Computers & Security 140 (2024) 103798



Contents lists available at ScienceDirect

Computers & Security

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





TOMSAC - Methodology for trade-off management between automotive safety and cyber security

Giedre Sabaliauskaite [a,*], Jeremy Bryans [b], Hesamaldin Jadidbonab [b], Farhan Ahmad [c], Siraj Shaikh [a], Paul Wooderson [d]

[a] Systems Security Group (SSG), Department of Computer Science, The Computational Foundry, Swansea University Bay Campus, Fabian Way, Swansea, SA1 8EN, UK
[b] Centre for Future Transport and Cities, Coventry University, Coventry, CV1 2TE, UK
[c] Department of Computer Science, School of Computing and Engineering, University of Huddersfield, Queensgate, Huddersfield, HD1 3DH, UK
[d] HORIBA MIRA Limited, Nuneaton, CV10 0TU, UK

ABSTRACT

Safety and security interdependencies have been of interest for researchers for several decades. However, in practice, they are not given the necessary consideration yet due to various reasons, such as lack of understanding and reluctance to change current practices. This research is aimed at advancing the state of the art in this area by developing a practical, easy to adapt and to use methodology for managing interdependencies and trade-offs throughout the development lifetime of cyber physical systems. The methodology is named TOMSAC, short for Trade-Off Management between Safety And Cyber security.

1. Introduction

A good general survey of co-engineering methods for safety and cyber security across the entire cyber-physical domain is given by Kavallieratos et al. (2020). It provides a comprehensive survey of 68 safety and cyber security co-engineering methods and discusses relevant open issues and research challenges. The 68 methods are categorised as "integrated" (i.e. two separate interrelated safety and security processes) or "unified" (i.e. one unified process combining both safety and security). 37 of the reviewed methods are integrated, and 31 are unified. The majority of the methods reviewed are model-based (52 out of 68) and are developed for a single application domain (45). Only 20 methods are informed by relevant standards, and interestingly the majority of reviewed methods (49) do not address the issue of conflict-resolution. Only 28 methods include techniques to communicate results to stakeholders, while the majority (41) are not supported by any software tool or toolkit. Taken together, these results suggest that the field of cyber security and safety co-engineering is far from mature.

Eames and Moffett (1999) make the point that there are disadvantages to approaches that attempt to unify safety and security analysis techniques concluding (re 'unification') that "in the majority of situations it is inappropriate to attempt to unify safety and security risk analysis techniques." Regarding 'integration' they conclude that "the value in integrating safety and security lies with harmonising techniques from each domain." This approach (integration) allows the specialised techniques from both the safety and security domain to remain unchanged, and the specialist expertise does not need to be retrained.

The AQUAS (Pomante et al., 2019) project began by trying to investigate the inter-dependence of safety, security and performance in the context of the increasing complexity caused by linking the open world and the embedded world. They set this work in five different domains (Air Traffic Management, Medical Devices, Rail Carriages, Industrial drive and Space multicore architectures).

A key contribution of AQUAS was to advance, where relevant, a combined approach for standards beyond the current state of the art. This was done by evolving the concept and practice of the security informed safety case with impact on performance taken into consideration. Implications for Systems of Systems were also drawn out. The AQUAS paper is closest to our approach, which is restricted to the automotive domain.

Looking specifically within the automotive domain, as early as 2013 Bloomfield et al. (2013) were working on "security-informed safety" based on the impact that security might have on structured safety cases. They point out the challenges facing an interworking of security and safety, including the need for a common ontology, the differences between the principles that underpin the areas, the differing underlying threat models, and the need for a common approach to the safety and

* Corresponding author.
E-mail addresses: g.sabaliauskaite@swansea.ac.uk (G. Sabaliauskaite), jeremy.bryans@coventry.ac.uk (J. Bryans), ad4953@coventry.ac.uk (H. Jadidbonab), farhanahmad@outlook.com (F. Ahmad), s.a.shaikh@swansea.ac.uk (S. Shaikh), paul.wooderson@horiba-mira.com (P. Wooderson).

https://doi.org/10.1016/j.cose.2024.103798
Received 15 December 2023; Received in revised form 20 February 2024; Accepted 1 March 2024
Available online 7 March 2024
0167-4048/© 2024 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

security standards. This interest resulted in Robin Bloomfield and others from his company writing the BSI code of practice PAS:11281 "to provide recommendations for managing security risks that might lead to a compromise of safety in a connected automotive ecosystem" (B. S. Institution, 2018).

More recently, cybersecurity has become a regulated area for several vehicle categories, including passenger cars, buses and trucks. UN Regulations 155 (UNECE, 2021a) and 156 (UNECE, 2021b) specify requirements for cybersecurity and software updates respectively, which manufacturers must meet in order to be granted type approval for those vehicles in countries that implement the regulations. In particular, the EU has implemented UN R155 as part of the General Safety Regulation (GSR2), further establishing the important role that cybersecurity plays in overall safety. Compliance with R155 is also required as part of other UNECE regulations including R157 (UNECE, 2021c) on the type approval of Automated Lane Keeping Systems (ALKS), which requires consideration of "cyber-attacks having an impact on the safety of the vehicle."

In August 2021, the new international standard ISO/SAE 21434 "Road vehicles – Cybersecurity engineering" (ISO/SAE, 2021a) was published to support the practical implementation of UN R155. This document was developed by experts from across the automotive industry including vehicle manufacturers, the tiered supply chain, cybersecurity consultants and government organisations. It is now in widespread use by the automotive industry as the state-of-the-art for cybersecurity engineering, providing guidance on implementing a cybersecurity management system and carrying out the cybersecurity activities needed to support compliance with UN R155. ISO/SAE 21434 explicitly requires organisations to identify other engineering disciplines that interact with cybersecurity, such as functional safety, and establish communication channels between those disciplines. In addition, the international standard ISO 26262 for functional safety (ISO, 2018) contains a reciprocal requirement to identify interactions and establish communication channels between functional safety and cybersecurity. The strong relationship particularly between cybersecurity and functional safety can be seen in the way the two standards ISO/SAE 21434 and ISO 26262 share common elements of the process frameworks they define, for example the aligned lifecycle phases and risk management approach.

Within automotive, the first area in which the safety / cyber security trade-off became apparent was within the area of the CAN bus. This bus was designed for inter-ECU communication. It was defined without security in mind and with very high reliability. Kleberger et al. (2011) provide an overview of in-vehicle security threats and potential protections with respect to the CAN network.

Authenticity is an important security requirement for automotive systems, and many software or hardware authentication solutions are surveyed in Kleberger et al. (2011). Of these solutions, Message Authentication Code (MAC) is the key technique. The limited bandwidth and payload size of the CAN protocol means those techniques tend to be lightweight in order to keep other design requirements satisfied. Since CAN is primarily a protocol designed for safety, this can be seen as an early step in trading off between safety and security requirements.

Lin and Yu (2016) give a good review of safety and security trade-offs looking at TTEthernet (Time Triggered Ethernet). This is seen as one of the competitors to replace the CAN bus, although the authors use TTEthernet as a communication medium between vehicles, rather than inside them. They look at three use cases: secret key management, frame replication and elimination, and Virtual Local Area Network (VLAN) segmentation.

Apvrille and Li (2019) work on the basis that a single person (or a single team) is responsible for the initial design of the system, and so it is relatively straightforward to harmonise safety, security and performance requirements. TTool (Apvrille, 2008) (their tool of choice) keeps the entire modelling and verification process in a single toolkit, which is carried out simultaneously for safety, security and performance requirements. Apvrille and Li (2019) note that the soundness of the model transformation for ProVerif is partially proved. They also offer Design Space Exploration within their work. But by looking at security, safety and performance separately it seems that they then lose out on any chance to exploit interdependencies between these. They propose making one of security, safety or performance a primary requirement of the tool, and provide ways to deal with unsatisfied elements from the other two. This is an indication that the paper (although it uses vehicles in the case study) is in fact focused at the moment on smaller CPS sectors. Our work is very much focused on vehicles at the moment, and we look at the question of comparing the interrelationships of safety and security from their point of view.

Looking more widely than communication technologies, in Huber et al. (2018) the authors look at how organizations from the automotive industry "tackle the challenge of integrating safety and security aspects during system development." Their overall conclusion is that currently "there are significant deficits in the integration of both domains." The authors present an exploratory survey (restricted to Europe) of integrating safety and security aspects during system development within the automotive industry. Four key findings (KFs) emerged from this study:

(KF1) the majority of (automotive) organizations do not actively take interdependencies between safety and security requirements into account.
(KF2) prevalent problems concerning complexity, traceability change management and availability of resources complicate the integration of security.
(KF3) the objectives of both the security domain and the safety domain span across multiple organizations.
(KF4) there is a relatively uniform understanding and general awareness within the organisations concerning the fundamental differences between the safety and security domain.

The conclusion from these key findings was the need for a holistic model that unifies documentation artifacts in order to reduce complexity and facilitate effective change management.

Four types of interactions between safety and security have been introduced by Pièvre-Cambacédès (2010) (in French), and then published by Kriaa et al. (2015). These interactions include:

(1) Conditional dependency: fulfilment of safety requirements is a condition for security, or vice versa;
(2) Mutual reinforcement: safety requirements or measures increase security, or vice-versa;
(3) Antagonism: safety and security requirements or measures conflict with each other;
(4) Independency: no interaction.

Kolb et al. (2021) argue that more rigorous definitions of safety and cyber security are needed, which would consider:

- Directionality: are safety and security uni-directional or bi-directional and from which direction do they flow?
- Intensity: for a quantifiable co-analysis, the intensity of these interactions has to be considered.
- Nature of the interaction: for each of the possible interactions, from influence to dependency or antagonism, accounting for the positive or negative impact of such an interaction is fundamental. Moreover, conditional dependencies raise the question of who is responsible for actions when safety and security are heavily dependent.

Kolb et al. (2021) performed comparative analysis of 14 methods for model-based safety and security co-analysis. The following are the key findings/challenges:

- Most methods combine attack trees and fault trees.

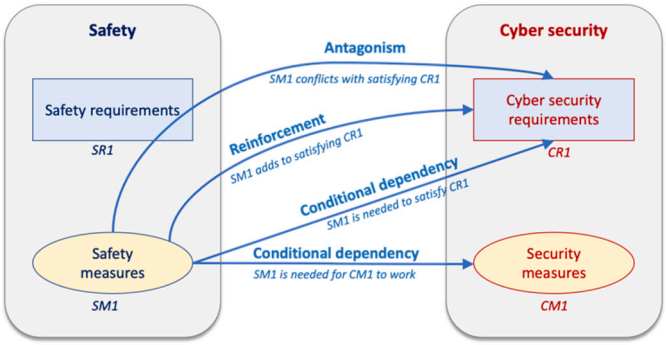


Fig. 1. The Impact of Safety Measures on Cyber Security.

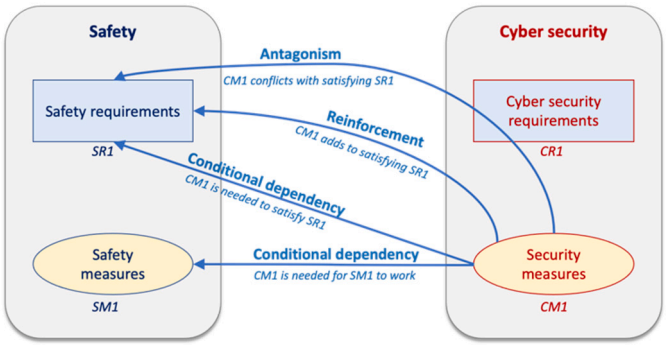


Fig. 2. The Impact of Cyber Security Measures on Safety.

- No novel constructs for capturing safety-security interactions are introduced. Instead, the existing constructs for safety and security modelling are merged.
- Safety and security interactions are not fully understood yet.
- No novel metrics have been proposed to quantify safety-security interactions.
- No large case studies on safety/security co-analysis were carried out.

The overall aim of our research is to continue to address these challenges.

2. Safety and cyber security interdependencies

Figs. 1 and 2 show the interdependencies between safety and cyber security measures and requirements. Fig. 1 shows the impact of safety measures on cyber security, while Fig. 2 the impact of cyber security measures on safety. Three types of relationships, defined in Piètre-Cambacédès (2010), Kriaa et al. (2015), are depicted in Figs. 1 and 2: antagonism, reinforcement, and conditional dependency.

In addition to interdependencies between the safety and cyber security requirement and measure levels, there could be dependencies between the failure and attack levels as well. E.g., a safety failure could contribute to enabling a security attack, or vice versa. Furthermore, a safety failure could block a security attack, or vice versa. Thus, two new types of relationships can be defined: “enabling” and “blocking”. We have expanded the initial classification of safety and security interdependencies, proposed in Kolb et al. (2021), and added “enabling” and “blocking” relationships, as shown in Fig. 3.

Along with relationship types, Fig. 3 includes various factors, relevant for all relationship types, such as:

- Direction – there are two directions, either from safety to security (the effect of safety on security), or vice versa.
- Intensity – the measure of the intensity of the interdependency.
- Methods/models – various methods and models to facilitate the analysis of interdependencies.

The aim of our work is to present a method that allows the relationship between safety and cyber security to be considered together at each stage of the Cyber Physical System (CPS) lifecycle, and that will highlight the interaction between them both.

3. Methodology overview

Fig. 5 shows the framework of TOMSAC methodology, which includes:

- lifecycle phases of CPS;
- teams involved in the development process, such as design/development, safety and cyber security teams, suppliers and users;
- synchronization points at different lifecycle phases for teams to align their work products and make trade-offs, if necessary.

There are numerous teams involved in CPS development, such as developers, safety team, cyber security team, etc., who follow their own standards, have different processes, develop different work products, and, even speak different languages, or use the same terms to mean different things, which makes it difficult for them to fully understand each other and integrate their work results. The aim of the TOMSAC methodology is to provide these teams with a unified framework to facilitate communication and alignment of their work.

4. The TOMSAC methodology tailored for the automotive domain

The automotive sector, more precisely, automated road vehicles, is our main area of expertise. Thus, we will first tailor the TOMSAC methodology to this sector. Lifecycle phases are therefore adjusted to the ISO 26262 (ISO, 2018) and ISO/SAE 21434 (ISO/SAE, 2021a) activities. ISO 26262 is road vehicle functional safety standard, while ISO/SAE 21434 is the cyber security standard. Both ISO 26262 and ISO/SAE 21434 require the identification of related disciplines and to establish and maintain communication channels between those disciplines. ISO 26262 explicitly mentions cybersecurity, and similarly ISO/SAE 21434 identifies functional safety as related disciplines.

The following sub-sections describe the application of the TOMSAC methodology to the automotive concept and product development phases.

4.1. Trade-off management during concept phase

Fig. 4 includes an overview of the TOMSAC methodology applied to automotive development concept phase.

In this phase, the automotive Original Equipment Manufacturers (OEMs) or the teams involved share responsibilities, and develop a system concept model. As part of the system concept model they would carry out an initial risk assessment concluding by agreeing on the associated safety and cybersecurity requirements and measures.

As we can see from Fig. 4, there are three teams involved in this phase: development, safety, and cyber security. We propose three synchronization points in this phase for teams to align their work products and make any necessary trade-offs.

4.1.1. Synchronization point (1): agreed roles, responsibilities, regulations

At this point, a meeting should be organized among all teams to agree on how they will coordinate their work. The agreement could include the defined roles, responsibilities, regulations they will follow, schedules, and so on.

4.1.2. Synchronization point (2): agreed safety and cyber security goals

It is useful to have a synchronization point at the end of risk assessment, when safety and cyber security goals (high-level requirements)

Relationship type / Factors	I. Interactions between safety requirements or measures and security requirements or measures			II. Interactions between safety failures and security attacks	
	(a) Conditional dependency: fulfilment of safety requirements is a condition for security, or vice versa	(b) Reinforcement: safety requirements or measures increase security, or vice-versa	(c) Antagonism: safety and security requirements or measures conflict with each other	(d) Enabling: safety failure enables security attack, or vice versa	(e) Blocking: safety failure blocks security attack, or vice versa
Direction	Safety -> Security Security -> Safety	Safety -> Security Security -> Safety	Safety -> Security Security -> Safety	Safety -> Security Security -> Safety	Safety -> Security Security -> Safety
Intensity	If requirement is not fulfilled, how strong is the effect?	How big is the increase?	How strong is the conflict?	What is the probability?	What is the probability?
Methods/ Models	Interdependency identification; Trade-off analysis	Interdependency identification; Trade-off analysis	Interdependency identification; Trade-off analysis	Interdependency identification; Trade-off analysis	Interdependency identification; Trade-off analysis

Fig. 3. Safety and security interdependencies.

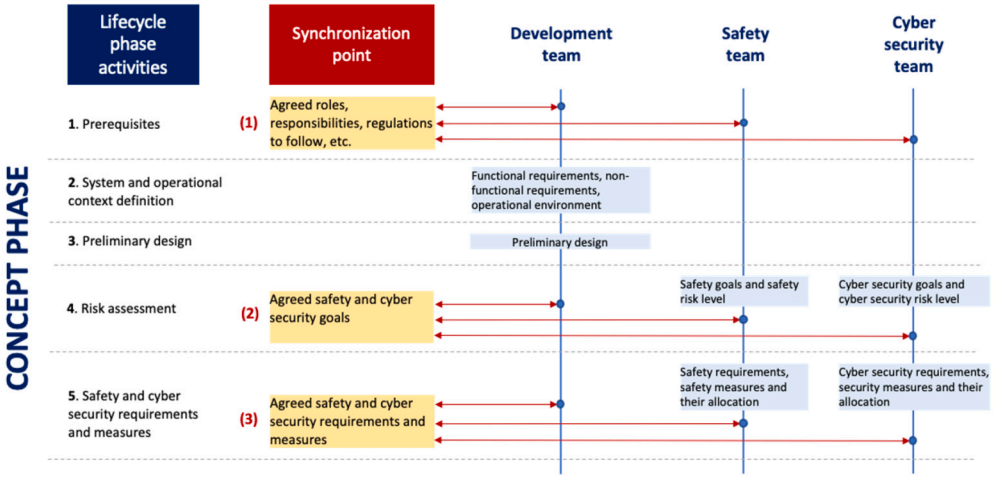


Fig. 4. The concept phase activities and synchronization points between development, safety, and cyber security teams.

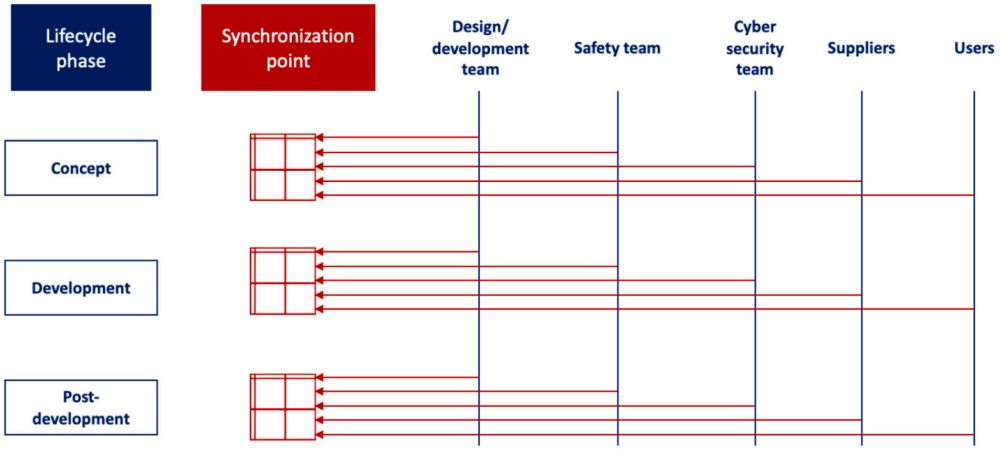


Fig. 5. The lifecycle phases of CPS, the teams involved and the synchronisation/trade-off points.

Goals	Risk level	Risk treatment	System assets		
			A1	...	An
Safety goals					
SG1				GA1	O
...			O		
SGn					
Cyber security goals					
CG1			O	GA2	
...					O
CGn					

Fig. 6. Concept phase activities and synchronization points between development, safety, and cyber security teams.

are defined, and their corresponding risk levels are determined. The objectives of this synchronization point are twofold:

(1) To verify if all important assets of the system (from the developers' point of view) are protected - i.e., to make sure that the safety and cyber security teams haven't missed anything; and
(2) to make an initial interdependency analysis between safety and security by analysing the relationships between safety and cyber security goals.

To meet the first objective, we could use relationship matrices to map safety and cyber security goals to system assets, as shown in Fig. 6. In Fig. 6, "O" denotes that the goal (row) contributes to protecting the asset (column).

All three teams need to agree on the safety and cyber security goals, their risk levels, and risk treatment option (either reducing or avoiding, sharing, retaining) for each asset, in accordance with ISO 26262 and ISO/SAE 21434 respectively.

To meet the second objective, we could use the relationship matrices GG1 and GG2, shown in Figs. 7 and 8 respectively. GG1 helps to analyse the impact of cyber security goals on safety goals, while GG2 focuses on the impact of safety goals on cyber security goals.

In Fig. 7, "O" denotes that cyber security goal (column) contributes to satisfying safety goal (row), while "X" means that cyber security goal (column) conflicts with safety goal (row).

Meanwhile, in Fig. 8, "O" shows that safety goal (column) contributes to satisfying security goal (row), while "X" – that safety goal (column) conflicts with cyber security goal (row).

Matrices GG1 and GG2 are also useful to agree on risk treatment options for interdependent safety and cyber security goals.

4.1.3. Synchronization point (3): agreed safety and cyber security requirements and measures

Once safety and cyber security goals have been finalized, the requirement with risk treatment option "reduce" are refined into requirements – design-independent strategies to achieve goals. Safety and cyber security requirements are also assigned safety and security measures, which are then allocated either to the vehicle's systems or environment.

At this point, when safety and security measures have been determined by respective teams, we can start to analyse possible interdependencies between them.

To identify and resolve potential conflicts between measures, we can use Cyber Risk Assessment Framework (CRAF) (Asplund et al., 2019). The CRAF method includes:

- A pre-defined mapping between data security and safety properties (see Fig. 9);
- A set of tables, completed by both safety and security teams (see Figs. 10-12).

Fig. 10 can be used by the safety team to analyse if cyber security requirements and measures do not conflict with safety, while Fig. 11 is used to check if safety requirements and measures do not conflict with cyber security.

If potential conflicts are identified in Figs. 10 and 11, both teams need to try to resolve the conflicts by exploring alternative solutions. To evaluate the alternatives, Fig. 12 can be used.

Fig. 12 shows the types of safety and cyber security relationships, that can be analysed using the CRAF method. As we can see from Fig. 16 our work considers the antagonism relationship and includes models for interdependency and trade-off analysis (alternative solution evaluation). The options in the key as possible entries in matrices MR1-4 in Fig. 14 include satisfaction, contributing to satisfaction and antagonism. These are captured in Fig. 16.

In addition to the CRAF method, we can use relationship matrices to help analyse other types of relationships, namely conditional dependency and reinforcement. Fig. 14, shows a relationship matrix which integrates four smaller matrices, MR1-MR4, for analysing the relationships between safety/cyber security requirements and measures.

The following are the steps for completing matrices MR1-MR4:

(1) Safety team fills in MR1.
(2) Cyber security team completes MR2.
(3) Cyber security team shares their list of security measures with safety team and safety team completes MR3;
(4) Safety team shares the list of safety measures with cyber security team and cyber security team completes MR4;
(5) Safety and cyber security teams meet and discuss the results of matrices MR3-MR4 to reach the final agreement on safety and security measure selection. In case of conflicts Fig. 12 could be used to evaluate alternative measures.

If quantitative data of the effectiveness of safety/security measures in satisfying the requirements is available, this data could be used in Fig. 13 (throughout matrices MR1-MR4) to replace symbol "O", which only indicates that the measure contributes to satisfying the requirement, but does not specify how effective this is. Thus, these matrices could be used to record "intensity" information as well.

Fig. 16 summarizes the types or safety and security relationship considered in matrices proposed so far.

Once the safety and cyber security teams have finalized the selection of safety and security measures, they should agree with the development team about the allocation of measures to vehicle-level systems that implement the item (vehicle-level function) or to the environment. To facilitate this process, relationship matrices ME1-ME2, which map measures to vehicle systems or environment, could be used, as shown in Fig. 17.

These matrices are particularly useful to integrate the threat analysis results of multiple items, since each item is analysed independently, therefore safety and cyber security requirements are specified and measures are selected independently as well.

4.1.4. Summary of matrices used in concept phase

Fig. 15 and Fig. 18 provide the summary of the matrices used in the concept phase. There are 10 matrices in total: four matrices are constructed at goal level and six at the requirement level.

4.2. Trade-off management during product development phase

In the product development phase we have four synchronization points, as shown in Fig. 19.

4.2.1. Synchronization point (4): agreed system-level requirements, safety mechanisms and security controls, and their allocation

Once a detailed system design is developed by the development team, the safety and security teams can refine concept-level safety and cyber security requirements into more detailed system-level requirements. Furthermore, concept-level safety and security measures are

Goals (high-level requirements)	Cyber security goals			Safety risk level	Risk treatment
	CG1	...	CGn		
Safety goals	O				
SG1		**GG1**	X		
...	X				
SGn		O			
Cyber security risk level					
Risk treatment					

Fig. 7. Relationship matrix GG1 to analyse conflicts of cyber security goals with safety goals.

Goals (high-level requirements)	Safety goals			Cyber security risk level	Risk treatment
	SG1	...	SGn		
Cyber security goals					
CG1		**GG2**	X		
...	X		O		
CGn		O			
Safety risk level					
Risk treatment					

Fig. 8. Relationship matrix GG2 to analyse conflicts of safety goals with cyber security goals.

Data security property	Data safety property
Confidentiality	Accessibility, disposability/ delectability, intended destination/ usage, suppression, traceability
Integrity	Accuracy, completeness, consistency, fidelity/ representation, format, history, integrity, resolution, sequencing
Availability	Accessibility, availability, lifetime, priority, sequencing, timeliness
Non-repudiation	History, integrity, traceability, verifiability
Authorisation/authentication	Accessibility, disposability/ delectability, integrity, intended destination/ usage, lifetime, suppression

Fig. 9. Mapping between data safety and security properties.

Cyber security requirement	Security measure	Data security property	Data safety Property	Conflict?	Conflict resolution	Selected alternative
CR1	CM1			X	Alternatives 1...n	
CR2	CM2					
Competed by cyber security team			*Completed by safety team*		*Completed by both teams*	

Fig. 10. CRAF table for conflict analysis between security measures and safety.

Safety requirement	Safety measure	Data safety property	Data security property	Conflict?	Conflict resolution	Selected alternative
SR1	SM1			X	Alternatives 1...n	
SR2	SM2					
Competed by safety team			*Completed by cyber security team*		*Completed by both teams*	

Fig. 11. CRAF table for conflict analysis between safety measures and security.

Alternative	Security probability	Security impact	Safety probability	Safety impact
1				
n				
	Competed by cyber security team		*Completed by safety team*	

Fig. 12. CRAF alternatives' evaluation.

Requirements	Initial risk level	Safety measures			Security measures			Residual risk level
		SM1	...	SMn	CM1	...	CMn	
Safety requirements								
SR1			MR1	O	O	MR3	C	
...		O						
SRn			X			X		
Cyber security requirements								
CR1		O	MR4		O	MR2		
...				X			O	
CRn		C				X		

Fig. 14. Relationship matrices MR1 – MR4 for interdependencies between measures and requirements.
O – measure (column) contributes to satisfying the requirement (row);
C – having the measure (column) is a condition for satisfying the requirement;
X – measure (column) may violate the requirement (row).

Relationship type / Factors	I. Between safety requirements or measures and security requirements or measures		
	(a) Conditional dependency	(b) Reinforcement	(c) Antagonism
Direction			Safety -> Security Security -> Safety
Intensity			
Methods/ Models			• Interdependencies • Trade-off analysis

Fig. 13. Relationships addressed by the CRAF method.

refined into technical safety mechanisms and security controls, which are assigned to corresponding system elements, where they will be allocated. Several relationship matrices can be used at this stage to help teams identify interdependencies and make trade-offs, if necessary.

Firstly, matrices MR5-MR8 can be constructed, as shown in Fig. 20. These matrices are more refined versions of MR1-MR4, developed in concept phase.

The following are the steps for completing matrices MR5-MR8:

(1) Safety team completes in MR5.
(2) Cyber security team completes MR6.
(3) Cyber security team shares their list of security controls with safety team and safety team completes MR7;
(4) Safety team shares the list of safety mechanisms with cyber security team for completing MR8;
(5) The safety and cyber security teams meet and discuss the results of matrices MR5-MR8 to reach the final agreement on safety and security measure selection. In the event of conflicts, the teams need to make trade-offs to remove conflicts while retaining an acceptable residual risk level.

Once safety and cyber security teams have finalized the selection of safety mechanisms and security controls, they should agree with the development team about the allocation of measures to system elements. To facilitate this process, relationship matrices ME3-ME4, which map safety mechanism and security controls to system elements, are shown in Fig. 21.

4.2.2. Synchronization point (5): agreed hardware and software-level safety and cyber security requirements

At this stage, system-level cyber security requirements are refined into hardware and software-level cyber security requirements, which are specified for hardware and software implementation.

This synchronization point is aimed at identifying possible interdependencies between safety and cyber security requirements for the same hardware and software components. Four matrices, RE1-RE4 can be used for this purpose, as shown in Fig. 22. Furthermore, these matrices are useful for defining software/hardware component performance requirements.

Matrices	Rows	Columns	Possible symbols and their meanings
GA1	Safety goals	System assets	O – goal (row) contributes to protecting the asset (column)
GA2	Cyber security goals	System assets	O – goal (row) contributes to protecting the asset (column)
GG1	Safety goals	Cyber security goals	O – cyber security goal (column) contributes to satisfying safety goal (row); X – cyber security goal (column) conflicts with safety goal (row)
GG2	Cyber security goals	Safety goals	O – safety goal (column) contributes to satisfying security goal (row); X – safety goal (column) conflicts with cyber security goal (row)
MR1	Safety requirements	Safety measures	O – measure (column) contributes to satisfying the requirement (row); X – measure (column) may violate the requirement (row)
MR2	Cyber security requirements	Security measures	O – measure (column) contributes to satisfying the requirement (row); X – measure (column) may violate the requirement (row)
MR3	Safety requirements	Security measures	O – measure (column) contributes to satisfying the requirement (row); C – having the measure (column) is a condition for satisfying the requirement; X – measure (column) may violate the requirement (row)
MR4	Cyber security requirements	Safety measures	O – measure (column) contributes to satisfying the requirement (row); C – having the measure (column) is a condition for satisfying the requirement; X – measure (column) may violate the requirement (row)
ME1	Safety measures	Systems/ environment	X – measure (row) is allocated to the system/environment (column)
ME2	Security measures	Systems/ environment	X – measure (row) is allocated to the system/environment (column)

Fig. 15. Description of the 10 matrices used in the concept phase.

Relationship type / Factors	I. Between safety requirements or measures and security requirements or measures		
	(a) Conditional dependency	(b) Reinforcement	(c) Antagonism
Direction	Safety -> Security Security -> Safety	Safety -> Security Security -> Safety	Safety -> Security Security -> Safety
Intensity		Measure effectiveness	
Methods/ Models	• Interdependencies • Trade-off analysis	• Interdependencies • Trade-off analysis	• Interdependencies • Trade-off analysis

Fig. 16. Relationships addressed by matrices GG1-GG2 and MR1-MR4.

4.2.3. Synchronization point (6): agreed detailed design

At this stage, safety mechanisms and cyber security controls are added to detailed system design by the development team, which then need to be reviewed by all three teams.

Mechanisms/controls	Allocation to system/environment		
	E1	...	En
Safety measures			
SM1		**ME1**	X
...	X		
SMn			
Security measures			
CM1	X	**ME2**	
...			X
CMn			

Fig. 17. Relationship matrices ME1 and ME2 to allocate safety and security measures to vehicle systems/environment
X – the measure (row) is allocated to the item/environment (column).

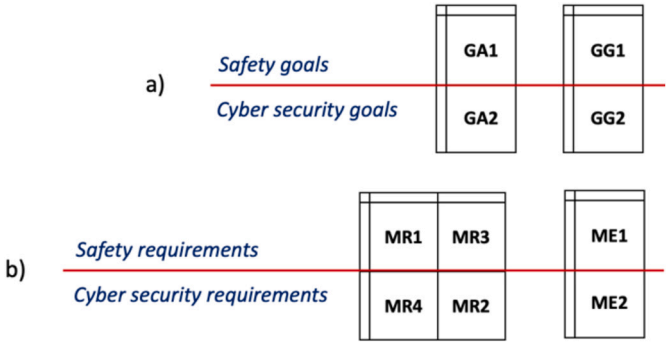


Fig. 18. Summary of concept phase matrices at: a) goal level; b) requirement level.

4.2.4. Synchronization point (7): agreed post-development safety and cyber security requirements

At the end of product development phase, safety and cyber security requirements for post-development phase have to be defined. These phases include production, operation and maintenance, and decommissioning. A relationship matrix can be used for each phase, as shown in Fig. 23. In total, six matrices are defined, RA1-RA6.

Additional requirements for post-development phase activities, to facilitate the implementation of post-development safety and cyber security requirements, can be defined and added at the bottom of Fig. 23.

4.2.5. Summary of matrices used in product development phase

Fig. 23 and Fig. 24 include a summary of matrices used in the product development phase.

In total, sixteen matrices have been defined for this phase: six for analysis of interdependencies at system-level requirement level; four for hardware and software-level requirement level; and six for post-development requirement level.

5. Case study

The case study chosen is a vehicular platoon. Platooning is an application where a group of vehicles move one after another in close proximity, acting jointly as a single physical system. The aims of platooning are to improve safety, reduce fuel consumption, and increase road use efficiency (Balador et al., 2022).

Platooning was chosen as a cyber-physical system use case because it directly involves both safety and cyber security, and decisions made about safety and security decisions can likely interact.

Any cyber security breach in such a high-speed network can compromise the safety and security of the system.

The safety and security analysis used for this case study have been done by ISO/SAE (2021b) and in-house using a commercial automotive threat modelling and security analysis tool named ThreatGet (Christl and Tarrach, 2021), respectively. The Safety Analysis has been conducted with The Hazard Analysis and Risk Assessment (HARA) methodology in accordance with (ISO, 2018) and the security analysis utilised the Threat Analysis and Risk Assessment (TARA) process as instructed in ISO/SAE (2021a).

5.1. The platoon architecture

Transportation by vehicular platoon has many advantages within the logistics industry where it can reduce fuel and environmental costs (Taylor et al., 2022). Fig. 25 shows the high-level architecture of vehicular platoons. It can be seen that the architecture consists of two distinct domains:

The *platoon domain* contains the platoon vehicles with Vehicle-to-Vehicle (V2V) communication between them. Further, it can be seen that the platoon contains two types of vehicles. (1) A single leader vehicle – user driven and responsible for all the decisions regarding the speed and distance the other vehicles need to keep to maintain safety. The leader transmits this information to the member vehicles continuously. (2) Multiple member vehicles – these vehicles are part of the platoon, and they are mostly driven autonomously. They rely on the information received from the leader vehicle, with sensor information to keep them informed of the vehicle in front of them, where they maintain the minimum distance among them as instructed by the leader vehicle. For instance, if the leader instructs the member vehicles to reduce speed by 5 mph, the member vehicles need to simultaneously reduce speed. Otherwise, collisions can occur between the platoon vehicles. Moreover, every vehicle in the platoon is equipped with CACC (Cooperative Automated Cruise Control) which enables the vehicles to navigate in a cooperative manner.

The *infrastructure domain* in the architecture represents the static part of the network and includes a Roadside Unit (RSU) and a Traffic Control Centre. The platoon leader communicates with the Control Centre via the RSU using Vehicle-to-Infrastructure (V2I) communication. The vehicle platoon communicates continuously with the Control Centre in order to provide significant information, including its current location, which helps the Control Centre to keep track of the vehicle platoon.

5.2. Cyber security and safety issues in vehicular platoons

Cybersecurity and safety are critical concerns in vehicular platoons, which are, as defined in Section 5.1, groups of vehicles that communicate and coordinate their movements to improve safety, efficiency, and fuel consumption. Safety and cybersecurity are directly related to each other for vehicular platoons. Vehicular platoons rely specifically on wireless communications, which can be subjected to various attacks (Taylor et al., 2021).

A conflict between safety and security in automotive systems may seem counterintuitive. After all, the primary goal of both disciplines is to protect the users and ensure the optimal operation of the vehicle. However, the strategies for achieving these goals sometimes conflict, particularly when we examine connected and modern vehicles used for platooning.

For instance, the attacker can intercept the significant message shared by the leader vehicle and then transmit a message with tampered information to the member vehicles. This can have a significant impact on safety as any false information can result in the collision of the vehicles which not only results in personal injuries but also will result in operational and financial losses. Therefore, to ensure the safety of the vehicular platoons, it must be ensured that the cyber security issues are addressed properly.

The implementation of vehicular platoons raises both safety and cybersecurity concerns, including but not limited to:

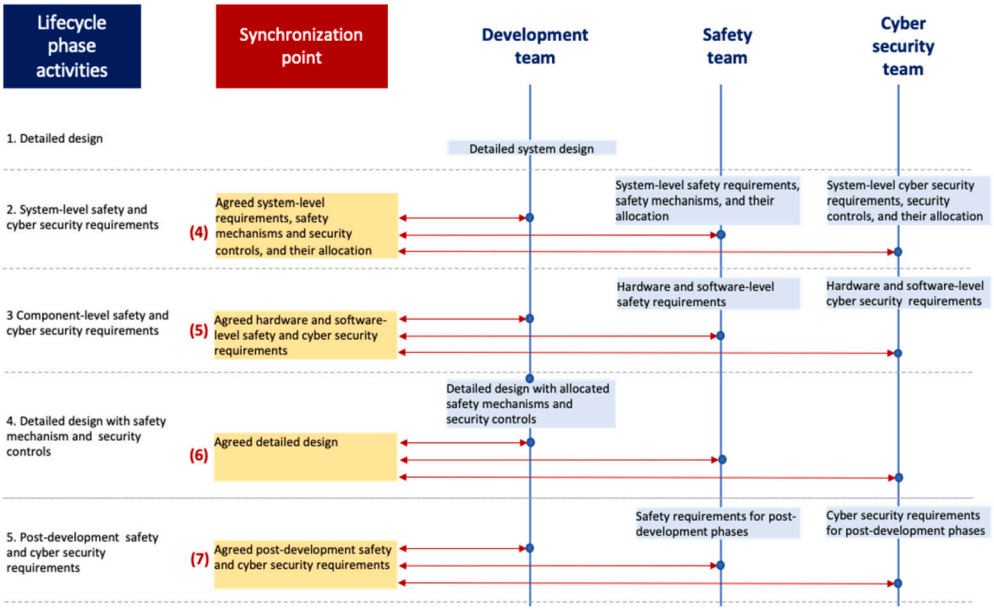


Fig. 19. Product development phase activities and synchronization points between development, safety, and cyber security teams.

Requirements	Initial risk level	Safety mechanisms			Security controls			Residual risk level
		S-SM1	...	S-SMn	S-CM1	...	S-CMn	
System-level safety requirements		C						
S-SR1			MR5	O	O	MR7	C	
...		O						
S-SRn			X			X		
System-level cyber security requirements							C	
S-CR1		O	MR8		O	MR6		
...				X			O	
S-CRn		C				X		

Fig. 20. Relationship matrices MR5 – MR8 to analyse interdependencies between measures and requirements.
O – mechanism/control (column) contributes to satisfying the requirement (row);
C – having the mechanism/control (column) is a condition for satisfying the requirement;
X – mechanism/control (column) may violate the requirement (row).

Mechanisms/controls	System elements		
	S-E1	...	S-En
Safety mechanisms			
S-SM1		ME3	X
...	X		
S-SMn			
Security controls			
S-CM1	X	ME4	
...			X
S-CMn			
Performance requirements			

Fig. 21. Relationship matrices ME3 and ME4 to allocate safety mechanisms and security controls to system elements.
X – mechanism/control (row) is allocated to the system element (column).

Safety: Vehicle-to-vehicle (V2V) communication is critical for the operation of vehicular platoons, and any failure in this communication can result in safety issues. For example, if one vehicle in the platoon fails to communicate with the others, it could cause the formation of the platoon to break, leading to a potential collision.

Cybersecurity: Reliance on V2V communication to coordinate the movements of a platoon makes them vulnerable to cyber-attacks. Attackers could potentially manipulate the communication between vehi-

Goals	Hardware components			Software components		
	HW-E1	...	HW-En	SW-E1	...	SW-En
Hardware-level safety requirements						
HW-SR1		RE1	X			
...	X					
HW-SRn						
Software-level safety requirements						
SW-SR1					RE2	X
...				X		
SW-SRn						
Hardware-level cyber security requirements						
HW-CR1	X	RE3				
...			X			
HW-CRn						
Software-level cyber security requirements						
SW-CR1				X	RE4	
...						X
SW-CRn						
Performance requirements						

Fig. 22. Relationship matrices RE1-RE4 to assign hardware and software-level requirements to hardware and software components respectively.
X – requirement (row) is assigned to the hardware or software component (column).

Goals	Production phase activities			Operation and maintenance phase activities			Decommissioning phase activities		
	PR-A1	...	PR-An	OM-A1	...	OM-An	DC-A1	...	DC-An
Post-development safety requirements									
P-SR1		RA1	X		RA2	X		RA3	X
...	X			X			X		
P-SRn									
Post-development cyber security requirements									
P-CR1		RA4	X	X	RA5			RA6	X
...	X					X	X		
P-CRn									
Additional requirements									

Fig. 23. Relationship matrices RA1-RA6 to assign safety and cyber security requirements to post-development phase activities. X – requirement (row) is assigned to an activity (column).

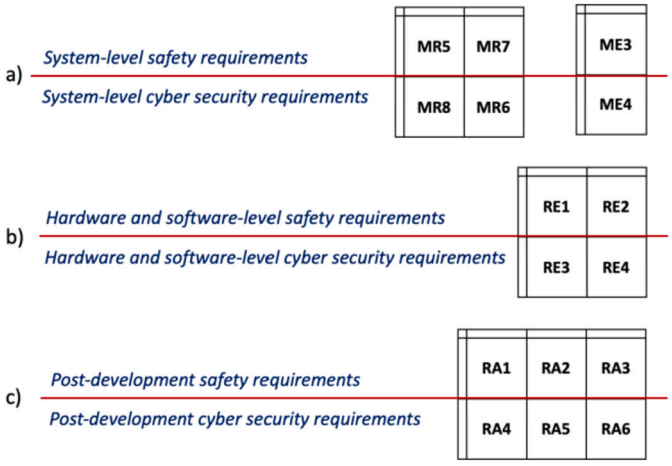


Fig. 24. Summary of product development phase matrices at: a) system-level requirement level; b) hardware and software requirement level; c) post-development requirement level.

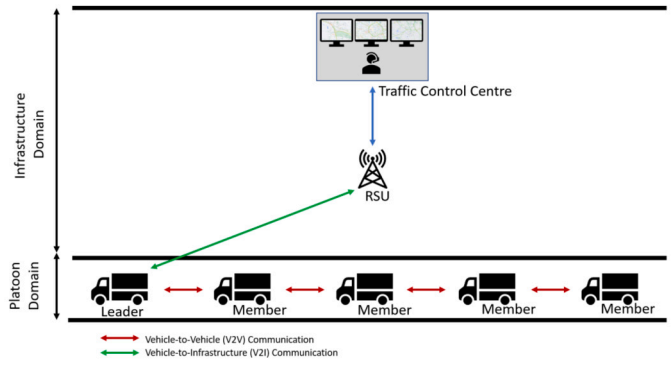


Fig. 25. The architecture of a platoon.

cles, causing them to behave in unexpected ways and putting the safety and security of the vehicles and their occupants at risk.

Data privacy: Vehicle-to-everything (V2X) communication technology enables vehicles to communicate with other vehicles and infrastructure, such as traffic lights, roadside units (RSUs), and other road users. The collection and sharing of this data raise privacy concerns, as sensitive information, such as the location and speed of vehicles, could be misused by malicious actors.

Interference: Interference from other wireless communication technologies, such as Wi-Fi, could potentially disrupt V2V communication, leading to safety issues and compromising the reliability of the platoon system.

Sensors: The use of sensors, such as cameras, lidars, and radars, is essential for the operation of vehicular platoons. However, any failure or malfunction in these sensors could result in incorrect information being transmitted, which could compromise the safety of the vehicles and their occupants. They can also raise cybersecurity concerns, as they can be vulnerable to cyber-attacks. Attackers could potentially manipulate the data being transmitted from the sensors, causing the platoon system to behave in unexpected ways and putting the safety of the vehicles and their occupants at risk. The collection and transmission of data from sensors, such as cameras and radars, can also raise privacy concerns. The sensitive information collected by these sensors, such as the location and speed of vehicles, could be misused by malicious actors.

The above concerns emphasize the importance of balancing the trade-off between cybersecurity and safety in vehicular platoons which requires a comprehensive approach, i.e., the proposed methodology in section 3, that considers the potential risks and consequences of both safety and cybersecurity compromises.

Generally, to address the above concerns, organizations implement robust cybersecurity measures and safety features including (i) encryption and authentication, to protect V2V and V2X communication from cyber attacks, and (2) redundant communication systems and fail-safes, to minimize the risk of safety issues in the event of a communication failure.

The proposed methodology provides a comprehensive approach that considers the potential risks, and consequences of both security and safety compromises with or without each other's effects, their respective requirements, and measures to achieve an optimal balance between security and safety.

5.3. Discussion

An Excel tool has been built from the proposed methodology which takes in the main findings of the safety and security analysis reports and generates the defined interrelationship matrices in a step-by-step fashion. As explained in Section 3, these matrices, and in particular Fig. 10 and Fig. 11, are analysed by CRAF methods to resolve the potential conflicts. Due to constraints concerning space, the analysis artefacts presented below are simply meant to be indicative of how the proposed methodology can be applied. Fig. 26 is a snapshot of the Excel tool. The colourful series of spreadsheets are step-by-step implementations of the proposed methodology and its generated matrices.

Communications in network and system levels such as V2X (Vehicle-to-Everything) and V2V (Vehicle-to-Vehicle) communication systems are essential components of connected vehicles, i.e., vehicular platoons, and they enable vehicles to communicate with each other and with the surrounding infrastructure. These communication systems use various encryption mechanisms to secure communication and prevent unauthorized access. However, as identified by the TOMSAC tool Fig. 27, they are some of the main points of the safety and security conflicts. Safety requirements dictate that the communication system must operate in real-time with minimal latency and with high reliability to ensure the safety of passengers and other road users. On the other hand, security requirements dictate that the communication system must be secure and resistant to cyber-attacks.

The encryption mechanism used in V2X and V2V communication systems adds latency and complexity to the system, which can impact the safety aspects of the system. For example, if the communication system experiences a delay due to encryption or decryption, it can cause a delay in the reaction time of the vehicle's safety systems, which can result in accidents.

Therefore, it is crucial to balance the safety and security aspects of V2X and V2V communication systems. A carefully designed system that integrates both safety and security requirements can ensure that the system operates optimally without compromising the safety of passengers and other road users.

To first ensure safe and efficient autonomous driving and secondly resolve the conflict, the hardware (HW) must be designed with sufficient processing power, memory, and bus resources. Specifically, the HW should be capable of tracking and updating relevant metadata of

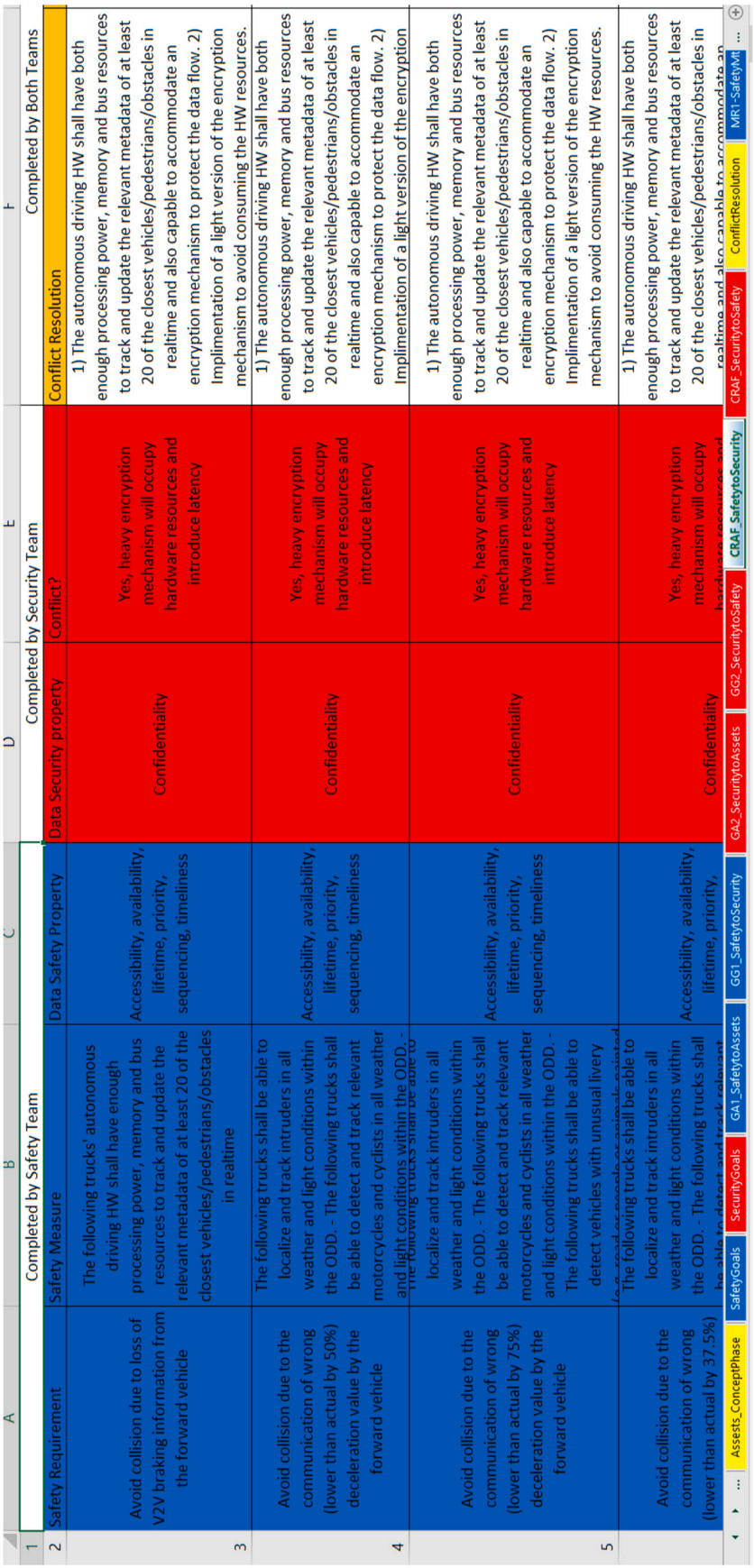


Fig. 26. Overview of the TOMSAC tool.

	Threat Description	Threat Category	Safety Malfunction Category	Impact Level	Attack Feasibility (Likelihood	Risk Level	Treatment	Security Goal
CG1	Messages received by the vehicle (for example V2V or diagnostic messages), or transmitted within it, contain malicious content	Tampering		Moderate	Medium	2	Accept	Avoid receiving malicious
CG2	Manipulation of the connectivity of vehicle functions enables a cyber-attack, this can include telematics; systems that permit remote operations; and systems using short-range wireless communications	Tampering		Moderate	Medium	2	Accept	Avoid manipulation of the connectivity
CG3	Physical manipulation of systems can enable an attack	Tampering		Moderate	Medium	2	Accept	Avoid physical manipulatio
CG4	Parts or supplies could be compromised to permit vehicles to be attacked	Tampering		Moderate	Medium	2	Accept	Avoid manipulation of the
CG5	Install a compromised update	Tampering		Negligible	Medium	1	Accept	Avoid installation of a compr
CG6	Physical Tampering of Sensor	Tampering		Severe	High	5	Reduce	Avoid manipulation of the
CG7	Spoof messages in the vehicle network	Spoofing		Severe	Very Low	1	Accept	Avoid spoof communication on t
CG8	Viruses embedded in communication media are able to infect vehicle systems	Spoofing		Moderate	Medium	2	Accept	Avoid having viruses embedded in c
CG9	Attack against remote wireless interfaces	Spoofing		Severe	High	5	Reduce	Avoid attcks on the remote wireless interface
CG10	Data Flow Sniffing	Information Disclosure		Negligible	High	1	Accept	Avoid data flow sniffing acro
CG11	Information can be readily disclosed. For example through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders	Information Disclosure		Moderate	Medium	2	Accept	Avoid information dis
CG12	Misuse or compromise of update procedures	Information Disclosure		Moderate	Medium	2	Accept	Avoid installation of a compr
CG13	Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks	Elevation of Privilege		Moderate	Medium	2	Accept	Avoid information dis
CG14	Deceive vehicles by falsifying vehicle identity	Elevation of Privilege		Negligible	Very Low	1	Accept	Avoid falsifying vehicle identity
CG15	An unprivileged user is able to gain privileged access to vehicle systems	Elevation of Privilege		Moderate	Medium	2	Accept	Avoid unprivileged user to gain
CG16	Manipulation of vehicle data/code	Elevation of Privilege		Major	Medium	3	Reduce	Avoid spoof communication on t

Concept Phase Guidlines | Assests_ConceptPhase | SafetyGoals | SecurityGoals | GA1_SafetytoAssets | GG1_SafetytoSecurity | GA2_SecuritytoAssets | GG2_SecuritytoSafety | CRAF_SafetytoSecurity | CRAF_SecuritytoSafety | Conflict

Ready | Accessibility: Investigate | Display Settings

Fig. 27. Identified vehicular platoons safety and security conflicts.

a specific range to monitor the closest vehicles, pedestrians, and obstacles in real time. Additionally, the HW must also accommodate an encryption mechanism to protect the data flow. However, implementing a full encryption mechanism could potentially consume too many HW resources, which could impact performance. To address this concern, a light version of the encryption mechanism may be implemented to avoid consuming excessive HW resources. This would strike a balance between maintaining the security of the data flow and optimizing the performance of the autonomous driving system.

Additionally, consider the conflict between secure software updates and the system's need for uptime. Secure software updates are crucial in modern vehicles to address new security vulnerabilities and update vehicle functionalities. However, these updates can conflict with the requirement for high system uptime, especially in a commercial platooning scenario where downtime translates directly to lost productivity. In such a case, for example, it could be proposed that a compromise solution such as using Over-The-Air (OTA) updates combined with a dual-banking system can resolve the conflict. In a dual-banking system, the vehicle's software is stored in two separate memory banks. Updates can be downloaded and installed in the inactive memory bank while the active one continues to run the vehicle, thereby maintaining uptime. Once the update is complete, the system switches over to the updated bank (Feng et al., 2017).

Another potential conflict arises from the requirement for continuous and reliable communication within a platooning fleet. Each vehicle in the platoon needs to maintain a consistent and secure connection with the others, sharing information about their status, position, speed, and more. However, ensuring both the safety and security of these communication channels is a complex task. Security measures such as encryption could introduce delays or data loss, leading to dangerous situations like sudden braking or swerving. To resolve this, advanced algorithms could be developed that prioritize safety-critical data for immediate transmission and processing, while non-critical data could undergo more thorough security measures without risking safety (Yaacoub et al., 2020).

6. Future work

Looking to the future, we hope to consider CPS generally (not just automotive). Here, there are a variety of other factors beyond safety and security which should be taken into account to fully understand the possible conflicts that can arise within a CPS.

Connected and autonomous vehicles face a wide range of potential conflicts, each with its own unique challenges. Here, we delve into a few of them, which are aimed to be included in the methodology.

Cost vs Security: Implementing robust cybersecurity measures, such as secure communication protocols and hardware encryption modules, may incur substantial costs. But skimping on these measures could leave the system vulnerable to cyberattacks. The crux of the issue lies in determining the extent to which a cost increase is justifiable for enhanced security. There's no straightforward answer as it varies from one case to another, depending on factors like the vehicle's function, intended user group, and more. High-end Electric Vehicle (EV) manufacturers prioritize the implementation of robust cybersecurity measures to protect their cars and customers against potential cyber threats. This commitment to cybersecurity often leads to an increase in the overall cost of the vehicle, making it more expensive than other EV alternatives. The investment in enhanced cybersecurity measures is critical due to the potential vulnerability of connected vehicles and EV charging stations to cyber-attacks, as highlighted in multiple references (Anon, 2023; Boulton, 2023; Wilson, 2023).

Usability vs Security: Enhanced security often comes at the cost of user convenience. For instance, a connected vehicle system requiring complex passwords or multi-factor authentication might offer better security but could frustrate users due to the additional time and effort required. A balance between the two is critical - designing systems that maintain a high level of security while remaining user-friendly is a challenging task. Consider the use of biometric authentication in some luxury car models. While the use of fingerprint recognition or facial recognition can provide high security, some drivers find it cumbersome and would prefer a traditional key or simple key fob. This might result in them disabling such security features, making the vehicle more vulnerable (Tengler, 2021; Nuspire, 2023; Vellinga, 2022).

Privacy vs Security: Connected vehicles generate a wealth of data, including potentially sensitive personal information. While ensuring the security of this data against cyberattacks is paramount, doing so may lead to privacy concerns. The balance between data security and privacy protection is a complex issue, with solutions often involving careful data management, including pseudonymization techniques and strict access controls. A case in point is the use of telematics data by insurance companies. This data can help insurers accurately price their policies based on a driver's actual driving behaviour, improving their risk models. However, collecting such detailed data about a person's driving patterns and locations can raise serious privacy concerns, and without proper safeguards in place, could potentially be exploited maliciously (Liu et al., 2022).

Standards vs Innovation: Adhering to established standards, such as ISO/SAE 21434 for cybersecurity management and ISO 26262 for functional safety, ensures a baseline level of security and safety. However, rigid adherence to these standards may stifle innovation. Balancing the need to follow established standards while fostering innovation is another significant challenge in the automotive industry. For example, a startup may develop a novel and more efficient safety system that doesn't align perfectly with ISO standards. This could delay the introduction of potentially lifesaving technology or lead to noncompliance with regulatory bodies. Google's self-driving project, Waymo, is an interesting case. They have developed their autonomous driving technology that includes unique solutions, which might not fully align with existing standards. First, standards are often developed based on known and established technologies, so, the novel techniques used by Waymo might not fit neatly into existing standardization frameworks. For example, their AI-driven decision-making process could be difficult to standardize as it might be viewed as a "black box" that operates in ways that are not fully understood or predictable (Anon, 2022b,a).

Each of these examples demonstrates how managing trade-offs in connected and autonomous vehicles is a complex task that requires careful consideration of many aspects, such as cost, usability, safety, security, privacy, and the need to foster innovation. Integration of these parameters into TOMSAC requires a right balance that can only be achieved by considering all these factors in a holistic and integrated approach.

7. Conclusions

In conclusion, this research has successfully developed and introduced TOMSAC, a novel methodology for managing trade-offs between safety and cybersecurity in the development lifecycle of cyber-physical systems. The methodology offers a practical, user-friendly solution that addresses the long-standing issue of under-consideration of safety and security interdependencies. By systematically combining safety and security analysis data, TOMSAC illuminates the underlying conflicts and interdependencies, thereby encouraging more holistic decision-making.

Furthermore, the creation of an accompanying Excel tool enhances TOMSAC's usability, providing a convenient, accessible way for practitioners to implement the methodology. This tool significantly boosts the feasibility of TOMSAC's application in the real-world setting, paving the way for its broader adoption.

The case study demonstrates in concrete terms how the proposed methodology could be used by automotive OEMs to establish the required communication channels between cybersecurity and functional safety, and how this could be extended to other related engineering disciplines, as required by ISO/SAE 21434. Such an approach will en-

able manufacturers to maximise the efficient deployment of their finite available resources with the required security and safety competence.

Nonetheless, this study also highlights the necessity for ongoing research in this area, particularly in the further refinement of TOMSAC and its validation in a variety of cyber-physical systems. The inertia and reluctance to adapt current practices, as stated in the beginning, underline the need for continued education, advocacy, and further proof-of-concept studies to promote a comprehensive understanding and acceptance of safety and cybersecurity interdependencies.

This paper has laid down the foundation and created a roadmap for this paradigm shift in the development lifecycle of cyber-physical systems. By enabling a more integrated and balanced approach to safety and cybersecurity, the TOMSAC methodology can significantly contribute to the creation of safer, more secure, and more reliable systems. The future implications of this research are expansive and significant, and it is hoped that this work will spur further investigations and developments in this essential domain.

CRediT authorship contribution statement

Giedre Sabaliauskaite: Writing – review & editing, Writing – original draft, Validation, Supervision, Software, Project administration, Funding acquisition, Data curation, Conceptualization. **Jeremy Bryans:** Writing – review & editing, Writing – original draft, Supervision, Methodology, Formal analysis, Conceptualization. **Hesamaldin Jadidbonab:** Writing – review & editing, Writing – original draft, Visualization, Methodology, Data curation, Conceptualization. **Farhan Ahmad:** Writing – review & editing, Writing – original draft, Methodology, Data curation. **Siraj Shaikh:** Writing – review & editing, Writing – original draft, Software, Methodology, Funding acquisition, Conceptualization. **Paul Wooderson:** Validation, Methodology, Investigation, Data curation, Conceptualization.

Declaration of competing interest

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

Data availability

Data will be made available on request.

Acknowledgements

This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC under grant number EP/S035362/1.

References

Anon, 2022a. Google self-driving spinoff Waymo begins testing with public in San Francisco. Waymo. https://www.reuters.com/technology/google-self-driving-spinoff-waymo-begins-testing-with-public-san-francisco-2021-08-24/.

Anon, 2022b. Waymo (formerly Google's self-driving car project): the smart person's guide. Waymo. https://www.techrepublic.com/article/waymo-formerly-googles-self-driving-car-project-the-smart-persons-guide/.

Anon, 2023. Exploring cybersecurity for electric vehicles. https://innovate.ieee.org/innovation-spotlight/exploring-cybersecurity-for-electric-vehicles/.

Apvrille, L., 2008. Ttool for diplodocus: an environment for design space exploration. In: Proceedings of the 8th International Conference on New Technologies in Distributed Systems. ACM, pp. 28–29.

Apvrille, L., Li, L.W., 2019. Harmonizing safety, security and performance requirements in embedded systems. In: 2019 Design, Automation and Test in Europe Conference and Exhibition (DATE), pp. 1631–1636.

Asplund, F., McDermid, J., Oates, R., Roberts, J., 2019. Rapid integration of cps security and safety. IEEE Embed. Syst. Lett. 11 (4), 111–114. https://doi.org/10.1109/LES.2018.2879631.

Balador, A., Bazzi, A., Hernandez-Jayo, U., de la Iglesia, I., Ahmadvand, H., 2022. A survey on vehicular communication for cooperative truck platooning application. Veh. Commun. 35, 100460. https://doi.org/10.1016/j.vehcom.2022.100460. https://www.sciencedirect.com/science/article/pii/S2214209622000079.

Bloomfield, R., Netkachova, K., Stroud, R., 2013. Security-informed safety: if it's not secure, it's not safe. In: Gorbenko, A., Romanovsky, A., Kharchenko, V. (Eds.), Software Engineering for Resilient Systems. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 17–32.

Boulton, A., 2023. EV cybersecurity: defending our mobility. https://blogs.blackberry.com/en/2021/04/ev-cybersecurity-defending-our-mobility.

B. S. Institution, 2018. Connected automotive ecosystems. Impact of security on safety. Code of practice. Standard. British Standards Institution.

Christl, K., Tarrach, T., 2021. The analysis approach of ThreatGet. arXiv preprint. arXiv:2107.09986.

Eames, D.P., Moffett, J.D., 1999. The integration of safety and security requirements. In: Proceedings of the 18th International Conference on Computer Safety, Reliability and Security. SAFECOMP '99. Springer-Verlag, Berlin, Heidelberg, pp. 468–480.

Feng, X., Dawam, E.S., Amin, S., 2017. A new digital forensics model of smart city automated vehicles. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, pp. 274–279.

Huber, M., Brunner, M., Sauerwein, C., Carlan, C., Breu, R., 2018. Roadblocks on the highway to secure cars: an exploratory survey on the current safety and security practice of the automotive industry. In: Gallina, B., Skavhaug, A., Bitsch, F. (Eds.), Computer Safety, Reliability, and Security. Springer International Publishing, Cham, pp. 157–171.

ISO, 2018. ISO26262: Road Vehicles – Functional Safety.

ISO/SAE, 2021a. ISO/SAE 21434, Road Vehicles - Cybersecurity engineering. Standard. International Organization of Standardization.

ISO/SAE, 2021b. First version Hazard Analysis and Risk Assessment and Functional Safety Concept. Tech. Rep., HORIZON 2020 H2020-ART-2016-2017/H2020-ART-2017-Two-Stages GA No. 769115. European Commission.

Kavallieratos, G., Katsikas, S., Gkioulos, V., 2020. Cybersecurity and safety co-engineering of cyberphysical systems—a comprehensive survey. Future Internet 12 (4). https://doi.org/10.3390/fi12040065. https://www.mdpi.com/1999-5903/12/4/65.

Kleberger, P., Olovsson, T., Jonsson, E., 2011. Security aspects of the in-vehicle network in the connected car. In: 2011 IEEE Intelligent Vehicles Symposium (IV), pp. 528–533.

Kolb, C., Nicoletti, S.M., Peppelman, M., Stoelinga, M., 2021. Model-based safety and security co-analysis: a survey. CoRR. arXiv:2106.06272 [abs]. arXiv:2106.06272. https://arxiv.org/abs/2106.06272.

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y., 2015. A survey of approaches combining safety and security for industrial control systems. Reliab. Eng. Syst. Saf. 139, 156–178. https://doi.org/10.1016/j.ress.2015.02.008. https://www.sciencedirect.com/science/article/pii/S0951832015000538.

Lin, C.-W., Yu, H., 2016. Invited - cooperation or competition? Coexistence of safety and security in next-generation ethernet-based automotive networks. In: Proceedings of the 53rd Annual Design Automation Conference. DAC '16. Association for Computing Machinery, New York, NY, USA, pp. 1–6. https://doi.org/10.1145/2897937.2905006.

Liu, B., Pavlou, P.A., Cheng, X., 2022. Achieving a balance between privacy protection and data collection: a field experimental examination of a theory-driven information technology solution. Inf. Syst. Res. 33 (1), 203–223.

Nuspire, 2023. Convenience vs. security: the risk of connected vehicles. EV Design and Manufacturing. https://www.evdesignandmanufacturing.com/news/convenience-security-risk-connected-vehicles/.

Pièrre-Cambacédès, L., 2010. Des relations entre sûretè et sécurité. Ph.D. thesis. France Télécom.

Pomante, L., Muttillo, V., Krena, B., Vonjar, T., Veljkovi, F., Magnin, P., Matschnig, M., Fischer Martinez, B., Gruber, T., 2019. The AQUAS ECSEL project aggregated quality assurance for systems: co-engineering inside and across the product life cycle. Microprocess. Microsyst.

Taylor, S.J., Ahmad, F., Nguyen, H.N., Shaikh, S.A., Evans, D., Price, D., 2021. Vehicular platoon communication: cybersecurity threats and open challenges. In: 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), pp. 19–26.

Taylor, S.J., Ahmad, F., Nguyen, H.N., Shaikh, S.A., Evans, D., 2022. Safety, stability and environmental impact of FDI attacks on vehicular platoons. In: NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium. IEEE Press, pp. 1–6.

Tengler, S., 2021. Connected car safety and security: the future, complex interchange between them. Forbes. https://www.forbes.com/sites/stevetengler/2021/05/11/connected-car-safety-and-security-the-future-complex-interchange-between-them/.

UNECE, 2021a. UN Regulation No. 155 - Cyber security and cyber security management system. Standard. UNECE.

UNECE, 2021b. UN Regulation No. 156 - Software update and software update management system. Standard. UNECE.

UNECE, 2021c. UN Regulation No. 157 - Automated Lane Keeping Systems (ALKS). Standard. UNECE.

Vellinga, N.E., 2022. Connected and vulnerable: cybersecurity in vehicles. Taylor and Francis Online. https://www.tandfonline.com/doi/full/10.1080/13600869.2022.2060472.

Wilson, J., 2023. Updated nhtsa automotive cybersecurity best practices. https://blogs.synopsys.com/from-silicon-to-software/2021/04/13/automotive-cybersecurity-best-practices-nhtsa/.

Yaacoub, J.-P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A., Malli, M., 2020. Cyber-physical systems security: limitations, issues and future trends. Microprocess. Microsyst. 77, 103201.

Giedre Sabaliauskaite is an Associate Professor in Cyber Security at the Department of Computer Science, Swansea University, UK. She is interested in inter-disciplinary research with focus on safety, security, and resilience on complex socio-technical systems of systems.

Giedre has received PhD in Software Engineering from the Osaka University, Japan in 2004. Since then, she worked in academia, industry, as well as applied research institutions in various countries, including Germany, Portugal, Sweden, Singapore, and the UK. In the UK, prior to her post at Swansea University, she worked at the Centre for Future Transport and Cities at Coventry University, where she led several research projects on autonomous system safety and cybersecurity.

Jeremy Bryans is an Assistant Professor in Automotive Cybersecurity at the Institute for Future Transport and Cities. He specialises in the use of formal methods. He recently finished a project developing a security mechanism to automatically analyse behaviour on internal vehicle networks. He is on the Industry Steering Group of the ZENZIC CAVWAY project between Applus+IDIADA and Bruntingthorpe. Prior to his post in the Institute, he worked at Newcastle University, where he was involved in large EU research projects on model-based techniques for developing and maintaining Systems of Systems (SoS) and Cyber-Physical Systems, and designed and led a project on the sustainability of smart grid communications infrastructure. He also designed and led a EPSRC/DSTL-funded project on the secure transmission of provenance metadata in dynamic coalitions. He is a member of the BCS (MBCS), INCOSE (The International Council on Systems Engineering) and a guest member of Newcastle University.

Hesamaldin Jadidbonab is an Assistant Professor in Automotive Cybersecurity at the Institute for Future Transport and Cities. His research will focus on designing and developing a multi-bus testbed demonstrator representing a full-scale automotive functional structure to prove the testing results. Before, he worked at the City University of London (CUL). During his PhD and post-doctoral study at the City University of London (CUL), he has developed his in-depth knowledge of processes related to highly turbulent single and two-phase flows and practical skills essential for experimental fluid mechanics, e.g. Particle Image Velocimetry, Phase Doppler Anemometry, X-ray imaging, Shadowgraph and Schlieren imaging.

Farhan Ahmad holds the position of Senior Lecturer in Cyber Security within the Department of Computer Science at the School of Computing and Engineering, University of Huddersfield, UK. Prior to his tenure at Huddersfield, he spent one year in the automotive industry in the United Kingdom, focusing on the implementation of Threat Analysis and Risk Assessment using ISO/SAE 21434 and designing Cyber Security Management Systems using UNECE R155.

Before moving to industry, Dr. Ahmad served as Assistant Professor (Research) at Coventry University, UK, and as a Post-Doctoral Research Fellow in Cyber Security at the University of Derby, UK. He earned his Ph.D. in Computer Science from the University of Derby in 2019, with an M.Sc. in Communication and Information Technology from the University of Bremen, Germany, and a B.Sc. in Electronics Engineering from COMSATS University Islamabad (formerly COMSATS Institute of Information Technology), Pakistan.

Dr. Ahmad's research is focused on addressing the cybersecurity challenges within Connected and Autonomous Vehicles (CAVs) and the Internet of Things (IoT). His expertise lies in performing Threat Analysis and Risk Assessments (TARA) and devising novel and innovative security solutions for CAV and IoT domains, particularly from a trust management perspective. Farhan has actively contributed to various research projects, including TOMSAC (Trade-off Management between Safety and Cybersecurity) and 5G-CAL (5G-enabled Connected Autonomous Vehicle Logistics).

Siraj Ahmed Shaikh is a Professor in Systems Security at Swansea University (UK). His research interests lie at the intersection of cybersecurity, systems engineering and computer science addressing cyber-physical systems security for automotive and transport systems. He is also Co-Founder and Chief Scientist at CyberOwl, which is dedicated to risk analytics and security monitoring for the maritime sector. He has published over hundred peer-reviewed papers and supervised over ten PhDs. He is currently a NCSC/EPSRC RIT-ICS Fellow (2023-24) and a member of the College of Experts at the UK's Department for Transport (DfT).

Paul Wooderson is Chief Engineer for cybersecurity at HORIBA MIRA. He is a Chartered Engineer with over 20 years' experience in embedded and cyber physical systems security in the automotive and previously smartcard domains.

Paul leads the technical delivery and development of HORIBA MIRA's cybersecurity engineering, consultancy, testing and assessment solutions. He is a UK Expert to the international ISO and UNECE working groups developing new standards and regulations for cybersecurity engineering and software updates for road vehicles. He has played a lead role in the recent UK government funded collaborative research projects ResiCAV, 5StarS and UK CITE, and has several publications on side channel attacks and automotive cybersecurity engineering.

Paul is also a member of the UK Department for Transport College of Experts, advising on cybersecurity.