersection or to provide an ISA-like service to the platoon. Within this use case the focus will be on the safety- and time-critical V2V communication, and less on the I2V communication or connected communication functions.

From a safety perspective the automation level for platooning is of importance. That is, whether platooning is an autonomous driving system or a driver assist function. Within the EU truck platooning project ENSEMBLE[7], two platooning levels were defined:
1. platooning support function (PSF):
PSF is an assist function with the driver responsible for the driving task, with automated controls; and
2. platooning autonomous function (PAF):
PAF is an automated driving system, where the lead truck driver is responsible for the driving task and following trucks are fully automated.

With ENSEMBLE, implementational work focused on the PSF-based solution, as it is the first to be expected to be introduced to market. Platooning communication protocols and V2V message sets were defined to support the needed platoon manoeuvring, platoon management and status functions. Figure 10 shows a high-level overview of the communication architecture for platooning.

The main information flow focusses on the V2V communication at vehicle level. This is the real-time information required for the PSF to operate. It is needed at individual vehicle level, at platooning level for operating and managing the system-of-vehicles, and for possible interactions with neighbouring vehicles. Shortrange communication is used to exchange the platooning messages. At the roadside level, shortrange I2V communication is possible to provide external information to the platoon, or V2I communication to share platoon information externally. This can, for example, help with interaction with traffic lights by giving priority to the platoon. On the central level, it is possible to use cellular communication to connect the platoon to external connecting services such as the OEM, fleet management services or navigation services.

Use case 3.
Truck Platooning and C-ACC

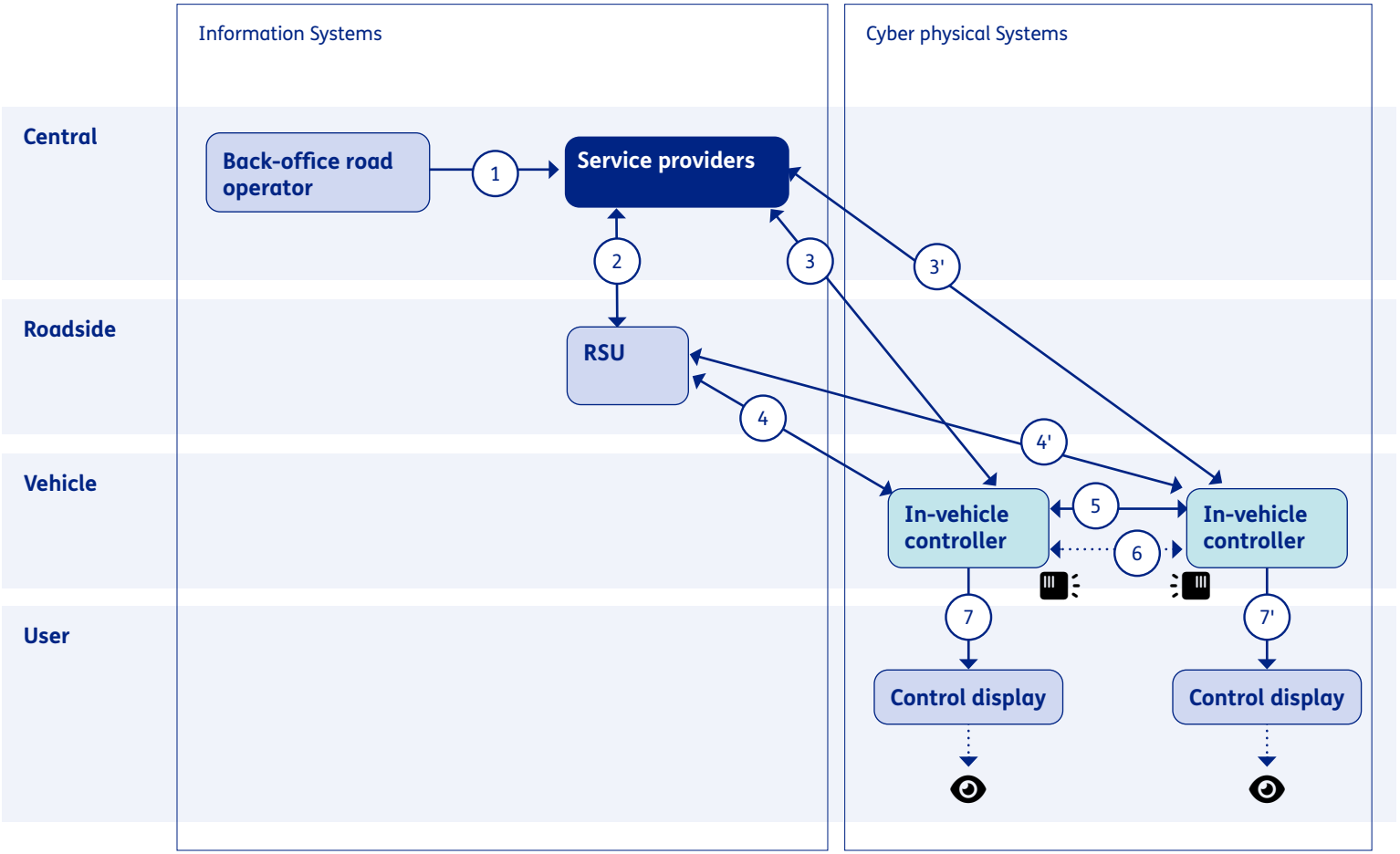


Figure 10. Overview of system elements and communication interactions for use case 3: platooning.

5. Threat analysis, state of the art & gaps in mitigation measures

In this section, a threat analysis is presented for the combined described use cases (UC) from Section 4. To start, table 2 on the left gives a general assessment of potential attackers and their motivations.

An attack can occur both on the individual systems as well as the communication between these systems. Depending on the implementation, the impact can either be limited to the system under attack or can propagate to other systems as well. We use the STRIDE model[8] for threat categorisation as shown in the table 2 on the right: Based on STRIDE, we analyzed the three use cases from Section 4.

The current state of the art regarding the cybersecurity aspects for the three selected use cases is summarized in Table 3 on page 14. Next to the current state of the art, the table also describes which next steps can be taken for mitigation and/or the tools that are currently missing.

Table 1.
General assessment of potential attackers and motivation examples

Actor	Motivation examples
Organised crime	Financial, attacking the availability of central systems for ransom.
State actors	Would attack assets in the system to gain certain foothold. Will try to stay below the radar and to not disrupt the system until state business would yield a benefit to exploit the obtained foothold.
Terrorists	Probably none
Cyber vandals and script kiddies	Trying to find weaknesses in the system, less attention to potential effects. Usually, best practices are sufficient to counter these actors.
Hacktivists	Trying to artificially block entire roads in order to protect the environment
Insiders	Disgruntled employee trying to harm (former) colleagues or to disrupt a use case, trying to find weaknesses in order to improve the system.
Researchers	Trying to find weaknesses in the system, for personal profiling, focussed on improving security or a combination of both.
Private organisations	Probably focussed on a specific asset, in order to obtain commercial advantage in relation to competitors.

Table 2.
STRIDE model

Category	Description
Spoofing	Illegally accessing and then using another user's authentication information, such as username and password
Tampering	Malicious modification of data, such as unauthorized changes made to persistent data held in a database, or the alteration of data as it flows between two computers over a network.
Repudiation	Associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations.
Information Disclosure	Exposure of information to individuals who are not supposed to have access to it, such as users that can read a file that they were not granted access to, or an intruder that can read data in transit between two computers.
Denial of Service (DoS)	Deny service to valid users, such as making a Web server temporarily unavailable or unusable.

Table 3. 1 Identify

STRIDE category	State of the Art	Next step
	All UCs: General risk assessment methodologies (TARA, etc)	**All UCs:** Information sharing on cybersecurity threats, vulnerability databases **Platooning:** TARA often focusses on platform-level or single vehicle level. System-of-systems or system-of-vehicles approach is still in research (low TRL)
Spoofing **Tampering**	**All UCs:** Security-by-design: Signing of messages, sensor/ network redundancy **Platooning:** Public Key Infrastructure (PKI), Encryption, also as part of ENSEMBLE security framework **All UCs:** Cloud network monitoring	**All UCs:** Standardisation of Cybersecurity Management System with auditing and monitoring options. Standards for information security (monitoring, diagnostics, smart response, recovery). Tooling for full lifecycle compliance testing. Timing analysis to prove compliance with Fault Tolerant Time Intervals (FTTI) in Automated Vehicles. **Platooning:** Standards for information security (monitoring, diagnostics, smart response) used for complex manoeuvring (e.g. CCAM supported platoon lane changes).
Repudiation	**All UCs:** Security-by-design: signing of (V2V, V2X, X2V) messages	**All UCs:** general cybersecurity logging, V2V logging
Information Disclosure	**Platooning:** Public Key Infrastructure (PKI), Encryption, also as part of ENSEMBLE security framework	**Platooning:** ENSEMBLE security framework is used as input to standards, but currently no standards available
Denial of Service	**All UCs:** Cloud network monitoring	**All UCs, mainly platooning:** In-vehicle network monitoring

Table 3. 2 Protect

STRIDE category	State of the Art	Next step
Spoofing **Tampering**	**All UCs:** System health monitoring: Parameter boundary checks & message frequency. Tampering detection based on message signing, message numbering, check sum.	**All UCs:** Anomaly detection based on input from redundant communication channels Plausibility checks using fused sensor data. **Platooning:** Advanced sensor attack detection.
Repudiation	**All UCs:** Detect signage errors/ fault	**All UCs:** Cybersecurity logging, **Platooning:** Misbehaviour Detection functionality
Information Disclosure		**Platooning:** Privacy protection in logging
Denial of Service	**All UCs:** V2X communication channel/ network load detection	**All UCs:** Multi-channel operation **Platooning:** redundant communication links/ technologies
Elevation of Privilege		**All UCs:** Tooling to detect illegal privileges

Table 3. 3 Detect

STRIDE category	State of the Art	Next step
Spoofing Tampering	**All UCs:** System health monitoring: Parameter boundary checks & message frequency. Tampering detection based on message signing, message numbering, check sum.	**All UCs:** Anomaly detection based on input from redundant communication channels Plausibility checks using fused sensor data. **Platooning:** Advanced sensor attack detection.
Repudiation	**All UCs:** Detect signage errors/ fault	**All UCs:** Cybersecurity logging, **Platooning:** Misbehaviour Detection functionality
Information Disclosure		**Platooning:** Privacy protection in logging
Denial of Service	**All UCs:** V2X communication channel/ network load detection	**All UCs:** Multi-channel operation **Platooning:** redundant communication links/ technologies
Elevation of Privilege		**All UCs:** Tooling to detect illegal privileges

Table 3. 4 Respond

STRIDE category	State of the Art	Next step
Spoofing Tampering	**All UCs:** Standardised response (pre-programmed) similar for all attacks (e.g. communication stop & key revocation). **Platooning:** Graceful degradation mechanisms: e.g. increase following distance (time-gap), disengage from platoon, manual hand-over	**Platooning:** Advanced root cause analysis and detection of which part of the system is attacked to isolate attack and enable smart mitigation actions. Standard on how to inform others when system is attacked (intra/extra platoon). **ROVI:** Advanced root cause analysis and detection on which parts of the system are deprecated to support smart response (only partial stop of communication). **ISA:** Advanced root cause analysis and detection which parts of the system are deprecated to support smart response (only partial stop of communication). Standard on how to inform others when system is attacked.
Repudiation	**ROVI & ISA:** Key revocation/ blacklisting	**Platooning:** Key re-vocation/blacklisting (increase in speed and integrity requirements)
Information Disclosure	**Platooning:** Advanced platoon joining mechanisms, PKI	**Platooning & ISA:** Advanced cybersecurity logging for incident response/post analysis (for Automated Vehicles)
Denial of Service	**Platooning:** graceful degradation mechanisms: e.g. increase following distance (time-gap), disengage from platoon, manual hand-over	**ROVI & ISA:** Use redundant communication channel **Platooning:** Change Secure communication channel for platooning, rekeying/key updates

Table 3. 5 Recover

STRIDE category	State of the Art	Next step
	ROVI & ISA: Key updates Platooning: Reduced platooning functionality	**All UCs:** Standardised mechanisms for recovery of cyber-attacks depending on which part of the system has been attacked/compromised.

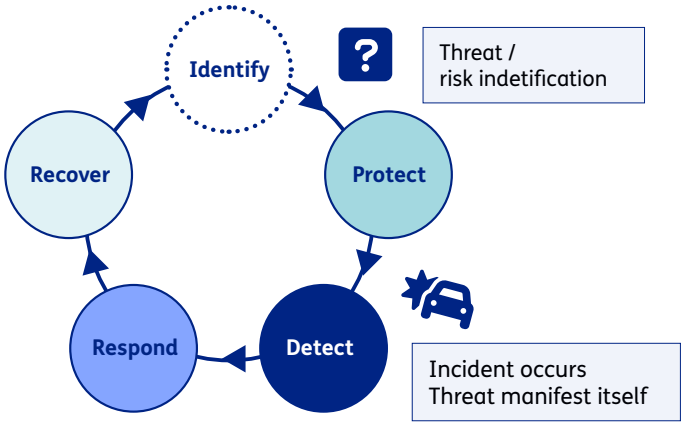


Figure 1. NIST Cybersecurity Framework, showing all five basic steps in cyber risk management.

Based on Table 3 above, the following general observations are made:

Spoofing attacks via cellular communication seem significantly less likely than via direct communication. Although there are countermeasures available, detecting spoofed messages depends on the implementation on the receiving end. Supporting the V2X standards does not automatically provide assurance that these implementations are protected against these attacks for cases in related to CPS and safety related mechanisms.

For some systems industry standards are applicable which guarantee a base level of security. However, an information system may have never been designed in accordance with the increasing integrity requirements related to cyber-physical systems. It can be secure by design, but may not be safe by design.

Whether or not non-repudiation needs to be considered depends mainly on how legislation will develop. At the current stage, messages are seen as advice with no legal binding. Establishing a legal status in a multi-vendor environment with high assurance requirements is a complex and potentially a costly endeavour.

Currently, information disclosure is mostly considered with regards to user privacy. In the future, when the safety of cyber-physical systems becomes dependent on information systems, a check is needed to see whether and how measures against information disclosure may impact the safety of cyber-physical systems.

Every communication interface is potentially vulnerable for a denial-of-service attacks, including wireless and wired communication.

The impact of escalation of privilege threats seems to be limited within the ROVI and ISA use cases. In general, privilege escalation becomes relevant when implementing authentication and authorization mechanisms i.e. at RSU's.

To close the complete NIST cybersecurity cycle (see Figure 1) for the entire vehicle lifecycle, several steps and protocols need to be standardized to make them applicable for automated driving. In the current state of the art, some standards and certifications are still lacking. For instance, system providers are currently not requested to share detailed information about their implementation.

The responsibilities for cybersecurity aspects are currently not well enough defined and a governmental monitoring organisation is not structurally in place. Security and risk analysis methods are often used for the implementation of standards. However, these do not seem to cover all NIST steps (e.g. response and recovery are not defined).

Regarding specific technical security tooling, we see that in the current state of the art, tooling is being developed and becoming available on the market for original equipment manufacturers (OEMs) and their supply-chain by companies already offering other automotive tooling. OEMs do have several of these capabilities with security tooling developed in-house or through specialized suppliers. For the design phase, various security consultancy and/or engineering services are being offered. This is often in the context to evaluate compliance to UNECE WP 29 regulations and ISO/SAE 21434 requirements for type approval. Consultancy- and automotive tooling companies sometimes also offer services related to automotive cybersecurity auditing and testing, and/or training services for automotive cybersecurity.

For verification and validation, testing equipment for hard- and software is specifically being designed or existing test setups are extended with security specific functionalities, for example with functional security testing, fuzzing or penetration testing. After production, a few companies offer product security incident response (PSIRT) teams and vehicle security operating centre (VSOC) services.

The available and developing technical security tooling mentioned above, however, shows different maturity levels across the market and is structurally not standardised, not integrated across several supply chain actors and not widely available in the market. Large players who have their own security tooling available, typically act on their own, define their own technical standards and do not typically share information. This can be motived by a lack of trust or for competitive advantage. As an example, the market shows a lack of experience with V2X specific security clients, and no common approach in assessing security/safety design and testing of these clients. Systems are therefore not interoperable, and security is not addressed at system-level.

Learning frameworks for assessing Vehicle Safety and Security (VSSF) are currently under development by the road authorities. The maturity of tooling and functionalities (e.g. in-vehicle intrusion detection systems or integrating safety and security) is still low. Furthermore, detection of still unknown sector-specific vulnerabilities and attacks will always remain a topic of research, as new threats will keep evolving. The maturity in this area is growing, but other research shows that leveraging these detection functions to a system-of-systems level requires further and broader collaboration across the industry. Security management should cover the in-vehicle systems, network connectivity and back-end systems. In general, integrated safety and security tooling is a challenge on its own, and even more complex for systems-of-systems.

On the organisational aspects, defining the responsibilities for cybersecurity aspects (especially for connected mobility systems) seems to be a significant bottleneck in the collaboration between system suppliers and governments. As a result, resolving the responsibilities and setting up organisational structures for collaboration seem to be the most pressing steps forward, followed by efforts on standardisation and structural information sharing to address the challenges of interoperability and maturity differences. With this in place, advanced security tooling needs to be (further) developed and integrated across the supply- and service chain.

6. Research challenges for automotive cybersecurity

Our analysis shows that based on the three selected use cases several aspects are acting as bottlenecks for the uptake of new (connected) mobility system concepts:

1. We expect a need to augment security-by-design with safety-by-design when connecting information systems directly or indirectly to cyber-physical-systems.

Currently, most systems are designed using principles and assurance requirements from either an information system (IS) or a cyber-physical system (CPS) perspective. Despite some similarities, their design properties are not the same. To take into account the increasing interaction between IS and CPS, their safety requirements need to be re-evaluated and/or re-designed. Assurance may not be sufficient in case where existing and proven functionality gets implemented for new safety-related technologies and purposes that were not foreseen when the functionality was originally assessed.

2. We expect differences in cybersecurity maturity of organizations in the automotive value chain

Observing the use cases from an organizational perspective, we see numerous organizations around the globe involved in the life cycle of various mobility systems. These organizations need to identify and implement changes related to the cybersecurity standards and best practices. Due to differences in the speed of adaptation, however, we cannot assume all systems to be at the same maturity level, even on a smaller European scale. This is not only the case for security and safety by design, but also for the other steps in the cybersecurity life cycle (e.g. detect, respond, and recover).

3. When both information systems and cyber-physical systems connect, the differences in maturity will cause unexpected and undesirable effects.

Where IS increasingly interact with CPS into an overall system-of-systems, an integrated fit-for-purpose approach is needed to achieve both safety-by-design and security-by-design. This requires re-evaluations and redesigns with a main focus on the increased integrity requirements. This is necessary to ensure that the resulting system-of-systems is not only secure, but also safe-by-design for the whole cybersecurity loop. Here, we see a challenge in bringing the right knowledge and expertise together in a scalable way. While there are more and more initiatives to bring together safety- and security knowledge, we still see wide variations in maturity across the domain. Initiatives should focus on closing and speeding up the cybersecurity loop both on an individual organizational level, and maybe even more importantly, the ability to automate the loop across the resulting system-of-systems.

Research challenges for automotive cybersecurity

4. We expect the automotive industry to be ahead of the digital road infrastructure (DRI) industry in cybersecurity maturity, due to the automotive industry being organized globally and the DRI industry being organized mainly locally.

With the progression of the use cases, more communication is being introduced between systems that are currently not communicating e.g. vehicle to vehicle, and vehicle to infrastructure. As a result, the cybersecurity loop needs to be extended from single systems to a systems-of-systems approach. Naturally, this involves multiple organizations. Here, we observe a difference in maturity between the automotive industry and the DRI industry. In initiatives such as the Automotive ISAC (Information Sharing & Analysis Center), OEMs are increasing their collaboration in sharing security knowledge and best practices. In the DRI domain we see some collaboration initiatives, but on a much more local (national) scale. A more EU focused approach is needed to be effective when moving from SAE level 2 to SAE level 3 for cooperative driving uses cases. Currently there are only limited collaboration on local road side level in EU wide initiatives. This means that response and recover maturity are hampered when moving to advice in vehicle and ADS in relation to the number of organizations involved.

Closing the cybersecurity loop on a systems-of-systems scale is in progress, but we expect the overall maturity to be not yet sufficient, especially in the areas of respond and recover. Due to the nature of cybersecurity incidents, it is a key effort to speed up the cybersecurity loop. This requires a high level of automation crossing both information and cyber physical systems, which is currently not yet available. There are initiatives on a local scale, but closing the loop for the presented use cases needs both a larger scale and an increase in speed in cases where safety is a crucial factor.

7. Conclusions and solution directions

Cybersecurity can be a 'showstopper' for the further introduction of new smart mobility systems. In particular, in cases where the lack of cybersecurity endangers road safety.

The window of opportunity is now: Security adjustments that are made too late will result in sub-optimal solutions.

The goal should be to combine security-by-design with safety-by-design that can be implemented at a sufficiently high system level. The domain as a whole is rapidly moving to use cases where technical and organizational designs are challenging but very important. Note that this is not only about technology at a system level, but also about organising processes and responsibilities at a system-of-systems level.

To address both safety and security, collaboration on European level is essential to ensure compatibility. Road authorities and governments will play an important role in development, assessment and certification of these complex eco-systems. This will have to be done together with the automotive and digital road side industry players, to cover the whole eco-ecosystem. Governments must get organised, on all levels, and take initiative by clearly defining roles and responsibilities and set up common initiatives and standardisation efforts. Encourage and facilitate information sharing and collaboration both from an organisational and technical point of view, between OEMs but also specifically between OEMs and the road side infrastructure. Regarding sharing information and cybersecurity knowledge, existing concepts from IT security that may be adapted to the automotive domain are: ISACs (Information Sharing & Analysis Centers), more technical TISCs (Threat Intel Sharing Groups), and crisis exercises.

In the current complex systems, the weakest link determines the vulnerability of the whole system. Due to the fact there are many interlinked components from several independent vendors, the system can be vulnerable on several levels. It is important to realise that not all cybersecurity issues/problems can be prevented upfront. Cybersecurity becomes more cyber resilience. It is therefore important to have the whole NIST framework in place, with the detection, respond and recover steps in addition to identify and protect steps, to anticipate with this. Also this will have to be done with all stakeholders in the ecosystem. Therefore, collaboration is essential to ensure that the right security level is in place and security-by-design principles are applied at all levels (on both technical and organisational level). All stakeholders have to invest to ensure safety on the system level instead of on subsystem level.

From experience in large R&D projects on digital infrastructure where cybersecurity is an integral part of the technologies and solutions, we see an increasing need to set up collaborative efforts on security and safety in this domain. Not only to prevent cybersecurity incidents, but maybe more important to achieve the full potential of sustainable future use cases. There is no single party that is able to solve the described challenges by themselves. TNO can support companies and governments to identify potential vulnerabilities and provide advice on possible solutions and support collaborative technology development required to prevent and mitigate cyberattacks, make the system more resilient. Especially in the context of a broad system-of-systems solution perspective.

TNO offers companies, organisations and governments the ability to:

Develop knowledge to support the design and implementation of detection, prevention & safe mitigation systems;

Develop knowledge on applications to define the performance requirements of security and resilience measures and analyse different concept implementations,

Explore sensor and communication attack tooling to assess the resilience of automotive systems,

Develop the knowledge to build the safety and cybersecurity case of novel AD/ADAS and connected applications in the automotive system domain,

Explore the requirements of cybersecurity logging and management systems for future applications.

The authors of this position paper invite you to cooperate with TNO on building a safe and secure future for new (connected) mobility systems.

References

[1] U. Nations, „UN Regulation No. 155 - Cyber security and cyber security management system," March 2021. [Online]. Available: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security.

[2] „UN Regulation No. 156 - Software update and software update management system," March 2021. [Online]. Available: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update.

[3] Cyberveilig Nederland i.s.m. Cybersecurity Alliantie, Cybersecurity Woordenboek. Van cybersecurity naar Nederlands, 2021.

[4] ISO/IEC, „ISO/IEC 13888-1:2020 Information security — Non-repudiation," ISO, ISO/IEC 13888-1:2020, 2020.

[5] IEEE, IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries, New York (USA), 1990.

[6] European Parliament, „Type-approval requirements to ensure the general safety of vehicles and the protection of vulnerable road users," 2019.

[7] ENSEMBLE is a Horizon 2020 project on truck platooning, see Homepage: https://platooningensemble.eu/

[8] „reference SECREDAS D3-8 Security analysis report v2".

[9] ENISA, „Hardware Threat Landscape and Good Practice Guide," 2017.

[10] United Nations, Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, 2021.

[11] ISO/IEC, „ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls," ISO, 2022.

[12] SAE International, „Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles," SAE International, 2018.

Authors
Yoram Meijaard
André Smulders
Frank Benders
Jacco van de Sluis
Peter-Paul Schackmann
Bastiaan Wissingh
Shari Finner
Joëlle van den Broek

Contact
Hein Franken

Senior Business Development Manager
Mobility & Built Environment

hein.franken@tno.nl
+31 615 438 683
https://www.linkedin.com/in/heinfranken

We are committed to ensuring that current and future generations can live, work and travel in a safe and sustainable living environment. This is summed up in our purpose, the statement that encapsulates our intent: 'A liveable future for all'. We envision a world without calamities, emissions and loss.

TNO innovation for life