



Cyber Threat Intelligence Framework and recommendations for C-ITS

**Cadre de renseignement sur les cybermenaces et
recommandations pour le C-ITS**

**Cyber Threat Intelligence Framework und Empfehlungen für
C-ITS**

CertX SA
Kilian Marty
Jens Henkner

ROSAS
Gabriel Python
Loan Bétend
Ivan Baeriswyl
Laurent Pichon

**Forschungsprojekt MB4_20_02C_01 auf Antrag der Arbeitsgruppe
Mobilität 4.0 (MB4)**

Der Inhalt dieses Berichtes verpflichtet nur den (die) vom Bundesamt für Strassen unterstützten Autor(en). Dies gilt nicht für das Formular 3 "Projektabschluss", welches die Meinung der Begleitkommission darstellt und deshalb nur diese verpflichtet.

Bezug: Schweizerischer Verband der Strassen- und Verkehrsfachleute (VSS)

Le contenu de ce rapport n'engage que les auteurs ayant obtenu l'appui de l'Office fédéral des routes. Cela ne s'applique pas au formulaire 3 « Clôture du projet », qui représente l'avis de la commission de suivi et qui n'engage que cette dernière.

Diffusion : Association suisse des professionnels de la route et des transports (VSS)

La responsabilità per il contenuto di questo rapporto spetta unicamente agli autori sostenuti dall'Ufficio federale delle strade. Tale indicazione non si applica al modulo 3 "conclusione del progetto", che esprime l'opinione della commissione d'accompagnamento e di cui risponde solo quest'ultima.

Ordinazione: Associazione svizzera dei professionisti della strada e dei trasporti (VSS)

The content of this report engages only the author(s) supported by the Federal Roads Office. This does not apply to Form 3 'Project Conclusion' which presents the view of the monitoring committee.

Distribution: Swiss Association of Road and Transportation Experts (VSS)



Cyber Threat Intelligence Framework and recommendations for C-ITS

**Cadre de renseignement sur les cybermenaces et
recommandations pour le C-ITS**

**Cyber Threat Intelligence Framework und Empfehlungen
für C-ITS**

**CertX SA
Kilian Marty
Jens Henkner**

**ROSAS
Gabriel Python
Loan Bétend
Ivan Baeriswyl
Laurent Pichon**

**Forschungsprojekt MB4_20_02C_01 auf Antrag der Arbeitsgruppe
Mobilität 4.0 (MB4)**

Impressum

Research center and project team

Project management

Kilian Marty (CertX)

Gabriel Python (HEIA-FR/ROSAS)

Members

Jens Henkner (CertX)

Laurent Pichon (HEIA-FR/ROSAS)

Loan Bétend (HEIA-FR/ROSAS)

Ivan Baeriswyl (HEIA-FR/ROSAS)

Accompanying Commission

President

Bertrand Ndzana (ASTRA)

Members

Patricia Egger (Proton)

Florian Leibenzeder (Swisscom)

Andrian Duerr (ICS Schweiz)

Erik Wilhelm (Kyburz)

Christoph Tschudin (Yunex Traffic)

Applicant

Working Group Mobility 4.0 (MB4)

Source

This document is available for free download at <http://www.mobilityplatform.ch>.

Table of contents

Impressum	4
Zusammenfassung	7
Résumé	9
Summary	11
1 Introduction	13
1.1 Context – Threat Intelligence for C-ITS	13
1.2 Current problems and limitations – Cyber Defense System at the national level	14
1.3 Research plan and report structure	14
1.4 Motivation and objectives of the research project	15
2 State of the art of Threat Intelligence in the C-ITS context and research overview.	17
2.1 Introduction to C-ITS	17
2.2 Technical description of C-ITS	18
2.2.1 Configuration of C-ITS	18
2.2.2 Frequencies	20
2.2.3 Type of V2X communication and coverage	20
2.2.4 Information messages	23
2.3 C-ITS laws and regulations	23
2.3.1 Swiss Laws	24
2.3.2 European Commission Laws	25
2.3.3 European standards for C-ITS	28
2.3.4 Cyber security standards for the automotive sector	30
2.4 State of the art of C-ITS	32
2.4.1 SCOOP project overview	32
2.4.2 SCOOP project C-ITS threat analysis	34
2.4.3 SCOOP project results	37
2.5 C-ITS threats	37
2.5.1 UN ECE R155 threat examples	37
2.5.2 CEN ISO/TR 21186-3 threat examples	38
2.6 Synthesis and conclusion of the state of the art	38
3 Cyberthreat methodology and identification of virtual platforms	41
3.1 Introduction	41
3.2 What are threat modelling and risk assessment?	42
3.3 Threat Analysis and Risk Assessment methodology	42
3.3.1 1. Asset definition	43
3.3.2 2. Threat scenario identification	44
3.3.3 3. Impact Rating	46
3.3.4 4. Attack path analysis	47
3.3.5 5. Attack feasibility rating	47
3.3.6 6. Risk determination	50
3.3.7 7. Risk treatment decision	50
3.4 Description of analyzed scenario	50
3.4.1 Presentation of the scenario elements	50
3.4.2 Description of the V2I communication scenario	52
3.4.3 Analyzed scope	53
3.5 Threat Modelling tools	54
3.5.1 Tool comparison	54
3.5.2 Tool selection	56
3.5.3 Microsoft Threat Modelling Tool	57
4 Approach and results of threat modelling and risk assessment	59

4.1	Introduction	59
4.2	Human-based approach	59
4.2.1	Introduction	59
4.2.2	Risk assessment implementation	59
4.3	Tool-based approach	61
4.3.1	Introduction	61
4.3.2	C-ITS template	61
4.3.3	TMT Usage	64
4.4	Human-based results	67
4.4.1	1. Asset definition	67
4.4.2	2. Threat scenario identification	67
4.4.3	3. Impact Rating	67
4.4.4	4. Attack path analysis	68
4.4.5	5. Attack feasibility rating	68
4.4.6	6. Risk determination	68
4.4.7	7. Risk treatment decision	68
4.4.8	Human-based summary	68
4.5	Tool-based results	69
4.5.1	1. Asset definition	70
4.5.2	2. Threat scenario identification	70
4.5.3	3. Impact Rating	72
4.5.4	4. Attack path analysis	73
4.5.5	5. Attack feasibility rating	73
4.5.6	6. Risk determination	74
4.5.7	7. Risk treatment decision	75
4.5.8	Tool-based summary	75
4.6	Sum up	75
5	Hybrid approach	77
5.1	Hybrid approach setup	77
5.2	Hybrid approach example	78
5.2.1	Threat modeling tool	78
5.2.2	Data extraction to Excel template	79
5.2.3	Completion of the TARA template	80
5.3	Sum up	81
6	Conclusion	83
6.1	Project valorization	83
6.2	Future perspectives	83
6.2.1	Cyber threat analysis model extension	83
6.2.2	Cyber threat assessment for Swiss C-ITS – Way forward	85
6.2.3	Follow-up project – From proactive approach to reactive methods	86
	Annexes	87
	Glossar	91
	Bibliography	95
	Projektabschluss	97

Zusammenfassung

Die kooperativen intelligenten Transportsysteme (C-ITS) sind fortschrittliche Transportsysteme, die hauptsächlich die drahtlose Kommunikation zwischen Fahrzeugen und der Straßeninfrastruktur nutzen, um die Sicherheit, den Verkehrsfluss und die Energieeffizienz zu verbessern. Allerdings bergen diese Systeme auch erhebliche Risiken für die Cybersicherheit aufgrund ihrer Vernetzung und ihrer Abhängigkeit von den zugrunde liegenden Informationstechnologien. Cyberangriffe auf C-ITS können schwerwiegende Folgen haben, von Verkehrsbeeinträchtigungen bis zur Gefährdung der Verkehrsteilnehmer. Daher ist es wichtig, einen proaktiven Ansatz zur Bewältigung dieser Risiken zu verfolgen, um sie frühzeitig vor der Implementierung dieser Systeme zu identifizieren und angemessene Maßnahmen zur Abwehr dieser potenziellen Bedrohungen zu planen.

In diesem Zusammenhang kann ein Cybersicherheitsbedrohungsmodell implementiert werden, um die relevanten Risiken für jeden Abschnitt eines C-ITS-Systems zu berücksichtigen. Dieses Modell ermöglicht die Identifizierung potenzieller Bedrohungen und Schwachstellen sowie die Bewertung ihrer Machbarkeit und der möglichen Auswirkungen. Die Ergebnisse der Anwendung dieses Bedrohungsmodells auf ein C-ITS-System können anschließend verwendet werden, um geeignete Sicherheitsmaßnahmen, sowohl technischer als auch verfahrenstechnischer Art, zu entwickeln, um eine sichere und geschützte kooperative Verkehrsumgebung für alle Verkehrsteilnehmer zu gewährleisten.

In der Schweiz gelten kooperative intelligente Transportsysteme (C-ITS) als vielversprechende Lösung zur Optimierung des Verkehrs hinsichtlich Sicherheit, Umwelt und Wirtschaftlichkeit. Das Land hat mehrere Pilotprojekte gestartet, um C-ITS in städtischen und ländlichen Gebieten zu testen, insbesondere in den Städten Zürich und Lausanne. Das Hauptziel dieser Projekte besteht darin, die technische Machbarkeit von C-ITS zu demonstrieren und deren Auswirkungen auf die Sicherheit und Effizienz des Verkehrs in der Schweiz zu bewerten. Vorläufige Ergebnisse zeigen, dass C-ITS dazu beitragen können, die Anzahl von Verkehrsunfällen zu reduzieren, den Verkehrsfluss zu verbessern und die Treibhausgasemissionen zu verringern. Allerdings werfen diese Projekte auch Fragen und Bedenken hinsichtlich der Datensicherheit auf.

Die vorliegende Studie hat zunächst die internationale Literatur zu diesem Thema untersucht, um die grundlegenden Elemente in Bezug auf Technologie, Sicherheit, Regulierungen und Forschungsstand zu definieren. Auf der Grundlage dieser Grundelemente wurden bestimmte Entscheidungen für das weitere Vorgehen im Projekt getroffen:

- **Technologie:** Die Forschungsgruppe hat beschlossen, ihre Bemühungen auf die V2X-Kommunikation zwischen Fahrzeugen und Straßeninfrastruktur zu konzentrieren. In der Schweiz wird dieses Segment von C-ITS durch die Verwendung des C-V2X-Protokolls abgedeckt. Die Forschungsgruppe hatte Zugang zu C-ITS-Geräten (OBU und RSU), die die Protokolle C-V2X und ITS-G5 nutzen, und hat ein Szenario mit vernetzten Ampeln entwickelt, die ihren Zustand und ihre Position an ein autonomes Fahrzeug übermitteln. Das Fahrzeug passt seine Manöver basierend auf diesen Daten an. Dieses Szenario diene als Grundlage für einen Proof-of-Concept, um die Machbarkeit eines tatsächlichen Cybersecurity-Angriffs zu veranschaulichen, der durch proaktive Risikobewältigung vermieden werden könnte;
- **Sicherheit:** Um Bedrohungen zu identifizieren und die mit der V2I (bzw. I2V) Kommunikation verbundenen Risiken zu quantifizieren, wurden zwei Entscheidungen getroffen:
 - Für die Modellierung des Systems/Szenarios wurde die Open-Source-Software "Microsoft Threat Modeling Tool" von Microsoft verwendet;
 - Zur Identifizierung relevanter Bedrohungen für das modellierte Szenario wurde eine spezifische Vorlage für C-ITS in der Open-Source-Software "Microsoft Threat Modeling Tool" entwickelt;

- Für die Risikoanalyse wurde die Methode "Threat Analysis and Risk Assessment" (TARA), wie sie im aktuellen Standard ISO/SAE 21434:2021 vorgeschlagen wird, verwendet.

Um den Mehrwert eines solchen Bedrohungsmodells und dessen Anwendung auf ein C-ITS-System zu bewerten, wurde parallel eine "traditionelle" Risikoanalyse durchgeführt, die manuell und weitgehend auf Expertenurteilen basierte. Diese beiden Ansätze, basierend auf einem Tool oder auf Expertenurteilen, wurden verglichen, um ihre Vor- und Nachteile sowie potenzielle Einschränkungen zu identifizieren. Zusammenfassend lässt sich sagen, dass der Tool-basierte Ansatz den Vorteil bietet, einen gewissen Automatisierungsgrad zu bieten, der es ermöglicht, schnell einen umfangreichen Katalog von zu berücksichtigenden Bedrohungen zu generieren. Diese Automatisierung erfolgt durch die Verwendung und Reife der im Projekt entwickelten C-ITS-Vorlage. Diese Vorlage wird kontinuierlich weiterentwickelt, um die dynamische Natur der Cyberrisiken widerzuspiegeln.

Der manuelle Ansatz basierend auf Expertenurteilen hat den Vorteil, keine "falsch-positiven" Bedrohungen in den Bedrohungskatalog einzuführen (z.B. vorhandene, aber nicht auf das betreffende System anwendbare generische Bedrohungen). Allerdings ist der Aufwand und die erforderlichen Fähigkeiten für die Anwendung dieses Ansatzes erheblich höher, und seine Machbarkeit in Systemen, die sich kontinuierlich weiterentwickeln sollen, ist kritisch.

Diese Erkenntnisse führten die Forschungsgruppe dazu, einen sogenannten "hybriden" Ansatz zu beschreiben, der die Vorteile beider Alternativen kombiniert, um die Bedrohungserkennung durch den Einsatz eines Tools zu maximieren, gleichzeitig aber das Auftreten von "falsch-positiven" Bedrohungen zu minimieren und die Risikokriterien basierend auf Expertenurteilen anzupassen. Neben diesen Aspekten ermöglicht dieser Ansatz eine geringere Beteiligung von Cybersicherheitsexperten während dieser Phase der Cyber-Risikoanalyse, da ihr Wissen in die C-ITS-Vorlage integriert wird und auch von potenziellen Nicht-Experten verwendet werden kann.

Abschließend lässt sich sagen, dass der von der Forschungsgruppe vorgeschlagene hybride Ansatz pragmatisch ist und einen soliden Rahmen für die proaktive Risikoerkennung und -analyse bietet. Es ist offensichtlich, dass eine solche Analyse nicht erschöpfend sein kann, und daher sollten auch reaktive Ansätze in Betracht gezogen werden, um ein Rahmenwerk für die zukünftige Erkennung neuer Bedrohungen und Schwachstellen bereitzustellen. Aufgrund der Entwicklung von Technologien und Angriffsmethoden werden neue Bedrohungen auftreten, und ihre Behandlung wird entscheidend sein, um eine sichere C-ITS-Umgebung in der Schweiz aufrechtzuerhalten.

Résumé

Les systèmes de transport intelligents coopératifs (C-ITS) sont des systèmes de transport avancés qui utilisent essentiellement la communication sans fil entre les véhicules et l'infrastructure routière pour améliorer la sécurité, la fluidité du trafic et l'efficacité énergétique. Toutefois, ces systèmes présentent également des risques de cyber sécurité importants en raison de leur interconnectivité et de leur dépendance à l'égard des technologies de l'information sur lesquelles ils se basent. Les cyberattaques sur les C-ITS peuvent entraîner des conséquences graves, allant de la perturbation du trafic à la mise en danger des usagers de la route. Ainsi, il est essentiel d'adopter une approche proactive vis-à-vis de ces risques, afin de les identifier en amont de l'implémentation de ces systèmes, et prévoir les mesures adéquates afin d'atténuer ces menaces potentielles.

Dans cette optique, un modèle de menace cybersécurité peut être mis en place afin de prendre en considération les risques pertinents à chaque segment d'un système C-ITS. Ce modèle permet d'identifier les menaces et faiblesses potentielles, leur faisabilité ainsi que les conséquences que ces dernières pourraient engendrer. Les résultats de l'application de ce modèle de menaces à un système C-ITS peuvent ensuite être utilisés pour développer des mesures de sécurité adaptées, tant techniques que procédurales, afin de garantir un environnement de transport coopératif sûr et sécurisé pour tous les usagers de la route.

En Suisse, les systèmes de transport intelligents coopératifs (C-ITS) sont considérés comme une solution prometteuse dans le cadre de l'optimisation des transports d'un point de vue sécuritaire, écologique et économique et sécuritaire. Le pays a lancé plusieurs projets pilotes visant à tester les C-ITS dans des zones urbaines et rurales, notamment dans les villes de Zurich et de Lausanne. L'objectif principal de ces projets est de démontrer la faisabilité technique des C-ITS et d'évaluer leur impact sur la sécurité et l'efficacité du transport en Suisse. Les résultats préliminaires montrent que les C-ITS peuvent aider à réduire le nombre d'accidents de la route, améliorer la fluidité du trafic et réduire les émissions de gaz à effet de serre. Cependant, ces projets soulèvent également des questions et préoccupations quant à la cyber sécurité des données qu'ils utilisent.

La présente recherche s'est tout d'abord penchée sur la littérature internationale en la matière afin de définir les éléments de base à analyser en termes de technologie, de sécurité, de réglementations et d'état de la recherche. Sur ces éléments de bases, certains choix ont été effectués pour la suite du projet :

- **Technologie :** Le groupe de recherche a décidé de concentrer ces efforts sur les communications V2X utilisées entre véhicules et infrastructures routières. En Suisse ce segment des C-ITS vise à être couvert par l'utilisation du protocole C-V2X. Ayant accès à des équipements C-ITS (OBU et RSU) utilisant les protocoles C-V2X et ITS-G5, le groupe de recherche a mis en place un scénario de feux de signalisation connectés communiquant son état et sa position à un véhicule autonome. Ce dernier a pour fonction d'ajuster ses manœuvres sur la base de ces données. Ce scénario a été utilisé comme base au Proof-of-Concept visant à illustrer la faisabilité d'une attaque cyber sécurité réelle qui pourraient être évitée en approchant ces risques en amont, de façon proactive ;
- **Sécurité :** Pour identifier les menaces et quantifier les risques inhérents à ces communications V2I (respectivement I2V), deux choix ont été faits :
 - Pour la modélisation du système / scénario, le logiciel Open Source de Microsoft « Microsoft Threat Modeling Tool » a été utilisé ;
 - Pour l'identification des menaces pertinentes au scénario modélisé, un template spécifique aux C-ITS a été développé sur le logiciel Open Source de Microsoft « Microsoft Threat Modeling Tool » ;
 - Pour l'analyse des risques, la méthodologie « Threat Analysis and Risk Assessment » (TARA) proposée dans le récent standards ISO/SAE 21434 :2021 a été utilisée.

Afin d'évaluer la valeur ajoutée d'un tel modèle de menace et son application à un système C-ITS, une procédure d'analyse de risque « traditionnelle » a été réalisée en parallèle, de façon manuelle et essentiellement basée sur un jugement d'expert.

Ces deux approches, respectivement basée sur un outil ou basée sur jugements d'experts, ont été comparées afin d'en extraire leurs avantages, inconvénients et limitations potentielles. En résumé, l'approche basée sur l'outil a pour principal avantage de fournir un certain niveau d'automatisation qui permet de rapidement générer un important catalogue de menaces à considérer. Cette automatisation provient de l'utilisation et la maturité du template C-ITS développé dans le cadre du projet. Ce dernier visera à continuellement évoluer afin de refléter l'aspect dynamique du paysage des menaces cyber.

L'approche manuelle basée sur jugements d'experts quant à elle a l'avantage de ne pas introduire de faux-positifs dans le catalogue de menaces (par ex. menace générique existante mais non-applicable au système en question). Cependant, l'effort et les capacités requises pour son application étant largement supérieurs, sa viabilité dans le cadre de systèmes visant à évoluer continuellement s'avère critique.

Ces constats ont amené le groupe de recherche à décrire une approche dite « hybride » combinant les avantages des deux alternatives afin de maximiser l'identification de menaces grâce à l'utilisation d'un outil, tout en minimisant l'apparition de faux-positifs et ajustant les critères de risques sur la base de jugements d'experts. En plus de ces éléments, cette approche permet de diminuer l'implication d'experts cyber sécurité lors de cette phase d'analyse de cyber risque, du fait de l'intégration de leurs connaissances dans le template C-ITS pouvant être utilisé par de potentielles non-experts.

Pour conclure, l'approche hybride proposée par le groupe de recherche s'avère pragmatique et fournit un cadre solide pour l'identification et l'analyse de risque proactive. Étant évident qu'une telle analyse ne peut être exhaustive, des approches réactives devraient être également considérées afin de fournir un cadre de gestion pour la détection future de menaces et vulnérabilités nouvelles. L'évolution des technologies ainsi que des méthodes d'attaques font que de nouvelles menaces apparaîtront et leurs traitements s'avèreront décisifs pour la maintenance d'environnement C-ITS sécurisé en Suisse

Summary

Intelligent Cooperative Transport Systems (C-ITS) are advanced transportation systems that primarily use wireless communication between vehicles and road infrastructure to improve safety, traffic flow, and energy efficiency. However, these systems also present significant cybersecurity risks due to their interconnectivity and reliance on information technologies. Cyberattacks on C-ITS can have serious consequences, ranging from traffic disruptions to endangering road users. Therefore, it is essential to take a proactive approach to these risks, identifying them prior to the implementation of these systems and implementing appropriate measures to mitigate potential threats.

In this regard, a cybersecurity threat model can be implemented to consider relevant risks in each segment of a C-ITS system. This model helps identify potential threats and weaknesses, assess their feasibility, and determine the potential consequences they may cause. The results of applying this threat model to a C-ITS system can then be used to develop suitable security measures, both technical and procedural, to ensure a safe and secure cooperative transportation environment for all road users.

In Switzerland, C-ITS is considered a promising solution for optimizing transportation from a safety, ecological, and economic perspective. The country has launched several pilot projects to test C-ITS in urban and rural areas, including the cities of Zurich and Lausanne. The main objective of these projects is to demonstrate the technical feasibility of C-ITS and evaluate their impact on safety and transport efficiency in Switzerland. Preliminary results show that C-ITS can help reduce the number of road accidents, improve traffic flow, and reduce greenhouse gas emissions. However, these projects also raise questions and concerns about the cybersecurity of the data they utilize.

This research initially examined international literature to define the basic elements to analyze in terms of technology, security, regulations, and research status. Based on these elements, certain choices were made for the project's continuation:

- **Technology:** The research group decided to focus its efforts on V2X communications used between vehicles and road infrastructure. In Switzerland, this segment of C-ITS aims to be covered by the use of the C-V2X protocol. With access to C-ITS equipment (OBU and RSU) using the C-V2X and ITS-G5 protocols, the research group implemented a scenario involving connected traffic lights communicating their status and position to an autonomous vehicle. The vehicle adjusts its maneuvers based on this data. This scenario was used as the basis for the proof-of-concept to illustrate the feasibility of a real cybersecurity attack that could be prevented by proactively addressing these risks;
- **Security:** To identify threats and quantify the inherent risks in V2I (respectively I2V) communications, two choices were made:
 - For system/scenario modeling, Microsoft's open-source software "Microsoft Threat Modeling Tool" was used;
 - For identifying threats relevant to the modeled scenario, a specific template for C-ITS was developed using Microsoft's open-source software "Microsoft Threat Modeling Tool";
 - For risk analysis, the "Threat Analysis and Risk Assessment" (TARA) methodology proposed in the recent ISO/SAE 21434:2021 standard was used.

To assess the added value of such a threat model and its application to a C-ITS system, a parallel "traditional" risk analysis procedure was carried out manually, primarily based on expert judgment. These two approaches, tool-based and expert judgment-based, were compared to extract their advantages, disadvantages, and potential limitations. In summary, the tool-based approach has the main advantage of providing a certain level of automation, enabling the rapid generation of an extensive catalog of threats to consider. This automation is facilitated by the use and maturity of the C-ITS template developed as

part of the project, which will continuously evolve to reflect the dynamic nature of the cyber threat landscape.

The expert judgment-based (human-based) approach, on the other hand, has the advantage of not introducing false positives into the threat catalog (e.g., existing generic threats that are not applicable to the specific system). However, the effort and expertise required for its application are significantly higher, making its viability critical in systems that aim to continuously evolve.

These findings led the research group to describe a "hybrid" approach that combines the advantages of both alternatives to maximize threat identification using the tool while minimizing the occurrence of false positives and adjusting risk criteria based on expert judgments. In addition to these aspects, this approach reduces the involvement of cybersecurity experts during the cyber risk analysis phase by integrating their knowledge into the C-ITS template, which can be used by potential non-experts.

In conclusion, the hybrid approach proposed by the research group proves to be pragmatic and provides a solid framework for proactive threat identification and analysis. It is evident that such an analysis cannot be exhaustive, and reactive approaches should also be considered to provide a management framework for the future detection of new threats and vulnerabilities. The evolution of technologies and attack methods will introduce new threats, and their handling will be decisive in maintaining a secure C-ITS environment in Switzerland.

1 Introduction

1.1 Context – Threat Intelligence for C-ITS

The automotive world of tomorrow will be defined by vehicles that not only communicate with each other, but also with roadside infrastructure and other road users. Cooperative Intelligent Transport Systems (C-ITS) and V2X communication are trustworthy and secure technologies that represent the future of intelligent vehicle networking. *Fig. 1* below illustrates a typical C-ITS environment where vehicles and infrastructures communicate with each other to provide advanced intelligence, allowing for optimized mobility services that potentially offer greater safety and security.

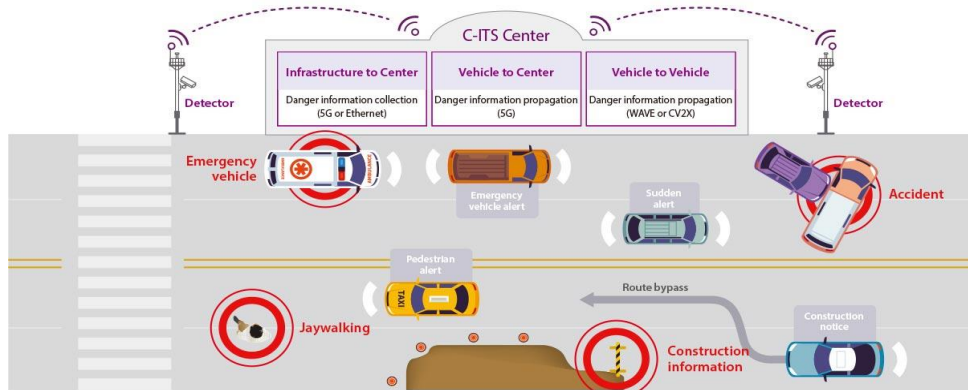


Fig. 1 Example of C-ITS (sample) [16].

Although these systems/items are intended to enhance and strengthen mobility systems, they can also be attractive targets for threat agents (see threat agent and attack vectors on *Fig. 1*). In this context, two risk management approaches should be jointly implemented by mobility stakeholders: proactive threat identification and reactive vulnerability management.

In a nutshell, relevant cyber security properties (the CIA triad) should be ensured across the C-ITS environment to reduce the risk of exploitation and potentially critical impacts on stakeholders. These impacts are usually categorized as follows: Safety impacts, Financial impacts, Operational impacts and Privacy impacts (a.k.a. the SFOP impact types). The goal of this project tender is to build the baseline of what could be named the Threat Intelligence Platform, a platform for proactive threat identification, systems and infrastructure monitoring, security hygiene maintenance, and development of reactive methods.

As an example, let us imagine a situation in which automated vehicles are jammed (jamming attack) in the context of the arrival of an emergency vehicle with first responders. How could this complicated case be evaluated and managed at the C-ITS level? What would happen in the case of rogue/adversarial V2X communications generated by an attacker?

1.2 Current problems and limitations – Cyber Defense System at the national level

Today, reports on cyber incidents ranging from safety-critical vehicle-side consequences [17] to operation-critical impacts on operator infrastructure and environment [18] are regularly published in the context of mobility-related applications. However, traditional databases and information sources are often unsuited to current needs. The heterogeneity of C-ITSs (encompassing IT systems such as cloud computing, datacenters, computers, servers, mobile, as well as Operational Technology (OT) such as critical infrastructures, connected vehicles, embedded systems, and industry-specific technologies, requires the development of a new baseline of critical cyber security environment. This framework should be approved by the authorities for delivery to C-ITS stakeholders, thus ensuring a common understanding of risks and the improvement of systems across sectors.

In order to ensure the cybersecurity of every aspect of C-ITS (incl. V2X communications among others), the European Commission is currently developing a cyber-security defense system for C-ITS, on the basis of which each EU member state will be able to develop its own C-ITS protection system. It follows that Switzerland has to initiate and develop its own C-ITS cyber defense system solution if the country is to ultimately integrate or interface with broader scale solutions.

Currently, Swiss authorities have neither the specifications nor a clear description of its future cyber defense system for C-ITS. This is why this research project is aiming to initiate the roadmap for building the primitive elements of a future cyber defense system for C-ITS.

1.3 Research plan and report structure

The research plan of the project is summarized in *Fig. 2*. First, an analysis of the state of the art on C-ITS was performed, including research on threat models, threat assessments, unknown vulnerabilities and classification. This first phase allowed us to elaborate a listing of the basic elements of a C-ITS.

On this basis, two activities took place in parallel:

- Identification of a tool and creation of a threat model to simulate and automatically identify threats related to C-ITS;
- Manual threat identification according to the ISO 21434 standard and the TARA (Threat Analysis and Risk Assessment) methodology.

The results of the tool-based and human-based methods were compared to obtain their strengths and weaknesses.

The last work package aims to integrate the results of the above-described activities into an end-to-end proof of concept for the creation of virtual C-ITS environments, automated cyber security analysis, and simulation of cyber-attacks including potential impacts.

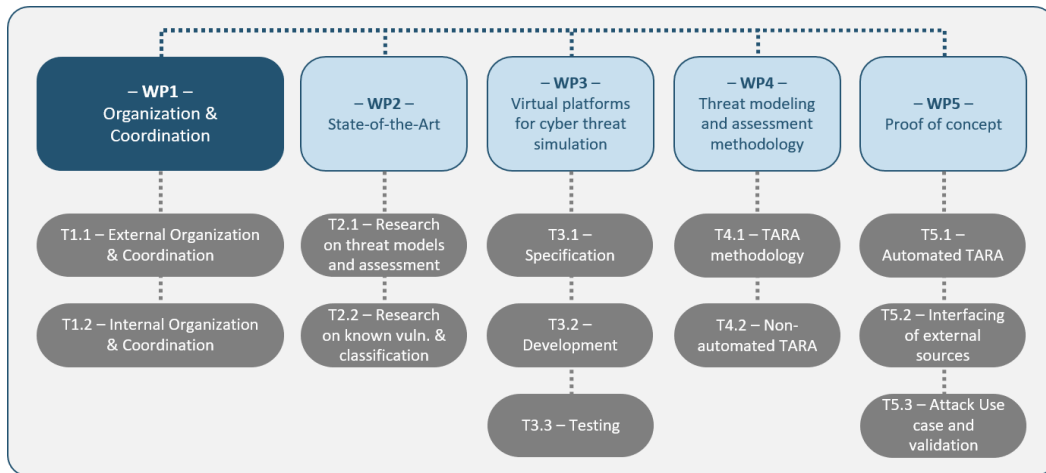


Fig. 2 Project structure.

1.4 Motivation and objectives of the research project

The results of this research project will allow Swiss national authorities to initiate their cyber defense system, which, in the near future, will become a mandatory aspect of secure C-ITS in the context of the monitoring and supervision of the cyber security hygiene of Swiss infrastructure as a whole. In addition to this key dimension, national authorities will also get a better understanding of the keys to cyber security in the mobility sector, which will allow them to more efficiently identify areas for further research and improvement. Regarding future authorization and homologation schemes, national authorities will be better able to define the requirements for external technical services in the context of future activities.

The objectives of the tender are listed below, with a summary of how our proposal will fulfill them.

Objective 1: Identify security vulnerabilities relevant to C-ITS and develop a classification of the identified vulnerabilities.

- Based on our strong background across projects with OEMs and Tier-1s/-2s, we are going to summarize our existing knowledge. Elements from key references (e.g. automotive regulations, standards, public databases) will be added, and classification schemes will be proposed;
- Covered through WP2 and final simulation in WP5.

Objective 2: Develop a virtual C-ITS environment to simulate scenarios of cyber-attacks on C-ITS services that can be used to conduct risk assessments.

- Using our existing laboratory for simulation (XiL-lab / X-in-the-Loop), we are going to prototype a SW-based simulator to test cyber-critical scenarios, assess their potential impact, and use the results to update the current knowledge of C-ITS vulnerabilities and threats;
- Covered through WP3 and WP4, with final simulation in WP5.

Objective 3: Develop a cyber-threat assessment model and test it in the virtual C-ITS environment developed in the previous step (proof of concept).

- Based on our experience with threat analysis and risk assessment with OEMs and Tier-1s/-2s, we are going to create a tailored framework for automated threat assessment in a simulated environment;
- Covered through WP3 and WP4, with final simulation in WP5.

2 State of the art of Threat Intelligence in the C-ITS context and research overview

2.1 Introduction to C-ITS

Intelligent Transportation Systems (ITS) is a container concept covering sensing, situation analysis, vehicle and infrastructure control, and communication technologies used in the world of ground transportation to improve safety, mobility and efficiency. Applications can, for example, process and share information to reduce congestion and environmental impacts while increasing the quality of commercial and public transportation.

Cooperative Intelligent Transport Systems (C-ITS) refers to the cooperation between two or more ITS subsystems (allocated to people, vehicles or road infrastructure units), enabling and providing ITS services with better quality and enhanced levels of service when compared to an equivalent ITS service provided by a single ITS subsystem. Fig. 3 shows an example of equipment used in cars to enable ITS services.



Fig. 3 Example of C-ITS “On Board Unit” (OBU) enabling ITS services on the vehicle side [19].

C-ITS are used to communicate between vehicles (V2V), vehicles and infrastructure (V2I), or generally between road vehicles and external elements (V2X). These types of communication cover a broad range of services, including communication to avoid collisions, information about road limitations, and traffic management, among others. Fig. 4 is an example of a C-ITS scenario.

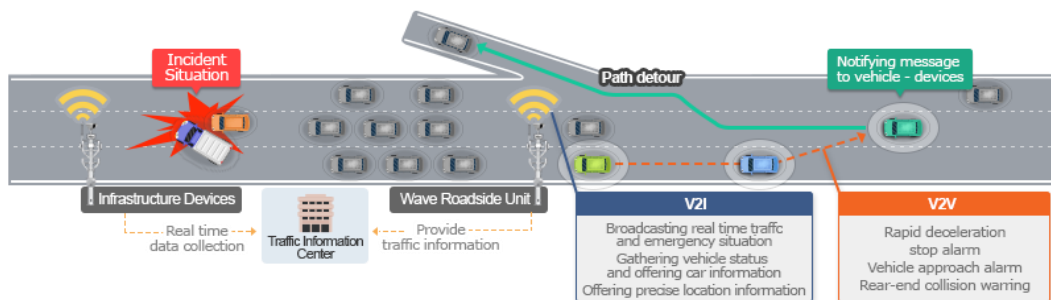


Fig. 4 Example of C-ITS usage in a highway accident situation [20].

“An accident on a 3-lane highway causes slowdowns detected by road infrastructure devices. The accident, congestion and location information are sent to a ‘Traffic Information Center’, which broadcasts this information to other, more distant elements of the infrastructure. These infrastructure elements will then be able to send traffic and emergency information (I2V), via RSUs (Road Side Units), to vehicles (OBU). This information can also be relayed from vehicle to vehicle (V2V), allowing vehicles approaching the accident to apply emergency braking, establish greater safety distances or even establish a path deviation.”

In the context of C-ITS threat analysis, non-exhaustive high-level threats can be cited as threat examples for this scenario. A hacker could send a false accident message to an infrastructure element, to create an unwarranted traffic jam. The hacker could also suppress an emergency and braking message relayed to RSU, thus increasing the risk of collision for approaching vehicles. The first example affects the availability of the function, while the second affects the safety of the drivers.

The technologies used by C-ITS and its stakeholders, such as the communication methods, are already well documented and will be discussed in Chapter 2.2. In contrast, there are not yet many laws or standards to regulate them. Currently there is no Swiss regulation on C-ITS except for the radio-frequency range defined by the Federal Office of Communication. On the standards side, there is a technical committee within the European Committee for standardization: CEN/TC 278/WG 16 [3]. The legislation of C-ITS will be discussed in Chapter 2.3 of the report.

2.2 Technical description of C-ITS

The following technical descriptions of C-ITS correspond to some of the physical, implementation and communication specifications found in the literature on ITS-S (ITS station) and C-ITS. They do not deal strictly with the management of risks and weaknesses of C-ITS, but can be used in the work packages of the MB4 project as starting hypotheses to define models, use cases or simulations.

2.2.1 Configuration of C-ITS

While ITS specifications are typically developed to address a specific ITS service domain, such as public transportation, road safety, or public emergencies, C-ITS specifications must support the interoperability of ITS services by exchanging information within the same application domain or between different application domains. C-ITS services are based on the exchange of ITS services.

To ensure complete interoperability, the ISO 21217 standard defines the general architecture of ITS stations. ITS station architecture is presented in *Fig. 5*.

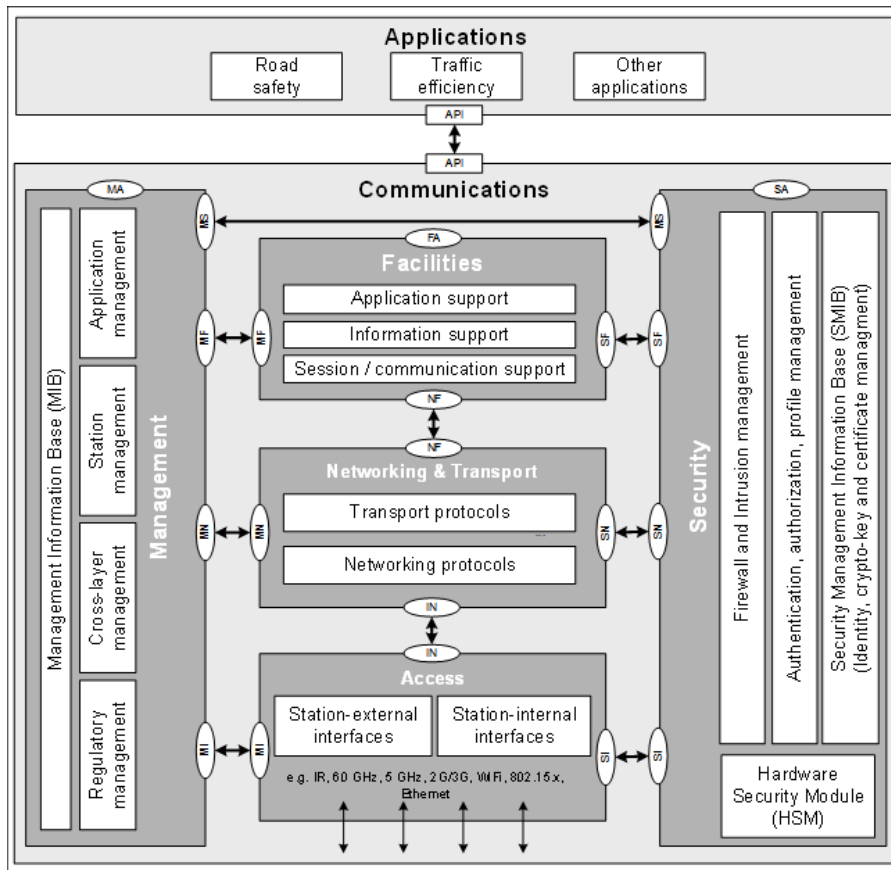


Fig. 5 ITS station architecture, ISO 21217 [4]

Each ITS-S is composed of 3 communication layers:

- The access layer;
- The networking and transport layer;
- The facilities layer, supporting applications.

Additional cross-layer entities, management of the ITS-SU (ITS station unit) and security entities support communications and applications.

C-ITS services are based on data exchanges between 4 categories of stakeholders, as shown in Fig. 6. Exchanges can be made between these categories, but also internally by between each stakeholder.

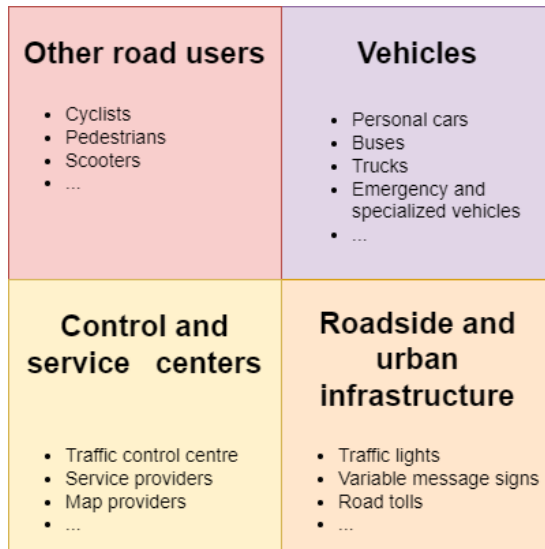


Fig. 6 C-ITS stakeholders

Some ITS services require cooperation by vehicles with their surrounding environment (including other vehicles, other road users, roadside and urban infrastructure, etc.) while other ITS services require connectivity to remote service platforms.

2.2.2 Frequencies

As described in more detail in chapter 2.3.1, the frequencies that can be allocated to C-ITS are in the following ranges:

- 5855 - 5875 MHz for non-safety ITS applications;
- 5875 - 5925 MHz for safety-related road ITS applications;
- 63.72 - 65.88 GHz for TTT (Transport and Traffic Telematics). Available for V2V, V2I and I2V systems.

2.2.3 Type of V2X communication and coverage

The communication distance coverage is closely linked to the wireless communication technology that will be used. Two wireless technologies coexist in C-ITS development: ITS-G5 and C-V2X.

- **ITS-G5**

ITS-G5 is the access layer technology (the physical layer and media access control) specified by ETSI and based on the IEEE 802.11p standard [5].

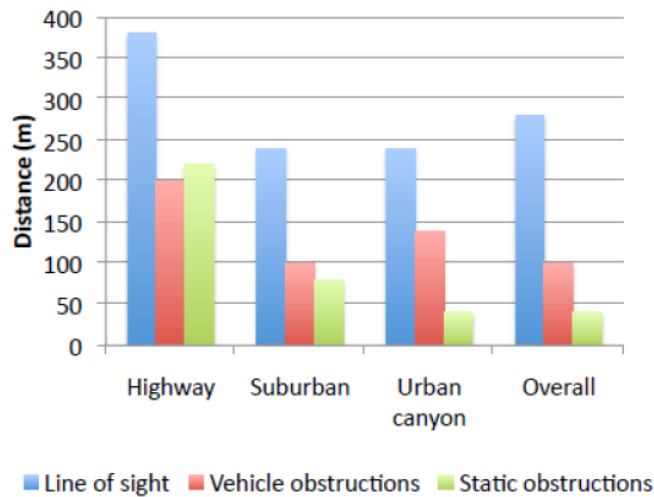
Tab. 1 shows the theoretical line-of-sight (LOS) communication coverage for V2V and V2I with a digital data rate of 6 Mbps assuming that the transmission power and noise level are 23 dBm and -95 dBm respectively.

Tab. 1 ITS-G5 Communication coverage [21]

	Antenna of the vehicle height	RSU antenna height	Coverage
V2V		-	510m
V2I	1.5 m	3m	700m
		5m	850m
I2V	-	3m	900m

The digital speed has a considerable impact on the communication coverage. Indeed, experimental results show that the V2I communication distance can be more than 800 and 700 m for 3 Mbps and 12 Mbps, while it is only 100 m for 27 Mbps.

Fig. 7 shows the ITS-G5 communication reliable distance that can be reached depending on the type of environment while remaining reliable.

**Fig. 7** Reliable communication range of ITS-G5 (PDR > 90%) [22]

- **C-V2X**

Vehicle-to-vehicle (V2V) communication, and more generally vehicle-to-anything communication (commonly referred to as "V2X"), has been heavily studied in the LTE evolution since 2015 and has increasingly become one of the main topics of the 3GPP Release 14. The standard version 14 is commonly called C-V2X. The physical layer of C-V2X allows for a better link compared to IEEE 802.11p. In addition, C-V2X can increase reliability, under certain conditions, by adding per-packet redundant packet transmission. Vehicles communicate with each other via the PC5 protocol or communicate with an eNB node.

Two modes are available for C-V2X:

- **Mode 4:** Vehicles select their radio resources autonomously, whether or not they are in cellular coverage. When vehicles are in cellular coverage, the network decides how to configure the V2X channel and informs the vehicles via the parameters. When vehicles are not in cellular coverage, they use a preconfigured set of parameters to override the configurable parameters;
- **Mode 3:** The selection of subchannels is managed by the eNB node and not by each vehicle as is the case in mode 4. Mode 3 is therefore only available when the vehicles are under cellular coverage.

The two modes are represented in Fig. 8.

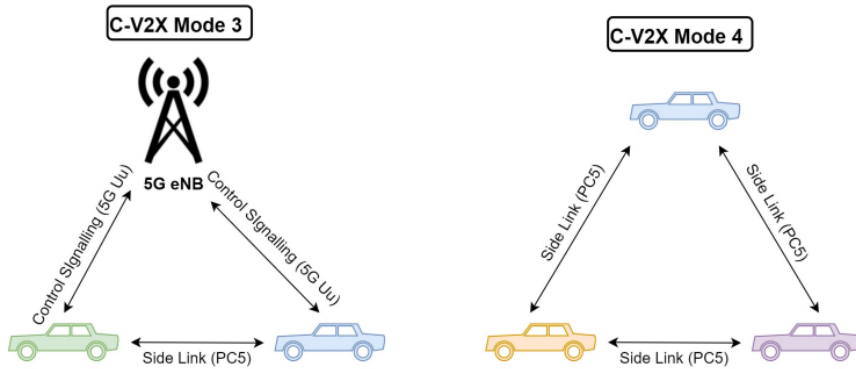


Fig. 8 Transmission modes 3 and 4 of C-V2X [23]

The diagram below (Fig. 9) shows the C-ITX communication distance that can be reached depending on the type of environment while remaining reliable.

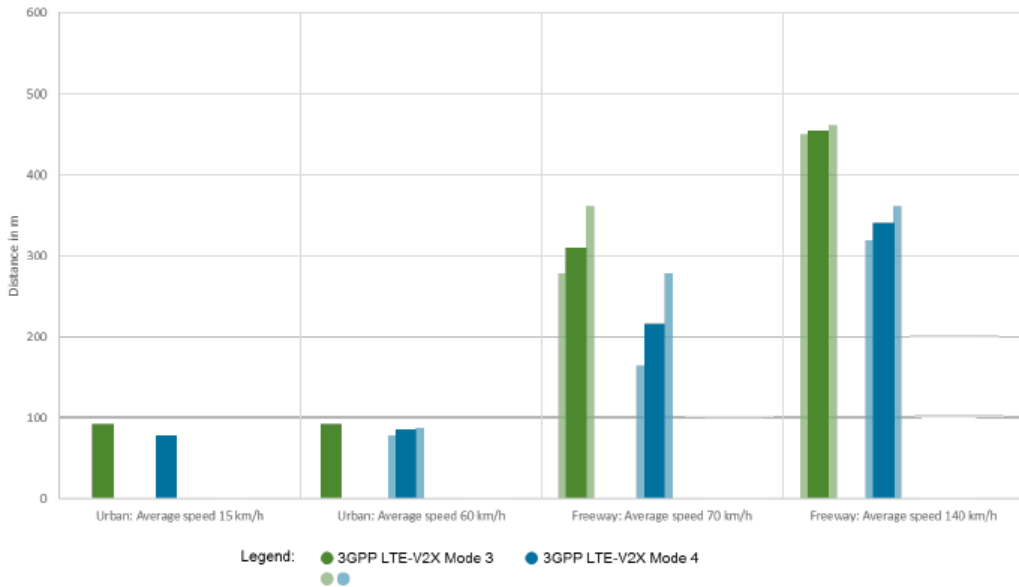


Fig. 9 Reliable communication range of C-V2X (PRR=90%) [24]

2.2.4 Information messages

C-ITS data is exchanged in the form of C-ITS messages described under European Commission [6]. The types of messages are classified according to the nature of the service to which they are attached. *Tab. 2* is a list of messages with an example for each.

Tab. 2 Message type descriptions for C-ITS

CAM (Cooperative Awareness Message)¹
CAMs are a kind of heartbeat message periodically broadcasted by each vehicle to its neighbours to provide information about presence, position, temperature, and basic status.
DENM (Decentralized Environmental Notification Message)²
DENMs are event-triggered messages broadcasted to alert road users of a hazardous event.
IVIM (Infrastructure-to-Vehicle Information Message)³
IVIM may be a lane change request received from the infrastructure due to road works.
SPATEM (Signal Phase And Timing Extended Message)³
SPATEM is responsible of the current status of one or more signalized intersections.
MAPEM (MAP Extended Message)³
This message is used to describe intersection geographies, and among other things to depict road segment descriptions, high-speed curve outlines or segments of a roadway.
SSEM (Signal request Status Extended Message)³
In response to the request (SREM), RSUs acknowledge with a SSEM notifying if the request has been granted, cancelled or changed in priority.
SREM (Signal Request Extended Message)³
SREM messages are sent by an OBU (On Board Unit) to an RSU (Road Side Unit) for requesting traffic light signal priority (public transport) or signal pre-emption (public safety).

2.3 C-ITS laws and regulations

Fig. 10 is an illustration of the regulatory hierarchy consisting of company standards, recognized standards and approved laws. An element at the bottom of the pyramid cannot contradict a law by making it more flexible. On the other hand, the reverse is possible and is often the case. A company standard will be more precise than a law.

The terms "standard" and "law" can have different meanings depending on the context. Here are their general definitions and the differences between them:

- A standard refers to a set of guidelines, specifications, or requirements that are established by a recognized authority or organization. Standards are typically developed to ensure uniformity, quality, safety, compatibility, or interoperability in various fields. They provide a framework for consistent practices, processes, or products;
- Law refers to a system of rules, regulations, or principles established by a governing authority, such as a government or legislative body. Laws are enforceable rules that govern behavior and relationships within a society or

¹ ETSI EN 302 637-2

² ETSI EN 302 637-3

³ ETSI TS 103 301

organization. They are created to maintain order, protect rights, provide justice, and regulate various aspects of human interactions.

The important difference between standards and laws is that the application of the former is not mandatory, yet it demonstrates the implementation of state-of-the-art technology that is usually considered a key requirement of the law. However, standards can be mandatory if they are referred to in contracts between parties or if the legislator prescribes mandatory compliance.

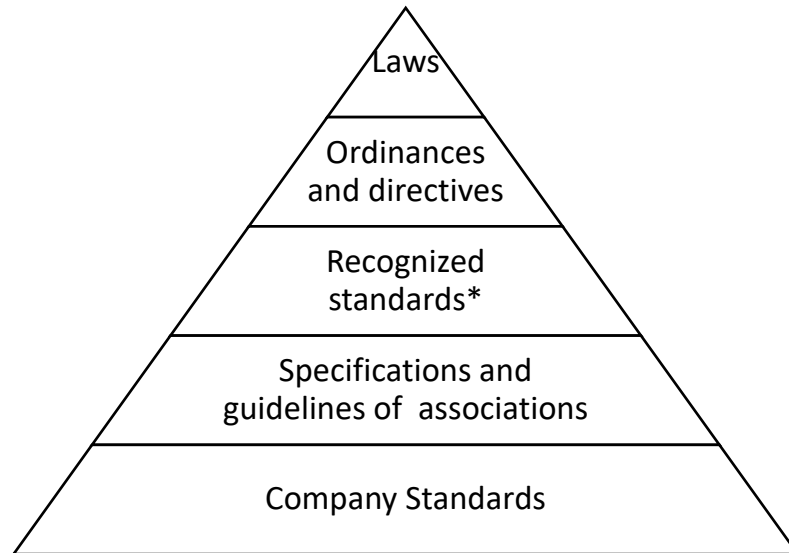


Fig. 10 The regulatory hierarchy

**Recognized standards include ISO, IEC, ITU, CEN, CENELEC, ETSI, SNV, CES and asut.*

To join the C-ITS framework, there is currently no Swiss law that stipulates the use of a standard for the cybersecurity of communication in vehicles themselves and/or between vehicles and infrastructure. Therefore, manufacturers are not required to follow these standards. However, the standards are listed and explained in the following subsections in order to understand today's cybersecurity standards in the automotive and C-ITS fields.

2.3.1 Swiss Laws

In Switzerland, the only law applicable to C-ITS is the one that defines usable frequency ranges. The Federal Office of Communications published a National Frequency Allocation Plan (NFAP) [25] that gives an overview of national utilization of the frequency spectrum. This NFAP is a mandatory guideline to allow for a complete use of the available radio frequency range. For any project in Switzerland using C-ITS or, more generally, an ITS, there is a list of allowed frequency ranges where communications can be transmitted.

According to the NFAP, the European Union and the Electronic Communications Committee, three ranges of frequencies are allocated to ITS:

- 5855 – 5875 MHz: Non-safety applications [26];
- 5875 – 5925 MHz: Safety applications;
- 63.72 – 65.88 GHz: ITS traffic safety and traffic efficiency applications [27].

2.3.2 European Commission Laws

Laws directly related to C-ITS

The European Commission published a law in 2019 related to C-ITS [6]. It describes the use cases and conditions for putting a new C-ITS on the market. Annex 4 of the law specifies the cybersecurity requirements with regard to risk assessment and evaluation. Although not applicable in Switzerland, the document provides a valuable basis for requirements and information about C-ITS risk assessment.

In particular, the law includes a list of minimum requirements and objectives for information classification activities in terms of Confidentiality, Integrity and Availability. The law also provides risk treatments containing control mechanisms (a link to the relevant standards is given when necessary). The following are some of the key points and requirements of the document:

- **Information Security Management System**

C-ITS station operators shall operate an ISMS in accordance with ISO/IEC 27001 [7]. This document describes the process framework for handling information security risk throughout an organization (including risk assessment activities).

The ISMS scope shall include all the operated C-ITS stations (ITS-S) and all other information-processing systems that process C-ITS data in the form of C-ITS messages whose type is detailed in chapter 2.2.

- **Information Classification**

This section lays down the minimum requirements for information classification.

C-ITS station operators/ stakeholders shall classify handled/managed information, whereby a security category can be represented as shown in *Fig. 11*.

Security Category information

= {(confidentiality, impact), (integrity, impact), (availability, impact)}

Security objective	Potential impact		
	LOW	MODERATE	HIGH
Confidentiality Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information	The unauthorised disclosure of information could be expected to have a limited adverse effect on organisational operations, organisational assets or individuals.	The unauthorised disclosure of information could be expected to have a serious adverse effect on organisational operations, organisational assets or individuals.	The unauthorised disclosure of information could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets or individuals.
Integrity Guarding against improper information modification or destruction; this includes ensuring information non-repudiation and authenticity	The unauthorised modification or destruction of information could be expected to have a limited adverse effect on organisational operations, organisational assets or individuals.	The unauthorised modification or destruction of information could be expected to have a serious adverse effect on organisational operations, organisational assets or individuals.	The unauthorised modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets or individuals.
Availability Ensuring timely and reliable access to and use of information	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organisational operations, organisational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organisational operations, organisational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets or individuals.

Fig. 11 Potential impact definitions for the security objectives of Confidentiality, Integrity and Availability [6]

As shown in the table in Fig. 12, C-ITS stakeholders are required to respect minimum impact values for every information message type handled. Each type of message can be considered in terms of Confidentiality, Integrity or Availability.

	Information originated by fixed C-ITS stations	Information originated by mobile C-ITS stations
Confidentiality	CAM: low DENM: low IVIM: low MAPEM: low SPATEM: low SSEM: low	CAM: low DENM: low SREM: low personal data contained in any of the three messages: moderate
Integrity	CAM: moderate	CAM: moderate
	DENM: moderate IVIM: moderate MAPEM: moderate SPATEM: moderate SSEM: moderate	DENM: moderate SREM: moderate
Availability	CAM: low DENM: low IVIM: low MAPEM: low SPATEM: low SSEM: moderate	CAM: low DENM: low SREM: moderate

Fig. 12 Minimum impact value to respect [6]

- **Risk assessment**

Security risk criteria shall be determined considering:

- the strategic value of the C-ITS service and C-ITS network to all C-ITS stakeholders and station operators of the service;
- the consequence for the reputation of the C-ITS network;
- legal and regulatory requirements and obligations.

The identification of risks and threats is not a list, and shall be identified in accordance with ISO/IEC 27005 [8]. Risk analysis is the product of the likelihood and impact levels as represented in *Fig. 13*.

Risk levels as product of impact and likelihood		Likelihood		
		unlikely (1)	possible (2)	likely (3)
Impact	low (1)	low (1)	low (2)	moderate (3)
	moderate (2)	low (2)	moderate (4)	high (6)
	high (3)	moderate (3)	high (6)	high (9)

Fig. 13 Risk levels [6]

At a minimum, moderate to high-level risks applicable to the C-ITS service and network shall be treated.

UNECE R155

The United Nations Economic Commission for Europe (UNECE) regulation R155, “Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system” [1], was created to address the growing risk that results from the increased connectivity and digitalization of the vehicle environment.

UN ECE R155 provides a list of threats and corresponding mitigations in its annex 5. Most of the listed threats are directly related to the vehicle, but some high-level threats could be applicable to a C-ITS system (V2X part), in particular:

- 4.3.2 Threats to vehicles regarding their communication channels;
- 4.3.5 Threats to vehicles regarding their external connectivity and connections.

General data protection regulation

GDPR (General Data Protection Regulation) [2] is a regulation in the EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). Its primary aim is to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business.

In the context of C-ITS, an opinion has stated that data broadcasted by vehicles must be considered personal data. Therefore, data exchanged via C-ITS shall be subject to the GDPR.

2.3.3 European standards for C-ITS

Overview

The CEN Technical Committee, a technical decision-making body with the European Committee for Standardization (CEN), works on standardization in the field of Communication Technology. This committee has supported the deployment of C-ITS in Europe and established multiple standards related to C-ITS: CEN/TC 278/WG 16 – Co-operative systems [3].

One of these standards, CEN ISO/TS 21177:2019 [9], is related to security, with a complete section about secure session establishment and authentication between trusted devices. A second standard, ISO/TS 21185:2019 [10], focuses on communication profiles for secure connections between trusted devices. Both standards are based on IEEE Std 1609.2™ [11], which formalized the authentication and encryption of broadcast messages. Finally, the CEN ISO/TR 21186-3 [12] design security standard covers both broadcast and unicast communications.

CEN ISO/TR 21186-3

This standard is the only one dealing with the analysis of C-ITS threats and the various controls mechanisms for these threats. It first gives an overview of security considerations for application specification and deployment in ITS. With regard to threat analysis, it includes a use-case driven threat model based roughly on common criteria processes for establishing threats, security objectives and SFR (Security Functional Requirement) relative to three genericized ITS station data sensitivity and access control scenarios. Each scenario can be used by security practitioners as a starting point to baseline ITS station platform protection profiles of varying application types and data sensitivities. The genericized protection profile security requirements are then compared to several existing (or under development) protection profiles established for automotive use cases to determine possible gaps in security controls that should be addressed when tailoring subsequent security targets or related protection profiles.

Below are various points summarizing the methodology of the standard and the section dealing with the cyber risk analysis of C-ITS.

1. Security Goals

The standard's high-level security goals are:

- To provide assurance that parties within the system receive the information necessary for achieving their functional goals;
- To provide assurance that unauthorized parties do not receive that information.

Those high-level security goals focus on two significant cybersecurity properties: Integrity for the first one and Confidentiality for the second one. However, there is a last one, which is Availability, that is not deeply addressed in this standard.

2. Methodology

The methodology used in this technical report is based on the IDX (Internet Data Exchange) device definition and on three types of scenarios. An IDX device corresponds to an ITS-S and belongs to a C-ITS which uses unicast connectivity to exchange data (including commands/requests) directly with a peer. Three types of scenarios, describing three types of data exchanges from IDX to another peer, are the basis for the threat methodology of the standard:

Tab. 3 *IDX scenarios*

Scenarios	Description	Resource sensitivity type
Scenario 1	IDX devices running public data retrieval applications, where the accessing device is requesting data that would not be subsequently linked to the device providing the data (for example, a road weather management system requesting road weather data from a vehicle on the road)	Public
Scenario 2	IDX devices running private data exchange applications, where the accessing device is requesting data that might be subsequently linked to the device providing the data (for example malfunction reports from a traffic signal controller, or path information from a pedestrian ITS-SU)	Privacy-relevant
Scenario 3	IDX devices running active access applications, where the accessing device is requesting to write to the host device or execute operations on the home device. An example of this is a management device wirelessly accessing a variable message sign (VMS) to change the message	Write-execute data

These resource types of security/privacy sensitivity are used to differentiate the three access scenarios seen above. The classification of individual assets into one or more of these categories allows for a better interpretation and classification of the results given in the various tables of this standard.

3. Device asset listing

The scenario-specific asset listing in the table on p. 22 of ISO/TR 21186-3 is intended to provide the security practitioner with the assumed assets of the IDX device that can be threatened in the operational environment. Five examples of assets are shown in *Tab. 4*.

Tab. 4 *Device assets examples*

Asset	Description	S1	S2	S3
IDX device firmware (platform)	Firmware for the IDX device.	X	X	X
User passwords and other authenticators	Authenticators that authorized users use to prove their identities.	X	X	X
IDX device application and data access control policy(s)	Access control policy residents on the IDX device that controls access to IDX device's client applications and data resources. This policy can be used by the IDX device to make grant/deny requests when the user using the IDX device requests certain operations or data accesses.		X	X
Application encryption public keys	An entity's application-specific 1609.2 encryption public key, typically embedded in a 1609.2 certificate.			X
Application encryption private keys	The pairwise private key for the encryption public key. This key is not shared/disclosed by the owner. It is used to perform an ECIES encryption over data.			X

4. Threat modelling process

The threat modelling process includes the following steps:

- Identify threat categories and attack vector types using table 2 (p. 26 of ISO/TR 21186-3);
- Characterize different attack motivations using table 3 (p. 26 of ISO/TR 21186-3);
- Identify threats using table 4 (p. 27 of ISO/TR 21186-3);
- For each threat, provide a qualitative risk rating based on a rough impact and probability level (Low, Medium and High).

Annex A of ISO/TR 21186-3 lists the different threats and their mapping to the data sensitivity scenario(s). For each threat, the following information is given:

- Brief description of the threat;
- A listing of the type of threat actors likely involved;
- One or more attack vectors likely to be associated with the threat;
- Possible motive;
- Objective(s) of the attacker;
- Desired outcome(s) of the attacker;
- A probability and impact level;
- One or more associated security objectives or organizational policies to counter the threat.

2.3.4 Cyber security standards for the automotive sector

ISO/SAE 21434 [13] is the standard on cybersecurity applied to road vehicles. It specifies engineering requirements for cyber security risk management, including norms on concept development, product development, production, operation, maintenance, and decommissioning of electrical and electronic (E/E) systems in road vehicles as well as their components and interfaces. Although this standard does not cover C-ITS (or at least ITS external to road vehicles), its methodology and requirements could be applied to the different C-ITS modules that can communicate with the vehicle.

A central focus of the standard is threat analysis and risk assessment (TARA). The overall process of conducting a TARA is described in *Fig. 14*.

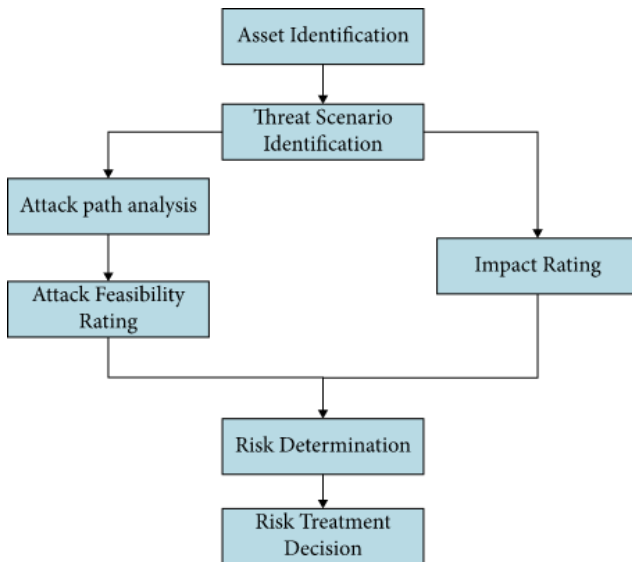


Fig. 14 TARA process in ISO 21434:2021

- The first step consists of the item definition describing the functions and limits of the system;
- The asset identification (set of functions, data components and flow) is then possible, as well as the definition of possible damage scenarios and an estimation of their impact;
- Threat scenarios can be deduced from the damage scenarios;
- The attack path analysis represents the identification and estimation of the steps involved in threat and damage scenarios;
- The feasibility of the attack is then evaluated; the combined metrics of the attack feasibility rating and the impact rating give a risk determination and, depending on the risk level, a risk treatment decision.

To focus on threat identification, part 15.4 of the standard suggests two different methods to find threat scenarios. The first is expert group discussions. The second is a systematic approach using frameworks such as TARA itself, EVITA (E-safety vehicle intrusion protected applications) or STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege).

The first two frameworks involve the use of risk analysis templates with different weights to determine the risk value, including threat scenario identification, impact rating, attack path analysis, and attack feasibility rating. The third framework, STRIDE, is a common model to identify security threats in the IT sector. These frameworks can be implemented to analyze the different threats of a C-ITS module.

The EVITA project [28], although older (2008), has issued a framework and examples of identification and treatment of cybersecurity threats. Threat scenarios are referred to as "dark-side scenarios".

The approach adopted in developing the dark-side scenarios is based on the following elements:

- Identification and classification of possible attack motivations;
- Evaluation of associated attacker capabilities (technical, financial);
- Attack modelling, comprising:
 - Identification of specific attack goals that could satisfy the attack motivations;
 - Construction of possible attack trees that could achieve attack goals, based on the functionality identified in the use cases.

Fig. 15 is a partial example of a threat identification using a tree construction for the attack goal defined as “Getting traffic lights green ahead of attacker”.

As we can see, threats can come from the vehicle, the C2I protocol and the infrastructure (in this case, the traffic lights). This methodology could then be adapted to the analysis of C-ITS threats.

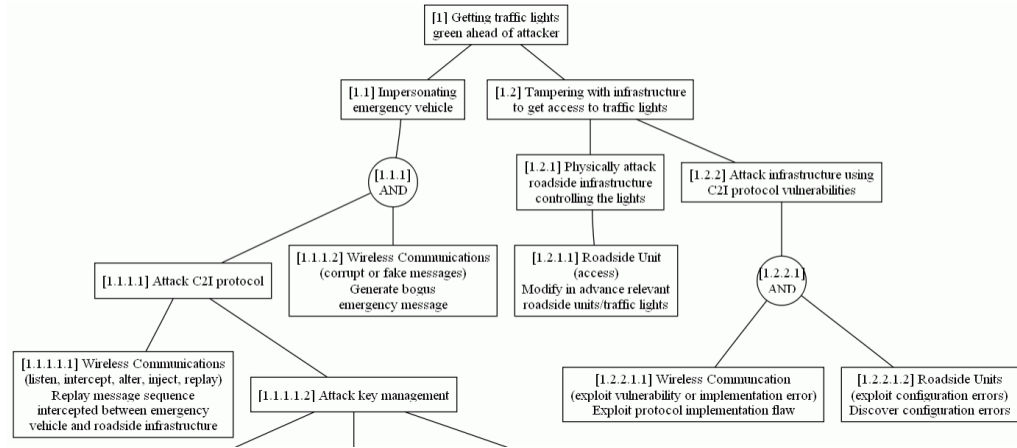


Fig. 15 Partial example of threat identification with the EVITA method

2.4 State of the art of C-ITS

There are not many projects focusing on C-ITS and the management of its threats, but one large-scale project that has been set up is the SCOOP project.



Fig. 16 Project SCOOP logo (Systèmes Coopératifs) [29]

2.4.1 SCOOP project overview

SCOOP is the only C-ITS deployment project in Europe built on a cooperation between road managers and car manufacturers to address real-world challenges such as privacy, cybersecurity, industrial processes, calls for tenders, compliance audits, and interoperability. Funded at 50% by the European Commission, project SCOOP was divided into two parts:

- 2014-2016: Specification and development;
- 2016-2018: Experimentation.

The project ended in December 2019. Fig. 17 shows the project’s key points:

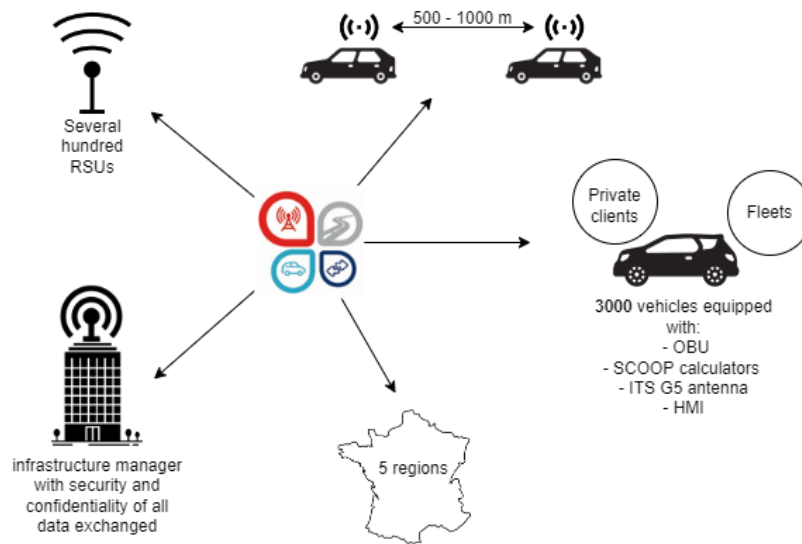


Fig. 17 Key points of the SCOOP project

The aim of the project was to lay the foundations of a C-ITS at the level of the specification and development of a network, and to provide a proof of concept with a real test on several sites.

2.4.2 SCOOP project C-ITS threat analysis

In the context of the SCOOP project, and especially in the specification and development phase, the cyber security aspect of C-ITS had to be addressed and dealt with. Some information is available in the presentation entitled “Security of SCOOP@F Wave1” [30].

The objectives were to:

- Specify, implement, test and validate the security of the system;
- Secure V2X messages;
- Implement the certificate management system (PKI);
- Design an interoperable security system with the security systems of other C-ITS deployed across Europe;
- Create an end-to-end secure architecture;
- Ensure the protection of personal data.

For risk analysis, an approach based on the **EBIOS** (Expression des Besoins et Identification des Objectifs de Sécurité – Expression of Needs and Identification of Security Objectives) risk analysis methodology was used, along with a compliance check with **ETSI** (European Telecommunications Standards Institute) **TVRA** (Threat and Vulnerability Risk Assessment). The combination of these methods offers both an assessment of the risks in the event of a breach in data Availability, Integrity and Confidentiality, and a technical vision of the architecture components based on a complete and precise TVRA assessment.

EBIOS risk analysis

EBIOS is a method for assessing and treating digital risks and is not specific to C-ITS. EBIOS is published by the National Cybersecurity Agency of France (ANSSI) [31].

The EBIOS Risk Manager method adopts an approach to the management of digital risk by studying possible risk scenarios. The method starts from the highest level (major missions of the studied object) to progressively reach the business and technical functions. The pyramid in *Fig. 18* is constituted according to the levels of cyber-attack.

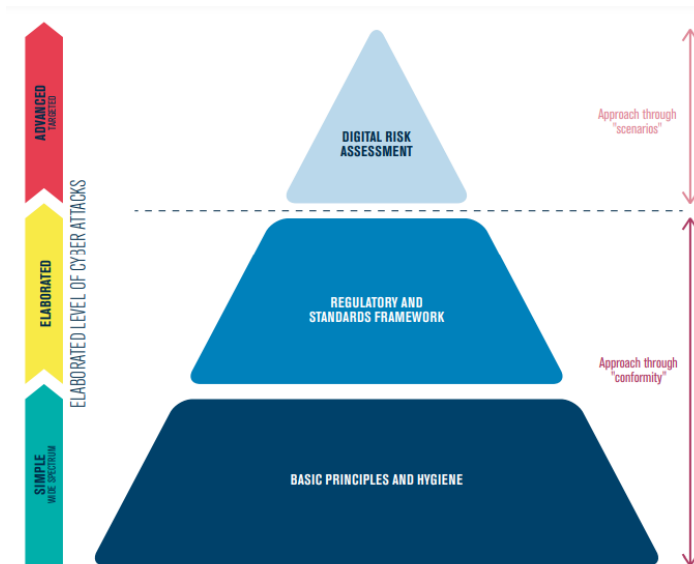


Fig. 18 EBIOS digital risk management pyramid

The method consists of an iterative approach in 5 workshops, as presented in *Fig. 19*.

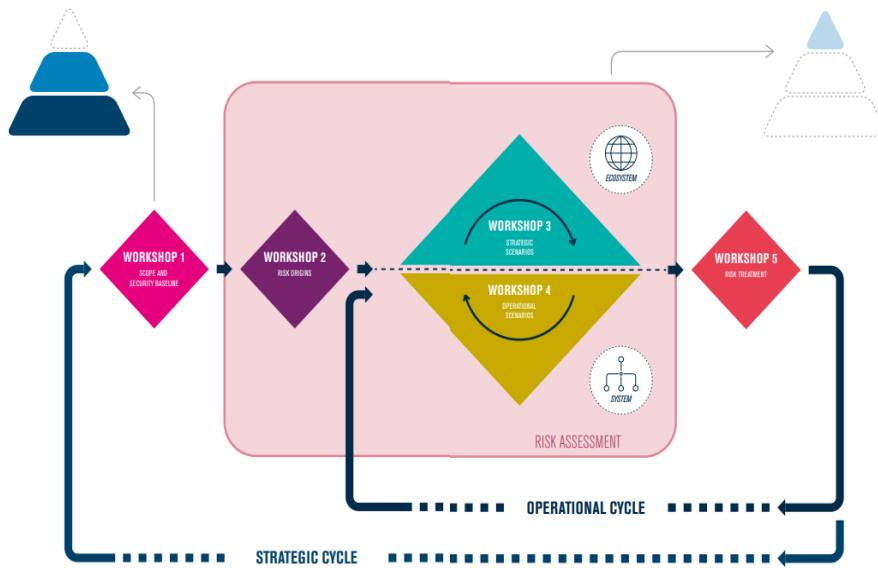


Fig. 19 EBIOS method

Tab. 5 presents the 5 workshops with an accompanying description.

Tab. 5 SCOOP Workshops

Workshops	Description
Workshop 1 – Scope and security baseline	Aims to identify the studied object, the participants in the workshops and the timeframe. It makes it possible to follow an approach by "compliance", corresponding to the first two stages of the digital risk management pyramid.
Workshop 2 – Risk origin	Identifies and characterizes the risk origins (RO) and their high-level targets, called target objectives (TO). The RO/TO pairs deemed the most relevant are selected at the end of this workshop.
Workshop 3 – Strategic scenario	Establishes a mapping of the digital threats to the ecosystem with respect to the studied object. High-level scenarios, called strategic scenarios, can be constructed. They represent the attack paths that a RO is likely to take to reach its TO. These scenarios are assessed in terms of severity.
Workshop 4 – Operational scenario	Constructs technical scenarios that include the methods of attack that are likely to be used by the RO to carry out the strategic scenarios. This workshop adopts an approach similar to the preceding workshops but focuses on critical supporting assets. Here, the level of likelihood of the operational scenarios is assessed.
Workshop 5 – Risk treatment	Creates a summary of the risks studied in order to define a risk treatment strategy. The latter is then broken down into security measures written into a continuous improvement plan. The summary of the residual risks is established to define the framework for monitoring risks.

ETSI TVRA

A Threat Vulnerability and Risk Analysis (TVRA) is used to identify risk to the system based upon the product of the likelihood of an attack and the impact that such an attack would have on the system. The methodology and protocols are defined in an ETSI standard [14].

The method systematically addresses aspects of Information and Communications Technology systems and quantifies their assets, vulnerabilities and threats. The primary focus of TVRA is on the assets of a system to ensure they can perform their primary function when subjected to malicious attacks. The output of TVRA is a quantified measure of the risks to the assets and a set of detailed security requirements that will minimize that risk.

In addition, the method proposes a general classification of threats in 5 categories:

- Interception;
- Manipulation;
- Denial of service;
- Repudiation of sending;
- Repudiation of receiving.

These 5 categories can be used as a basis for determining high-level threats related to the services offered by C-ITS.

The TVRA process is summarized in the diagram in Fig. 20.

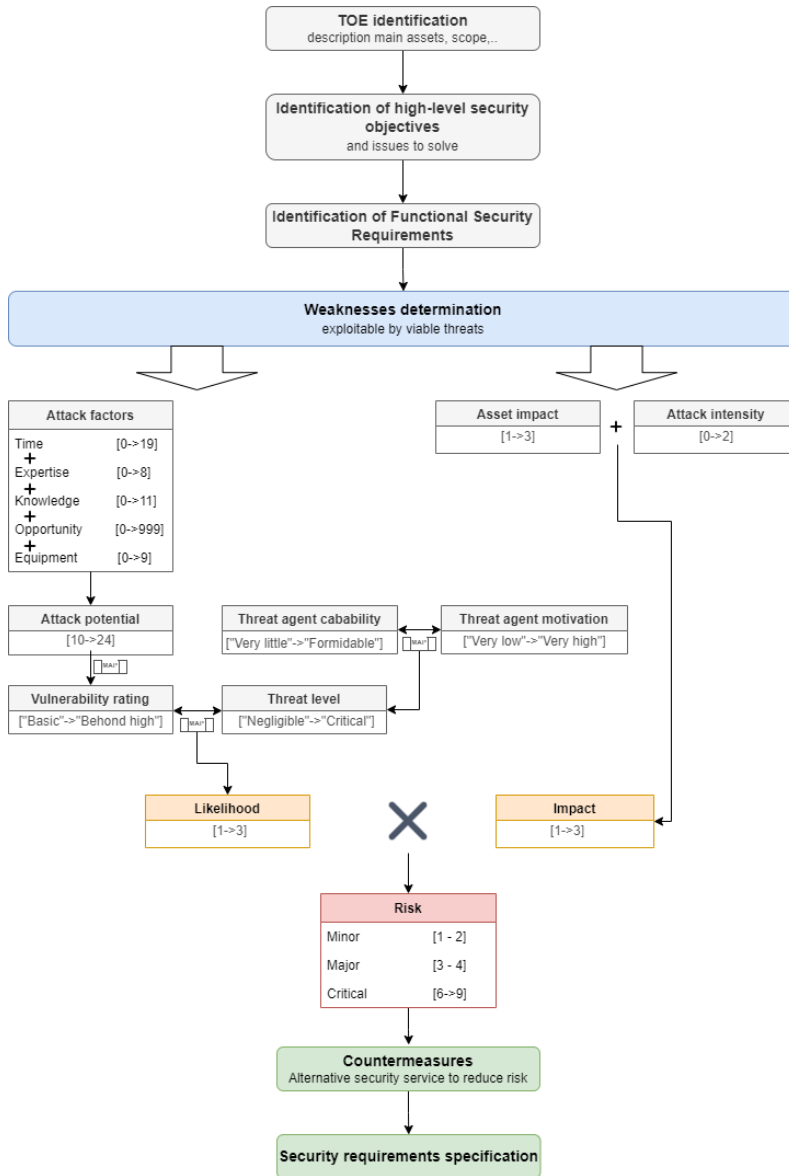


Fig. 20 TVRA process

2.4.3 SCOOP project results

Although the risk analysis of the SCOOP project is not available, the conclusions of the project reveal that 4 families of macro risks were identified:

- Unavailability of SCOOP services;
- Theft of user data;
- Data corruption, error in traffic management;
- Disturbance of controls of a vehicle.

These high-level risks were analyzed on 7 entities/objects related to the SCOOP project:

- Vehicles;
- RSUs;
- C-ITS platform;
- ITS-G5 (the network);
- Information systems of road operators;
- Cellular networks;
- Public Key Infrastructure.

2.5 C-ITS threats

The hazard analysis method to be implemented in this project should be partially based on the high-level threats highlighted in UN ECE R155 [1] and in CEN ISO/TR 21186-3 [12].

2.5.1 UN ECE R155 threat examples

Annex 5 of this regulation describes high-level threats to the vehicle which can be integrated into the V2X part of the C-ITS risk analysis. *Tab. 6* represents some examples of threats.

Tab. 6 *Examples of threats from R155*

High level and sub-level descriptions of vulnerability/ threat	Example of vulnerability or attack method
4.3.2 Threats to vehicles regarding their communication channels	Spoofing of messages or data received by the vehicle
	Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data
4.3.5 Threats to vehicles regarding their external connectivity and connections	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
	Hosted 3 rd party software, e.g. entertainment applications, used as a means to attack vehicle systems
	Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems

2.5.2 CEN ISO/TR 21186-3 threat examples

Standard 21186-3 describes generic and non-exhaustive threats to C-ITS. *Tab. 7* lists two examples of threats.

Tab. 7 Examples of threats from ISO/TR 21186-3

Category	Description
T.PHYSICAL_TAMPER	Asset: IDX device
	Area of Concern: An attacker could attempt to access the internal components of the IDX device to bypass software security controls and extract data including firmware which could lead to exposure of default passwords and other information.
	Actor: Disgruntled insider; stalker; hackers, taggers and script kiddies; criminal individual.
	Attack vectors: Maintenance environment; internal system; authorized actions of non-privileged users; authorized actions of privileged users; device port; immediate physical proximity.
	Motive: Notoriety; personal satisfaction; disgruntlement; positional/stepping stone.
	Outcome: Disclosure (identification of TOE vulnerabilities that can be able exploited or access to sensitive information stored within the device).
	Probability: M (Medium); Impact: L (Low)
T.ENVIRONMENT_ACCESS_PRIVACY_PROTECTED_DATA_WITHOUT_CONSENT	Asset: PII/tracking data/proprietary data.
	Area of concern: Privacy protected data is transmitted from the ITS-SCN to the IDX device and accessed without data owners explicit permission.
	Actor: Privacy actor.
	Attack vectors: Authorized actions of privileged user; normal user.
	Motive: Accidental, tracking/stalking, personal financial gain.
	Outcome: Disclosure.
	Probability: H (High), Impact: M (Medium)

2.6 Synthesis and conclusion of the state of the art

C-ITS represents a major evolution in the ITS domain. Applications already linking connected systems to provide functionality to road users will be able to communicate and exchange data to, among other things, further improve the road experience for drivers, other road users and pedestrians in terms of traffic flow and safety. Applications attached to the services provided by C-ITS will be required for the development and future circulation of class 4 and 5 automated vehicles.

The cybersecurity of C-ITS plays a crucial role in the areas of information confidentiality, data integrity and service availability. Analysis of the threats and weaknesses attached to C-ITS is the first step to defining cybersecurity requirements that guarantee a low level of risk and a high level of confidence in the C-ITS applications that will be widely deployed in the near future.

The state of the art of threats and threat analysis methods is an integral part of this report. The different regulations or standards that are relevant to the objectives of defining a

methodology were addressed, as well as the methods used in pilot projects on C-ITS. The results of the research are summarized in *Tab. 8*:

Tab. 8 *Synthesis of research*

Regulation / Standard / Methodology	Purpose of document
UNECE R155	<p>Purpose of document: This document concerns the approval of vehicles with regards to cyber security and Cyber Security Management Systems.</p> <hr/> <p>Positive elements in relation to the scope of the project: The document lists threats to vehicles involving their communication channels and their external connectivity and connections.</p> <hr/> <p>Negative elements in relation to the scope of the project:</p> <ul style="list-style-type: none"> • This regulation is for road vehicles only; • No method description. <hr/> <p>Possible utility in exploitation in the project: Use these threat lists as the basis for determining vehicle-related ITS-SU threats.</p>
ISO 21434	<p>Purpose of document: This document addresses the cyber security perspective in the engineering of electrical and electronic (E/E) systems within road vehicles.</p> <hr/> <p>Positive elements in relation to the scope of the project:</p> <ul style="list-style-type: none"> • The document describes an effective method of threat analysis and risk assessment (TARA); • TARA based on threat scenario determination. <hr/> <p>Negative elements in relation to the scope of the project: This standard is not dedicated to C-ITS but to road vehicles only. However, it could be adapted for the treatment of C-ITS threats.</p> <hr/> <p>Possible utility in the project: Use the well-defined TARA methodology with quantifiable risks and apply it to the broader C-ITS domain.</p>
ISO/TR 21186-3	<p>Purpose of document: This document provides guidelines on security applicable in Intelligent Transport Systems (ITS) related to communications and data access. It provides analyses and best practice content for secure ITS connectivity using ISO/TS 21177.</p> <hr/> <p>Positive elements in relation to the scope of the project:</p> <ul style="list-style-type: none"> • Dedicated to C-ITS; • Based on 3 distinct types of scenarios; • Lists of C-ITS assets, attack vector types, attack motivations and threats are quite complete but not exhaustive. <hr/> <p>Negative elements in relation to the scope of the project:</p> <ul style="list-style-type: none"> • Availability not considered in the cyber security goals; • Risk evaluation not accurate (qualitative judgment without rationales). <hr/> <p>Possible utility in the project: Use the different lists established by the document as a basis for defining assets, attack vector types, attack motivations and threats and for injection into a methodology like TARA or TVRA.</p>
C-ITS security policy release	<p>Purpose of document: Annex 4 to the Commission Delegated Regulation – Supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems - Definition of security policy.</p> <hr/> <p>Positive elements in relation to the scope of the project:</p> <ul style="list-style-type: none"> • Dedicated to C-ITS; • Drafted as clear requirements; • Risk evaluation is accurate, dependent on Impact and Likelihood; • Lists of C-ITS message categories. <hr/> <p>Negative elements in relation to the scope of the project: No proposal for C-ITS threats.</p>

	<p>Possible utility in the project: Regulation describes the methodology to be used for the risk analysis of the different communication messages. The methodology is similar to TARA and the threat analysis part of the messages could be integrated to a general TARA.</p>
<p>EBIOS risk analysis</p>	<p>Purpose of document: EBIOS is a method for assessing and treating digital risks.</p>
	<p>Positive elements in relation to the scope of the project:</p> <ul style="list-style-type: none"> • Based on an iterative workshop process; • Risk evaluation is accurate, dependent on Impact and Likelihood.
	<p>Negative elements in relation to the scope of the project: Methodology not dedicated to C-ITS.</p>
	<p>Possible utility in the project: The successive workshops can define the set of ITS-SU retained in a C-ITS simulation, as well as their main functions and threats, which can then be used in a defined methodology with a quantifiable risk level.</p>
<p>ETSI TS 102 165-1</p>	<p>Purpose of document: The document defines a method primarily for use by ETSI standard developers in undertaking an analysis of the threats, risks and vulnerabilities (TVRA) of an Information and Communications Technology (ICT) system.</p>
	<p>Positive elements in relation to the scope of the project: TVRA based on weakness determination.</p>
	<p>Negative elements in relation to the scope of the project:</p> <ul style="list-style-type: none"> • The TVRA method is not dedicated to C-ITS but to a more general level ICT system; • Requires detailed knowledge of the system and its scope for knowledge of the weaknesses (C-ITS represents a multitude of subsystems).
	<p>Possible utility in the project: Even if the weaknesses are not known, making the use of TVRA delicate, the 5 categories of threats found in the standard can be used as a basis for defining high level threats related to the services offered by C-ITS.</p>

High-level specifications of the C-ITS, such as the frequency ranges to be used, the types of messages exchanged by the ITS-SU as well as the V2X distances according to the type of technology used (ITS-G5 /C-V2X), have also been established based on the bibliography, in order to provide basic assumptions for the creation of the cyberthreat simulation.

On the basis of the above discussion, the choice of methodology shall now be made. As the study of threats is easier to apprehend than the study of weaknesses given that the system can be composed of many different objects (car, infrastructure, pedestrians, etc.), the **TARA method** is the most suitable as a structure for the analysis. The factors entering the analysis, such as assets, attack vector type, attack motivation, and threats can be extracted from other documents (**UNECE R155, ISO/TR 21186-3, ETSI TS 102 165-1**) and determined via workshops and expert judgment. The part concerning the risks related to messages can be extracted from the **C-ITS Security Policy Release, annex 4**.

3 Cyberthreat methodology and identification of virtual platforms

3.1 Introduction

Tomorrow's mobility will be defined by Cooperative Intelligent Transport Systems (C-ITS) coupled with V2X communication technologies. These systems and their interconnectivity aim to optimize the behaviour of fleets in terms of transport efficiency, carbon footprint, readiness for automated mobility and risk minimization for road users.

Cyberthreat methodology refers to the techniques and strategies employed by malicious actors to exploit vulnerabilities in digital systems and networks. These methodologies encompass a wide range of activities, including but not limited to phishing, malware attacks, social engineering, and distributed denial-of-service (DDoS) attacks. By understanding the various methods employed by cybercriminals, cybersecurity professionals can develop proactive measures to detect, prevent, and mitigate potential threats.

Threat modelling and risk assessment are two major components of cybersecurity practices during the development or analysis of a product. Threat modelling consists in identifying potential threats and vulnerabilities of a product, or system. Risk assessment is the process to quantitatively, or qualitatively, assess the likelihood and consequences of threats on the system under consideration; its goal is to provide valuable information for risk management, which ultimately decide on whether the risk is acceptable, or need to be mitigated. Threats are translated into risks via criteria, such as product safety integrity, and thresholds (in terms of experience and budget).

The following section will present the enumeration of these criteria, and their use for finding threats. This can be summarised in the six steps shown in *Fig. 21*. It should be noted that the linear procedure presented here is not always representative of real risk assessment processes, which are more commonly iterative processes triggered by modifications to the system, including software or hardware updates, and publication of new vulnerabilities for items built into the system.

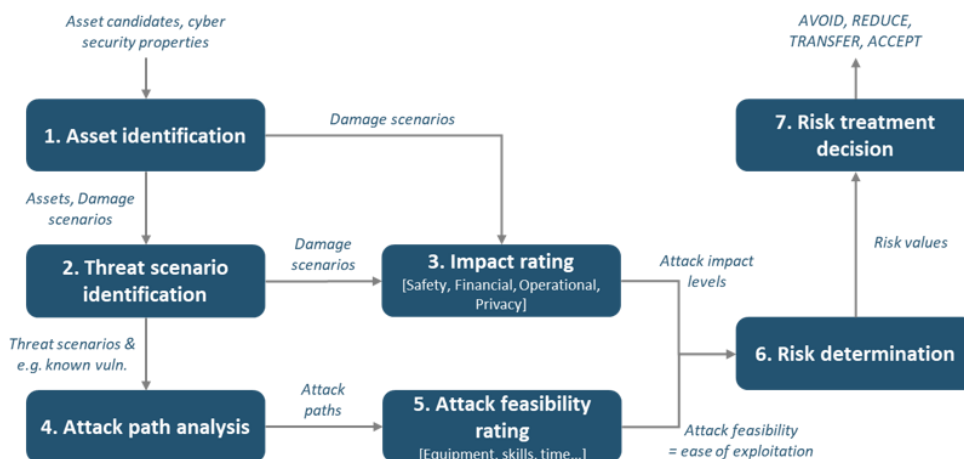


Fig. 21 Sequence of actions for threat modelling and risk assessment

This section begins by outlining the methodology for analyzing and modeling threats and risks, and by defining the scenario used in V2I (Vehicle-to-Infrastructure) communication. The following part of this section presents a benchmark of virtual platforms that facilitates the automated analysis of threats and risks. It also discusses the selection of the tool utilized for this project.

3.2 What are threat modelling and risk assessment?

Threat modelling enables the detection and mitigation of security issues at an early stage, or even at a developing stage, when they are the easiest to address and most cost-effective to resolve.

All the main IT-related threat modelling processes use a visual representation of the product/application/infrastructure being analysed. This element is usually broken down into various elements to aid in the analysis. A common visual representation is the data flow diagram (DFD), which typically uses five types of symbols for data flows, data stores, processes, interactors, and trust boundaries.

The model is usually built and worked on jointly by security and non-security experts, and has proven to be useful for interdisciplinary collaboration and integration over a common product.

Risk assessment aims to identify and analyse potential threats to a system. Risk assessment and threat modelling therefore have a common goal. The two processes differ, however, in terms of costs. Threat modelling is straightforward to put in place and can be run as many times as needed with little added difficulty and at virtually no cost. Risk assessment, on the other hand, requires the cooperation of multiple professional bodies, the identification of assets, the identification and assessment of vulnerabilities and threats, the definition of exploitability and levels of risk, and the definition of risk mitigation measures.

The following entertaining quote captures how risk assessment differs from threat modelling.

“So I guess, for me, risk assessments have always been very much like underwear. They’re incredibly personal, and not everybody wears the same one. Everybody’s risk is completely different. I don’t know what your risk is, you don’t know what my risk is, right? And it’s hard to apply risks to somebody’s product, and we did this when we were doing pen testing because we don’t know, we don’t understand. You might have completely different controls or regulatory requirements, or something else that says, ‘You need to do this because you feel that’s a risk.’ We don’t know that.” [32]

3.3 Threat Analysis and Risk Assessment methodology

Fig. 22 presents the 7 steps described in the ISO/SAE 21434 standard to perform Threat Analysis and Risk Assessment (TARA). This methodology has the advantage of considering all relevant threats, even those that are not currently feasible due to a technology gap, e.g. when encryption is too strong on the computer in question. As long as the threats are listed, they will be reviewed periodically to avoid any possible exploitation in the future due to new technologies. The first three categories ("Asset identification", "Threat scenario identification" and "Impact rating") are part of Threat Analysis, which is the first step of TARA. Its main objective is to identify and understand the different threats that could impact the security of an automotive system. This includes external threats from malicious actors such as hackers, as well as internal threats such as design errors or hardware failures. The four other categories ("Attack path analysis", "Attack feasibility rating", "Risk determination" and "Risk treatment decision") are part of Risk Assessment, the second step of TARA. Once potential threats have been identified in the first step, Risk Assessment focuses on evaluating and quantifying the risks associated with those threats.

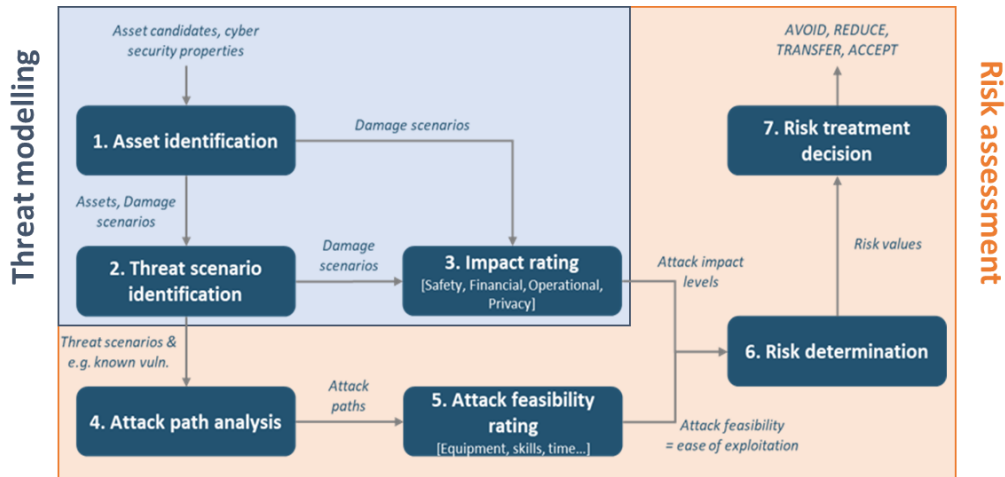


Fig. 22 Threat Analyses and Risk Assessment methodology

The following sections explain each of the seven steps in more detail.

3.3.1 1. Asset definition

The first step of risk assessment is to identify the sensitive elements of the system under analysis. These elements are called assets.

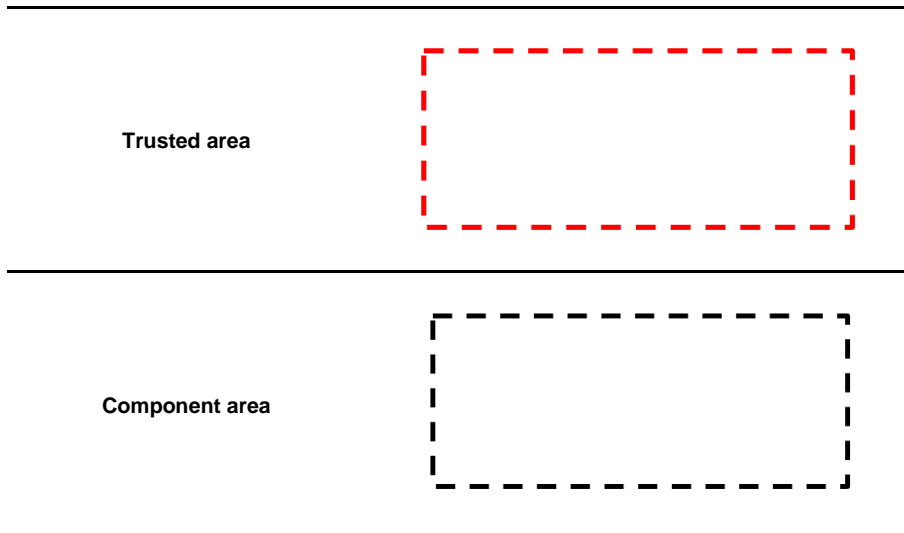
In the context of Cooperative Intelligent Transportation Systems (C-ITS), an asset refers to a component of resources that is essential for the functioning of the C-ITS ecosystem and for the exchange of information between vehicles and other entities. The value of an asset can be seen from three perspectives: Confidentiality, Integrity and Availability. Examples of assets can include: V2X messages, OBU/RSU firmware, and the network layer.

A recommended approach is to model the system and draw different communications between the elements. This visual approach allows for a global view of the system and ensures all elements are represented. The level of the model depends on the risk assessment level. The aim of risk assessment is to have an overview of the system and of the risk in the system. Thus, the model level is at component level: RSU, OBU, TMC, and so on.

The model of the system can be drawn using the elements presented in *Tab. 9*.

Tab. 9 Element allowing for representation of the system model

Elements	Representation
Component of the system	
Wireless communication	
Wired communication	



3.3.2 2. Threat scenario identification

A threat in cybersecurity terminology corresponds to a potential danger for a given system or systems. A threat can have different sources:

- **Unintentional:** An employee plugs an USB key into a computer and opens a corrupt attachment;
- **Intentional:** A voluntary action by a system insider or outsider (person or group).

These different threats cannot be treated in the same manner. Unintentional threats can only be avoided by providing a cybersecurity culture to the employees. This kind of threat will not be studied in this section. In what follows, the focus will be on intentional threats and the procedure to find them.

Threat modelling means analyzing the representations of the model to highlight concerns about privacy and security characteristics. To increase its effectiveness, this activity must be included in the system lifecycle and kept up-to-date to include newly found threats.

Different threat modelling methodologies have been discussed in recent years, including PASTA, STRIDE, Trike, and VAST [37]. These methodologies have advantages and disadvantages that will be listed in this section. Based on these observations, a methodology will be chosen for this project.

P.A.S.T.A

PASTA, which stands for **P**rocess for **A**ttack **S**imulation and **T**hreat **A**nalysis, is a framework that combines both threat modelling and risk analysis. PASTA can be split into 7 stages. The first three are related to scope definition and the interaction with others elements. Stage four is a threat analysis where the scope is analyzed to find and gather different threats. This analysis is based on probabilistic attack scenarios, security events and threat intelligence correlation on public sources like Hackerone reports, logs, incidents, etc. After that, stages five and six analyze these threats to establish if they can lead to weaknesses and vulnerabilities that constitute a risk for the system. Finally, in stage 7, an impact analysis is conducted to determine if these risks must be mitigated or not [35][36].

From the perspective of C-ITS, the main advantage of this framework is also a disadvantage: the fixed sequence of steps from the scope definition to the impact analysis leaves no room for the modifications to the framework that would be needed for a C-ITS. Its second disadvantage is that it does not provide a methodology to find new threats to the system. Discovery of new threats is mainly based on expert discussion.

Trike

Trike is a complete security audit framework from asset definition to risk value. The Trike framework articulates a defensive point of view. The first step is to build a requirement model by enumerating the system's actors, asset actions, and rules, and to transpose this information into an actor-asset-action matrix in which columns represent assets and rows represent actors. Each cell is then divided into four parts: Creating, Reading, Updating, and Deleting (CRUD). Each sub cell is assigned as an allowed action, a disallowed action, or an action with rules. Based on this matrix, a data flow diagram (DFD) is built to map all the actors and assets, which creates a global representation of the system. The DFD is analyzed to identify elevation of privilege or denial of service threats. For each discovered threat, a new attack tree is created. Finally, based on this attack tree, a calculation for each actor predicts if the attack presents a risk or not.

The advantage of Trike methodology is the use of a data flow diagram which allows for a complete representation of the system and makes it possible to determine if all elements are represented. Its main disadvantage is being a data-oriented framework, which means that other threats are not analyzed. In the case of C-ITS, however, data management is not the most significant problem.

VAST

VAST is based on "ThreatModeler", a paid software that can automate threat modeling and scale it throughout an entire organization. Its primary use is during a product's DevOps cycle, which is not the primary use case for this project.

Its advantage for this project is its well-designed visual features with DFD generation.

STRIDE

The STRIDE methodology is suggested in many standards and lists the 6 main categories of threat type from an attacker's perspective:

- Spoofing;
- Tampering;
- Repudiation;
- Information;
- DoS;
- Elevation of privilege.

Based on these six categories, different perspectives can be defined through brainstorming to gather different perspectives from different roles (i.e., cybersecurity specialist, safety engineer, business lead, etc.) and to list different threats specific to the project for each category. This methodology has the advantage of being well studied and easy to implement and use. There is also no need to buy software or access to a database.

Synthesis

Of the five studied frameworks, the most suitable for this project is STRIDE. STRIDE can be customized to create a framework specific to C-ITS. Trike and PASTA are too generic and focus on the complete risk assessment framework, which is not optimal for this project due to the singularity of risk assessment for a C-ITS system. Finally, VAST is based on unintuitive paid software and is not specially made for C-ITS.

Thus, the C-ITS threat modelling framework will be based on STRIDE with an add-on that allows for the representation of the system using a data flow diagram to ensure a complete representation of the assets under consideration.

3.3.3 3. Impact Rating

The impact of a potential attack on the system is evaluated under 4 categories: Safety, Operational, Privacy and Financial. Each category can receive one of four impact ratings: negligible, moderate, major and severe. This leads to the following categorization:

- **Safety:** If this attack is conducted against the C-ITS, the health of people using the system is in danger. The different impact ratings are illustrated in *Tab. 10*;
- **Operational:** If the attack reduces the operational level of the system to any degree, from a small degradation to a complete stop of operations. The different impact ratings are illustrated in *Tab. 11*;
- **Privacy:** If the attack leads to a data leak. The different impact ratings are illustrated in *Tab. 12*;
- **Financial:** If the attack leads to financial problems for system stakeholders. The different impact ratings are illustrated in *Tab. 13*.

The chosen method does not weight the relation between the different categories. However, a safety impact will often lead to a “severe” damage scenario, as the number one priority is user safety. The impact rating for the different categories is explained in the tables below. The criteria for the impact rating have been tailored to fit a C-ITS environment from well-known standards like ISO 26262 for automotive safety and ISO/SAE 21434 CS for road vehicles.

Tab. 10 Impact rating for safety damage, based on ISO/SAE 26262

Enumerate	Value	Description
Severe	2,0	S3: Life-threatening injuries (survival uncertain), fatal injuries
Major	1,5	S2: Severe and life-threatening injuries (survival probable)
Moderate	1,0	S1: Light and moderate injuries
Negligible	0,0	S0: No injuries

Tab. 11 Impact rating for operational damage, based on ISO/SAE 21434

Enumerate	Value	Description
Severe	2,0	The operational damage leads to the loss or impairment of a core vehicle function.
Major	1,5	The operational damage leads to the loss or impairment of an important vehicle function.
Moderate	1,0	The operational damage leads to partial degradation of a vehicle function.
Negligible	0,0	The operational damage leads to no impairment or non-perceivable impairment of a vehicle function.

Tab. 12 Impact rating for privacy damage, based on ISO/SAE 21434

Enumerate	Value	Description
Severe	2,0	The privacy damage leads to significant or even irreversible impact to the road user.
Major	1,5	The privacy damage leads to serious impact to the road user. The information regarding the road user is:

		a) highly sensitive and difficult to link to PII principal; or b) sensitive and easy to link to a PII principal.
Moderate	1,0	The privacy damage leads to inconvenient consequences to the road user. The information regarding the road user is: a) sensitive but difficult to link to a PII principal; or b) not sensitive but easy to link to a PII principal.
Negligible	0,0	The privacy damage leads to no effort or, negligible consequences or is irrelevant to the road user. The information regarding the road user is not sensitive and difficult to link to a PII principal.

Tab. 13 Impact rating for financial damage, based on ISO/SAE 21434

Enumerate	Value	Description
Severe	2,0	The financial damage leads to catastrophic consequences which the affected road user might not overcome.
Major	1,5	The financial damage leads to substantial consequences which the affected road user will be able to overcome.
Moderate	1,0	The financial damage leads to inconvenient consequences which the affected road user will be able to overcome with limited resources.
Negligible	0,0	The financial damage leads to no effect, negligible consequences or is irrelevant to the road user.

3.3.4 4. Attack path analysis

For this step, the experts conducting the risk assessment must adopt the attacker's point of view and find the path through the items and item components (software library, file permissions, etc.) to access to the asset. This analysis can be done using a root cause analysis.

3.3.5 5. Attack feasibility rating

The attacks evaluated in the previous step do not have the same feasibility due to variations in the architecture of the system or in the equipment needed to conduct the attack. The parameters used to normalize the feasibility rating are listed below. As shown in the tables on the following pages, each parameter has several possible values. The appropriate choice of value can be determined in consultation with cybersecurity and road experts.

- **Elapsed Time:** Time needed to perform the attack (*Tab. 14*);
- **Specialist Expertise:** Experience needed by the attacker to find the vulnerability and a path to reach it (*Tab. 15*);
- **Knowledge of the item (or component):** Define if a blueprint or technical specification of the item is publicly available, or if all information is strictly confidential, which influences the time the attacker would need to understand how the item works (*Tab. 16*);
- **Windows of opportunity:** The window of opportunity parameters summarize both time and type access conditions to the asset to perform the attack (*Tab. 17*);
- **Equipment:** This parameter is related to the tools needed by the attacker to discover and/or execute the attack (*Tab. 18*).

Tab. 14 Elapsed time as threat property, based on ISO/SAE 21434

Enumerate	Value
<= 1 day	0
<= 1 week	1
<= 1 month	4
<= 6 months	17
> 6 months	19

Tab. 15 Specialist expertise as threat property, based on ISO/SAE 21434

Enumerate	Value	Description
Layman	0	Unknowledgeable compared to experts or proficient persons, with no particular expertise.
Proficient	3	Knowledgeable in that they are familiar with the security behaviour of the product or system type.
Expert	6	Familiar with the underlying algorithms, protocols, hardware, structures, security behaviour, principles and concepts of security employed, techniques and tools for the definition of new attacks, cryptography, classical attacks for the product type, attack methods, etc. implemented in the product or system type.
Multiple experts	8	Different fields expertise are required at an expert level for distinct steps of an attack.

Tab. 16 Knowledge of the item or component as threat property, based on ISO/SAE 21434

Enumerate	Value	Description
Public information	0	
Restricted information	3	e.g. knowledge that is controlled within the developer organization and shared with other organizations under a non-disclosure agreement.
Confidential information	7	e.g. knowledge that is shared between discrete teams within the developer organization, access to which is constrained only to members of the specified teams.
Strictly confidential information	11	e.g. knowledge that is known by only a few individuals, access to which is tightly controlled on a strict needed to know basis and individual undertaking.

Tab. 17 Window of opportunity, as threat property based on ISO/SAE 21434

Enumerate	Value	Description
Unlimited	0	High availability via public/untrusted network without any time limitation. Remote access without physical presence or time limitations as well as unlimited physical access to the item or component.
Easy	1	High availability and limited access time. Remote access without physical presence to the item or component.

Moderate	4	Low availability of the item or component. Limited physical and/or logical access. Physical access to the vehicle interior or exterior without using any special tools.
Difficult	10	Very low availability of the item or component. Impractical level of access to the item or component to perform the attack.

Tab. 18 Equipment as threat property, based on ISO/SAE 21434

Enumerate	Value	Description
Standard	0	Equipment is readily available to the attacker. This equipment can be a part of the product itself, or can be readily obtained.
Specialized	4	Equipment is not readily available to the attacker but can be acquired without undue effort. This can include purchase of moderate amounts of equipment, or development of more extensive attack scripts or programs. If clearly different test benches consisting of specialized equipment are required for distinct steps of an attack, this would be rated as bespoke.
Bespoke	7	Equipment is specially produced and not readily available to the public, or the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment is very expensive.
Multiple bespoke	9	Is introduced to allow for a situation, where different types of bespoke equipment are required for distinct steps of an attack.

The attack potential corresponds to the addition of the 5 vectors. Threat definitions with examples of the values are available on the risk assessment excel sheet. The resulting attack feasibility can be mapped with the matrix on *Tab. 19*.

Tab. 19 Attack feasibility rating mapping from attack potential

Attack feasibility rating	Values
High	0-9
	10-13
Medium	14-19
Low	20-24
Very Low	≥ 25

3.3.6 6. Risk determination

The risk matrix is gleaned from the attack feasibility calculated in the Attack Feasibility Rating section. The impact of the threat is taken from the Impact Rating section.

The risk value outputted by *Tab. 20* is only an indicative value to prioritize certain risks, for example. The important step is actually conducted in the next subsection with the risk treatment decision.

Tab. 20 Classification for the attack feasibility rating

		Attack feasibility			
		Very Low	Low	Medium	High
Impact	Severe	1	3	4	5
	Major	1	2	3	4
	Moderate	1	2	2	3
	Negligible	1	1	1	1

3.3.7 7. Risk treatment decision

The final step of the risk assessment is to analyze the risk value resulting from the impact level and the attack feasibility, and to find the correct treatment of the threat. There are four use cases:





- **Avoiding the risk:** Removing the risk sources;
- **Reducing the risk:** Plans or compliance controls are in place;
- **Sharing the risk:** Sharing the risk through contract with other stakeholders or insurances;
- **Retaining the risk** or accepting the risk: In this case a rational justification must be written.

3.4 Description of analyzed scenario

3.4.1 Presentation of the scenario elements

In order to assist the working group in conducting threat analyses and risk assessments, a scenario implemented by ROSAS as part of an internal research project has been taken into consideration. This scenario is based on existing elements and allows for the execution of the seven previously defined steps. The scenario consists of a smart traffic light communicating with an intelligent car to indicate its status and location. *Tab. 21* presents different hardware elements that have been implemented.

Tab. 21 Scenario hardware elements

Name	Description	Picture
<p>Intelligent Vehicle PerceptIn</p>	<p>Connected and remotely operated vehicle used as a test vehicle. An OBU (On-Board Unit) has been installed to communicate with the infrastructure.</p>	
<p>OBU</p>	<p>The On-Board Unit (OBU), which is an embedded device in a vehicle, enables communication with other entities, such as other vehicles (V2V) or road infrastructure (V2I). This device has been integrated into the PerceptIn vehicle.</p>	
<p>RSU</p>	<p>A Road-Side Unit (RSU) is a device installed along roads or in proximity to road infrastructure, which allows for the transmission of information to vehicles through an OBU. This device has been integrated into the traffic light to transmit its status and location to the OBU integrated into the PerceptIn.</p>	
<p>Traffic Light</p>	<p>A temporary traffic light has been created in order to transmit the status of an infrastructure element to a vehicle. The different states of this traffic light are simulated using a script provided by Siemens, and the status is directly transmitted to the RSU, which broadcasts the information to the approaching vehicle.</p>	
<p>Teleoperation Control Center</p>	<p>Remote control center for a connected vehicle deployed at ROSAS. The goal is to be able to remotely drive an autonomous vehicle if it encounters an unknown situation.</p>	

3.4.2 Description of the V2I communication scenario

Only two types of messages are needed to establish the communication in the chosen scenario: SPAT for the traffic light status and MAP for the geometrical description of the corresponding intersections. These are the only message types analysed in this report.

Some RSUs and OBUs base their messages on an extension of the regular SPAT and MAP messages, resulting in the SPATEM and MAPEM types (for SPAT Extended Message and MAP Extended Message). The only difference with regular SPAT or MAP messages is their header, which includes information relative to the organization and the ITS domain. ETSI technical specifications 103 301 describe the SPATEM and MAPEM ASN1 file [15].

SPAT message

As defined in the dictionary, the SPAT message, signal phase and timing information describe the status of a traffic light. For example, signal phase and timing information can be used by the connected vehicles to determine imminent signal changes, and hence alert the driver if it appears that the vehicle will enter the intersection when such movements are not allowed. The timing of each state is not fixed due to pre-emptive and priority status functionalities. The priority status can be activated by a bus driver or an emergency vehicle to have a green lane when they are arriving to the intersection. This mechanism takes place between a traffic controller and the RSU (i.e. the traffic light). The message is continuously broadcasted by the RSU to all equipped vehicles in an area of circa 300m in normal conditions, and directly linked to the MAP message which contains the intersection's geometric information.

SPAT structure

This subsection lists the structure of a SPAT message based on the J2375 dictionary. Other definitions exist, but only this standard is listed on the specification sheet of both studied RSU/OBU. A practical analysis of a SPAT message will also be necessary to understand which optional fields are used and why. However, this is not the topic of this chapter. Here, only the mandatory fields are listed and graphically described (in *Fig. 23*).

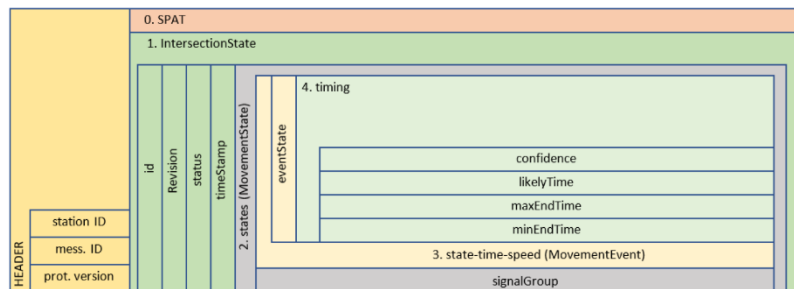


Fig. 23 Overview of a SPAT message

At the top-level, a SPAT message contains a header which describes the station emitter of the message, a unique message identifier and the protocol version of the C-ITS communication. At Level 0, there is a list of IntersectionState for each intersection linked to the RSU. For this report, the list will contain only one element. Then, for each IntersectionState, there is a second part that characterizes the intersection (id, revision, status and timestamp). The last part is the MovementStateList that describes the state and behaviour of each lane or group of lanes. It lists the current state of the traffic light, eventState and related information such as the maximal/minimal time of the current state.

Map message

The MAP message describes the base geometric information of an intersection, including roadway geometry, intersection descriptions, speed curve outlines, and roadway segment information. Thus, it is a static message, unless there is a modification of the traffic sign, in which case the OBU will only need to update a certain part of the MAP information. Finally, if a vehicle is entering the intersection for the first time, it will process the entirety of the message content. This mechanism makes use of the station ID and message ID. Like SPAT messages, a MAP message is broadcasted to all vehicles in an area of 300m of the RSU.

MAP structure

MAP messages also use optional and mandatory fields. *Fig. 24* shows only the first three levels of mandatory fields to keep the figure readable.

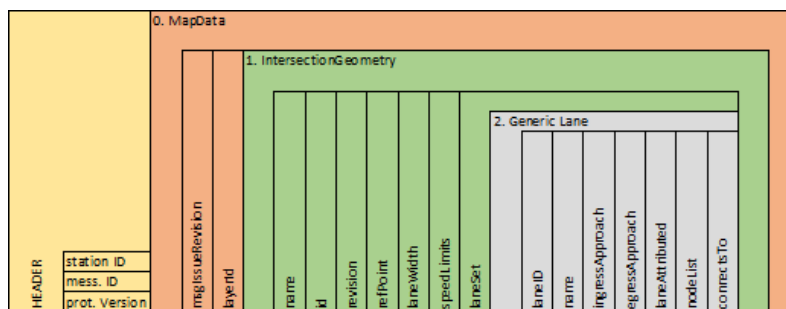


Fig. 24 Overview of a MAP message

As with SPAT messages, MAP messages include a header to identify the RSU emitter. If there is a change between the current geometric description and the old one stored on the vehicle, the message ID is also identified. The next level, represented as layer 1: IntersectionGeometry, contains a description of intersection geometry (this figure shows the case where there is only one intersection to describe). This description includes generic information like speed limits and the lane width at the intersection. After that, there is a specification for each lane (layer 2: Generic Lane), which indicates the relation between each lane and defines a path between them with a nodelist and ingress/egress approaches.

Like SPAT messages, MAP messages are continuously broadcasted at a certain frequency which depends of the speed limitation in the area. There can be multiple MAP messages broadcasted in the same area. The OBU must know which MAP message to process depending on its position.

3.4.3 Analyzed scope

Fig. 25 shows the scenario used to perform the different steps described in the previous chapter. The objective is to analyze the communication between "PerceptIn with OBU" and "Traffic light with RSU," specifically the SPATEM and MAPEM messages that are exchanged. This Proof-of-Concept is implemented at the Bluefactory site in Fribourg and allows for analysis without disrupting traffic on a public road. The implementation of this Proof-of-Concept was carried out as a research project called "SecV2IComm - Secured Vehicle-to-Infrastructure Communication [38]".

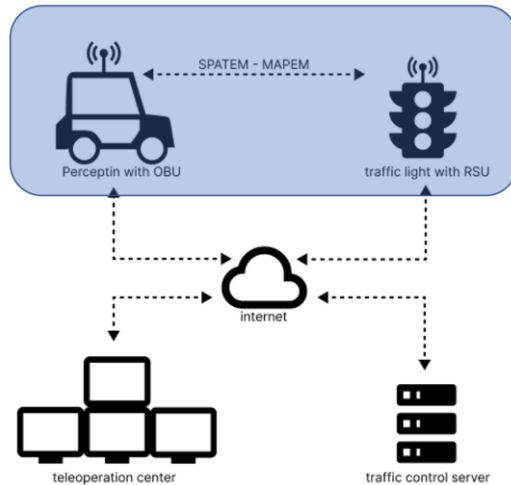


Fig. 25 Scenario used for cyberthreat analyses

3.5 Threat Modelling tools

3.5.1 Tool comparison

There is a plethora of threat modelling tools, the best known of which are compared in *Tab. 22* of the present document. Research was done around June 2022 with the most up-to-date software at that date. This evaluation is thus subject to change as new versions are released.

- **Microsoft Threat Modelling Tool** is a desktop-based tool that works solely on Windows. It is one of the most mature solutions available;
- **OWASP Threat Dragon** is a tool that has both a web-based and desktop-based platform. Their official website states that it has a powerful rule engine;
- **MyAppSecurity's ThreatModeler** is a web-based platform which uses draw.io for its diagrams. Their official website states that it has an API access;
- **IriuRisk** is also a web-based platform which uses draw.io for its diagrams. The CE (Community Edition) allows for only one project, and their EE (Enterprise Edition) has an API access;
- **Cairis** is a web-based platform that has extensive features, but a heavy and time-consuming development process;
- **Threagile** is a code-based modelling tool, and its input is in YAML format. It is an unusual approach that has some benefits, such as a great integration with Agile development;
- **Kenna. VM** uses data science to highlight sensitive vulnerabilities. It is part of Cisco;
- **SecuriCAD** by Foreseeti is a desktop-based tool that creates attack simulations. It has 3 different editions, Community, Professional, and Enterprise. The Community Edition is free to use;
- **SD Elements** by Security Compass is a web-based tool which collects information based on surveys. Only paid versions are available;
- **Trike Octotrike** is an open-source methodology and threat modelling tool, which is to be used as a spreadsheet (the other being a standalone desktop tool). It is in pre-alpha version, and was last updated in 2019 on GitHub;
- **Tutamantic** is a SaaS product aiming at fast prototyping. It is simple and free to use in Beta.

Tab. 22 Threat modelling tool comparison

Note: Information collected in June 2022

	Customization	Threat Generation	Handling Threats	Report generation	UX	Threat generation quality / exhaust.	Future perspective / community	Additional
								<ul style="list-style-type: none"> • Methodologies [M] • Price [P] • Remarks [R]
Microsoft Threat Modelling Tool	X	X	X	X	7	7	4	[M] STRIDE [P] Open-source [R] Possibility to create new components, threats, in custom templates. Successor of Microsoft Secure Development Lifecycle (SDL).
OWASP Threat Dragon [33]	-	-	X	X	5	NA	5	[M] STRIDE, CIA, LINDDUN [P] Open-source [R] DFD modelling. Decent for free solution, but lacks features. It explicitly says it has a rule engine to auto-generate threats, but where ?
MyAppSecurity's ThreatModeler	X	X	X	X	4	8	?	[M] STRIDE, VAST, Octave, PASTA, Trike [P] Paid [R] Threat Research Center keeps up to date. Community edition too limited.
IriusRisk (CE)	X*	X	X	X	4	7	3	[M] [P] Community Edition is free [R] Community edition is tested (limited to one model). Draw.io used for modelling *Documentation says so, couldn't reproduce.
Threagile	X	X	X	X	NA	6	5	[M] [P] Open-source [R] Code-modelling, 357 stars in GitHub.
Cairis	?	?	?	X	4	?	3	[M] [P] Open-source [R] DFD modelling. Concept is very interesting, and comes from research, but very complex to put in place (personas, rebuttals, etc.) CAIRIS: a tutorial introduction (Part 1): https://www.youtube.com/watch?v=-MVghCz48B4 98 stars GitHub

Some threat modelling tools were considered, but finally not tested. Some of these notes are presented in *Tab. 23*.

Tab. 23 *Untested threat modelling tools*

Note : Information collected in June 2022

Name	[M]ethodologies / [P]rice / [R]emarks
SecuriCAD	[M] [P] 479\$/month [R] Software from foreseeti.
SD Elements by Security Compass	[M] [P] Paid (unknown \$\$\$) [R]
Trike Octotrike	[M] [P] Open-source [R] White paper is in draft since 2005, last update on GitHub in 2019. [34]
Tutamantic	[M] [P] Beta is free to use (until launch) [R]

3.5.2 Tool selection

The decision for the tool choice is based on the results presented in *Tab. 22*. The most decisive criteria are:

- The generation of threats is a mandatory requirement;
- The UX, or user experience, has to be simple and intuitive enough, and should not require extensive training;
- The tool should support C-ITS system modelling.

Based on these criteria, the tools can be narrowed down to three main contenders:

- Threat Modeler;
- IriusRisk (CE);
- Microsoft Threat Modelling Tool.

Threat Modeler has a promising and proactive manner of keeping threats up to date through its Threat Research Center. However, the Community Edition is very limited, and thus gives little confidence about its usability for the specificities of the project (C-ITS).

IriusRisk is an interesting solution. However, key features mentioned in the documentation could not be produced as intended, and the UX is rather complicated compared to the alternatives.

Microsoft Threat Modelling Tool fulfills all the requirements. It offers a lot of freedom when it comes to building new templates, and the UX is quite intuitive. The fact that our team already has some experience with this tool further confirmed that it is the right tool for the job.

3.5.3 Microsoft Threat Modelling Tool

Microsoft Threat Modelling Tool is a free-to-download TMT developed by Microsoft as part of their Security Development Lifecycle (SDL). It is IT-based and uses DFD representation for the models. Microsoft documentation states that the tool enables anyone to:

- Communicate about the security design of their systems;
- Analyse those designs for potential security issues;
- Suggest and manage mitigations for these issues.

Microsoft documentation also states a few capabilities and innovations of their tool, namely:

- Automation: Guidance and feedback in drawing a model;
- STRIDE per Element: Guided analysis of threats and mitigations;
- Reporting: Security activities and testing in the verification phase;
- Unique Methodology: Enables users to better visualize and understand threats;
- Designed for Developers and Centered on Software: *“many approaches are centered on assets or attackers. We are centered on software. We build on activities that all software developers and architects are familiar with -- such as drawing pictures for their software architecture”*;
- Focused on Design Analysis: The term "threat modelling" can refer to either a requirement or a design analysis technique. Sometimes, it refers to a complex blend of the two. The Microsoft SDL approach to threat modelling is a focused design analysis technique.

Threat models are DFDs composed of stencils, which are the basic elements of a model (processes, interactors, trust boundaries, etc.). Some stencils from the default template are shown in *Fig. 26*, and an example of a basic model with those default stencils is presented in *Fig. 27*. It shows an interaction between a human and a web server, which in turn communicates with a database. This kind of IT infrastructure represents the main type of models to be built with the default template of MTMT.

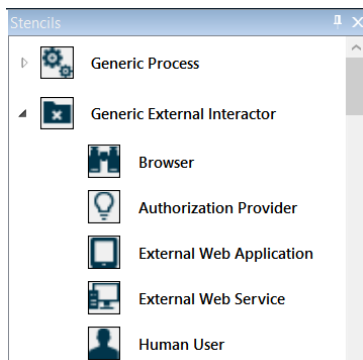


Fig. 26 Example of stencils, from the default template

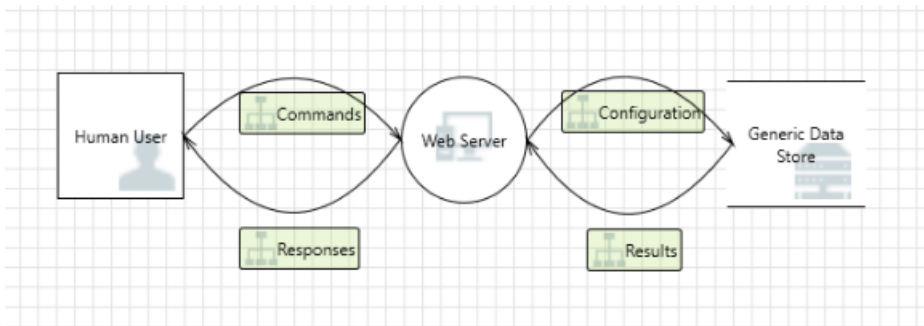


Fig. 27 Example of a threat model using the default template

One of the greatest features in MTMT is the ability to create and/or adapt templates to great extents. It is thus possible to add whole new domains, going from chemistry processes to autonomous vehicles.

4 Approach and results of threat modelling and risk assessment

4.1 Introduction

This chapter will focus on the comparison between a risk assessment based on the 7 steps described in section 3.3 (hereafter “human-based approach”), and a risk assessment supported by the “Microsoft Threat modeler” tool. The first two sections will specify how to conduct the risk assessments and the last two will focus on the comparative results.

The system under consideration for this risk assessment is the scenario described in section 3.4, an automated vehicle and a connected traffic light that emits i2v messages (traffic light status and traffic light localization).

4.2 Human-based approach

4.2.1 Introduction

This approach will follow the 7 steps described in section 3.3. The first part focuses on a small benchmark to choose the best implementation methodology. The risk assessment will be conducted on the basis of this benchmark.

4.2.2 Risk assessment implementation

The objective of this section is to implement a risk assessment methodology in the real use-case of an intersection using C-ITS to manage the traffic light state and a highly automated vehicle. To implement it, there are two solutions: using specialized software or developing an excel-based template.

Specialized software

Different consulting companies in the automotive world develop software that simplifies risk assessment with the TARA methodology by providing a user-friendly interface and quick guidelines on pre-defined threats for the automotive sector. An example of this software is CycurRISK, a new program developed by Escript, a consulting company specialized in automotive cybersecurity.

Excel-based solution

The Excel-based solution is a lightweight approach to dealing with risk assessment and does not require any fee or software license with other companies. Thus, it has the advantage of being easily updated and maintained. Moreover, thanks to its experience in automotive cybersecurity, CertX already has a proven and functional risk assessment template based on the TARA methodology.

Methods summary

Although the chosen risk assessment methodology applies TARA to road vehicle cybersecurity, there is a difference in use cases, as a C-ITS is not only onboard (i.e. on the vehicle) but also in the infrastructure. Thus, a specific program like CycurRISK could lead to a loss of completeness for threats on the infrastructure side.

Excel template

The Excel template summarizes all risk assessment steps explained in this section and does the calculation of the attack feasibility automatically. It also includes a second Excel

sheet with the data flow diagram and a third sheet with the different possible values. The main excel sheet is the TARA sheet, which can be split in four main categories:

- Item definition and threat analysis;
- Impact rating;
- Attack path and attack feasibility;
- Risk determination and risk treatment decision.

Item definition and threat analysis:

This part contains both the asset identification and its corresponding cybersecurity-relevant parameter. Then, based on that, the potential damage scenario is explained. Finally, a threat scenario based on the STRIDE methodology is described. An example is shown in Fig. 28.

0. Item traceability			1. Asset identification						2. Threat scenario identification			
Function id	Function description	SUC?	Component / Message	Asset	Cybersecurity			Damage scenario	Safety relevance?	Threat scenario id	STRIDE vector	Threat scenario description
					Confidentiality	Integrity	Availability					
Func1	Communication between RSU->OBU	X	Message from RSU to OBU	SPATEM message	X		ds.1	The vehicle does not stop on the traffic light due to an incorrect SPATEM message	X	ts101	Tampering	Tampering / modification of a SPATEM message between the RSU and OBU it leads to the loss of integrity in the data communication. This can lead to an incident due to a wrong message being sent, the vehicle will not know that the light is red

Fig. 28 Example item definition and threat analysis

Impact rating:

Based on the threat scenario, the impact rating can be calculated from the different impact categories (financial, operational, privacy and safety). An example is shown in Fig. 29.

3. Impact rating					
Impact				Worst impact - Description [+rationale if controllability used]	Highest Impact
Financial	Operational	Privacy	Safety		
Moderate	Major	Negligible	Severe	Command modification leading to a crash with humans	Severe

Fig. 29 Example impact rating

Attack path and attack feasibility:

This category is made of two different steps of the risk assessment: the attack path, and the resulting attack feasibility. From the “attack potential-based feasibility” values a total is outputted that gives the aggregated and total feasibility. An example is shown in Fig. 30.

4. Attack path analysis		5. Attack feasibility rating (alternatives to be chosen between A, B or C)						
Attack path id	Attack path	A. Attack potential-based feasibility					Aggregated and total feasibility	
		Elapsed time	Expertise	Knowledge	Window of opportunity	Equipment required		TOTAL
ap210101	- Reverse Eng. Practices on com' - Credential retrieving - Forging new packets using trusted credentials	< 1 week	Expert	Restricted	Unlimited	Bespoke	16	Medium

Fig. 30 Example attack path and attack feasibility

Risk determination and risk treatment decision:

From steps 3 to 5 a risk is automatically determined. An adequate risk treatment must then be chosen to secure the item under the risk assessment. An example is shown in Fig. 31.

6. Risk determination [Symmetric matrix]			7. Risk treatment decisions				
Risk criteria		Risk value [0-5]	Risk treatment options	Cybersecurity goals		Cybersecurity claims	
Impact	Feasibility			goal id	goal description	claim id	claim description
Severe	Medium	4	Reduce the risk	CSG1	- An attacker shall not be able to spoof any communication sent by the operation center to the vehicles - the system (both ends) shall not trust any packet replayed		

Fig. 31 Example risk determination and risk treatment decision

4.3 Tool-based approach

4.3.1 Introduction

The software used for the tool-based approach is MTMT. Section 4.3.2 introduces the C-ITS template, and how the tool programmatically generates threats. Section 4.3.3 presents the methodology pipeline, from the threat model in MTMT to the resulting Excel table.

4.3.2 C-ITS template

A template was created specifically for the purpose of this project; it was derived from the standard template for TMT models. C-ITS elements and relevant means of communication were thus added to the template.

Stencils

C-ITS-related stencils were created in a way that increases re-usability for other potential models. As shown in Fig. 32, the stencils can be derived from a few generic components, namely generic RSU, OBU, Data flows, and Ethernet.

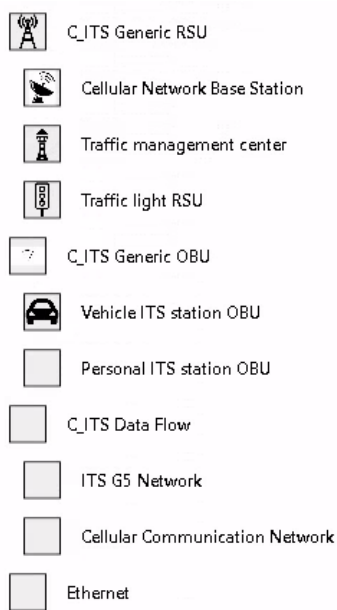


Fig. 32 Overview of customised stencils for C-ITS

Threats

In MTM, threats are categorised into STRIDE categories, namely Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of Privilege. This was kept, as well as standard threats, and built upon. Here is a list of the threats that were added for this template; each of these has additional properties that are defined in the next section.

Spoofing:

- Impersonation attack;
- GPS Spoofing;
- Masquerading.

Tampering:

- Collision attacks;
- Illusion attack;
- Bogus information attack;
- Alteration/Replay attacks;
- RSU replication attack;
- Downgrade attack.

Information disclosure:

- Location tracking;
- Eavesdropping attacks.

Denial of Service:

- Denial of Service;
- Sybil attack;
- Timing attack;
- Malware on OBU;
- Malware on RSU;
- Spamming;

- Misconfiguration;
- Black Hole;
- Radio Jamming Attack.

Elevation of Privilege:

- Elevation of Privilege;
- Weakness in SSO Authorisation.

Threat generation expression

Note: No official information was found concerning this threat generation expression language. All information gathered here is derived from existing threat expressions.

One of the strengths of MTMT is to be able to generate a list of vulnerabilities and threats of the system being modelled. This feat is accomplished using a language for such expressions. For each threat, both an include and an exclude property can be set up with a generation expression; as their names suggest, the include property is a statement that will include the threat if true; the exclude property can omit a threat even if the include statement is true.

Expressions are built as logic statements, meaning they can be used as “bricks” for longer expressions. Logic operators, namely *AND* and *OR*, can be used to build expressions. Parentheses are also part of the language grammar. For example:

(<statement A> and <statement B>) or <statement C>

Is a valid *expression*.

Atomic expressions can be built using a few keywords as described below. Expressions allow the specification of a “type” of stencil for both sources and/or targets using the keyword *is*. Here, *<stencil>* is to be replaced by the stencil’s full name.

source is [<stencil>]

target is [<stencil>]

Expressions can also focus on flows, or interactions, by using the keyword *flow*.

flow crosses [<stencil>]

Finally, expressions can make use of a property by using its name *<property>* as well as its value *<property.value.string>*. Note that the property value is in a string format, meaning that (simple) quotation marks are expected.

flow.[<property>] is <property.value.string>

As a last example, the included threat generation expression of the threat Cross Site Request Forgery is presented. Although long, the expression is not very complex, once the keyword and the logic are understood.

*# (source is [Generic Process] or source is [Generic External Interactor]) and (target is [Generic Process])
and
(flow.[Source Authenticated] is 'Not Selected' or flow.[Source Authenticated] is 'Yes')
and
(flow.[Forgery Protection] is 'None' or flow.[Forgery Protection] is 'Not Selected')
and
(flow crosses [Generic Trust Line Boundary] or flow crosses [Generic Trust Border Boundary])*

Excel template

An Excel template, annex II.1, was created in order to automate the calculation of feasibility, impact ratings, and other values. The input (resulting threats) to be copied from the analysis view of MTMT— is to be pasted in the first tab of the Excel file, as shown in *Fig. 33*.

This automation was made possible by using custom Excel commands and some functions written in Visual Basic.

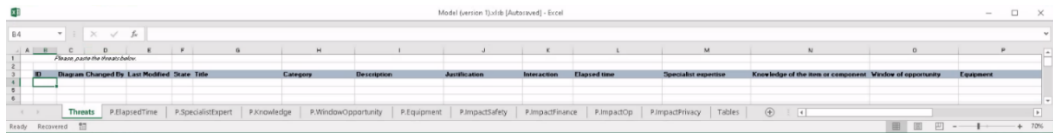


Fig. 33 Excel template for C-ITS as empty canvas

In *Fig. 34*, the functions written in Visual Basic are visible. Note that it is possible to modify them, for example if the risk value function is different. It should be noted that it is possible to avoid using Visual Basic and to enter these formulas directly into the Excel formula; however, doing so makes them much harder to read and understand.

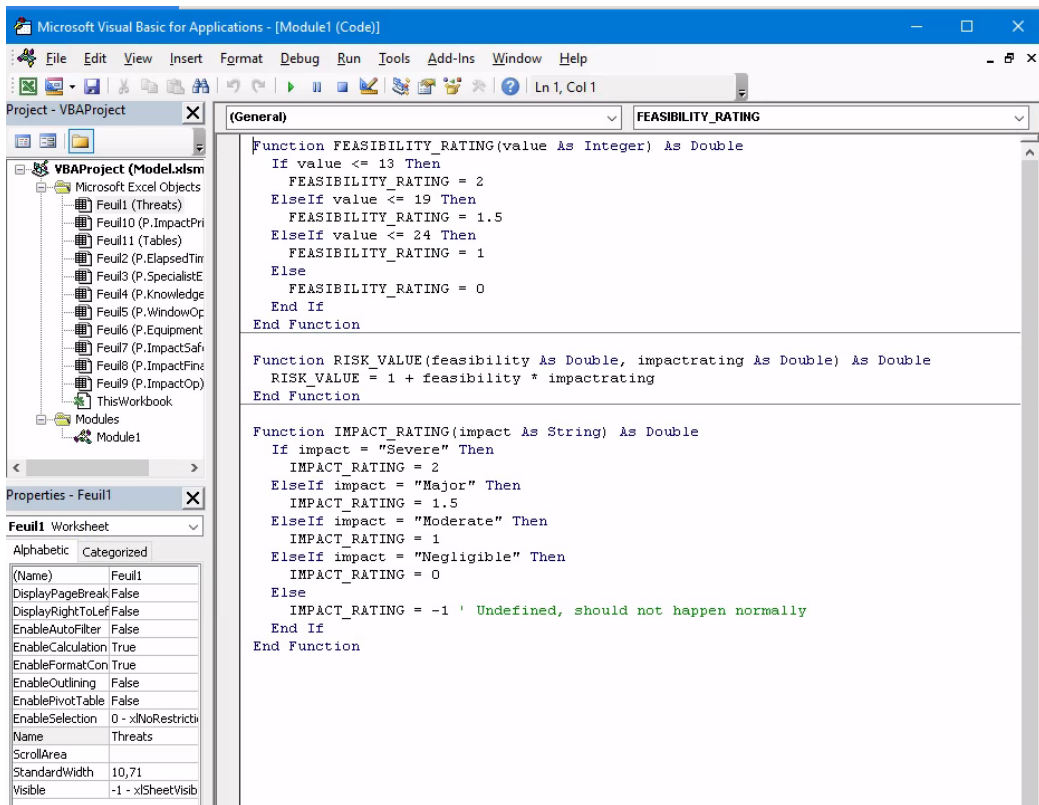


Fig. 34 Visual Basic functions for C-ITS template calculations

4.3.3 TMT Usage

Building a threat model with MTMT requires a template (a standard one can be used) and a component to be modelled (e.g., an infrastructure, a scenario, etc.). This is enough to use the tool and generate potential security threats for the component in question.

This project's methodology goes even further and exports the resulting threats to an Excel file using a predefined template to generate TARA-like tables. An overview of the threat modelling methodology, shown in *Fig. 35*, describes how tools interact with each other and where templates are being used.

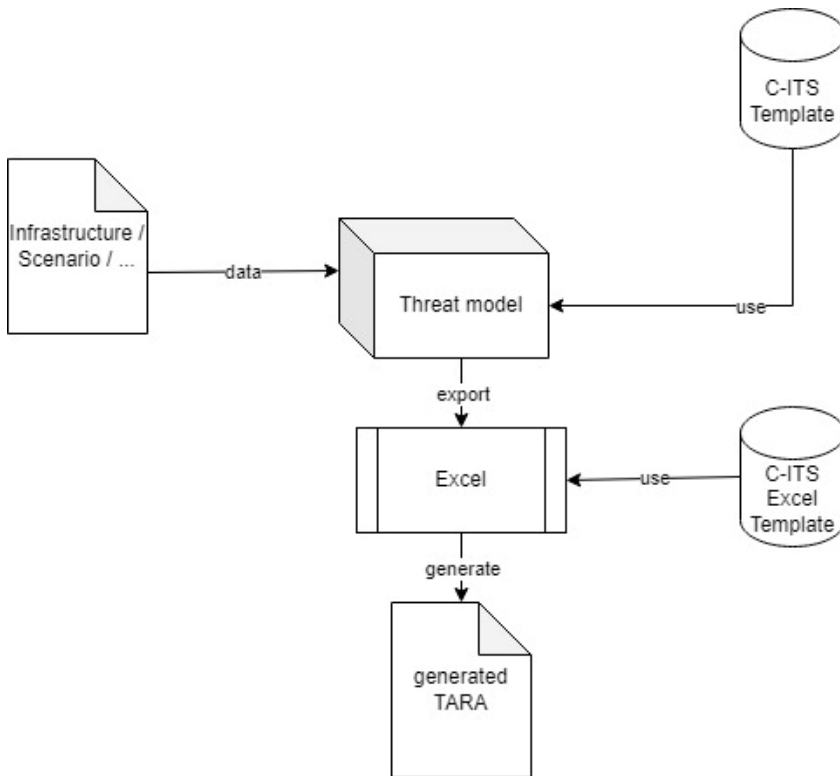


Fig. 35 Overview of the threat modelling methodology

TMT Model

The TMT model is to be implemented as intended by the program; the only difference is in the stencils used (as shown in the Stencils section). Refer to the official MTMT documentation for help on this matter.

Export to Excel

Exporting threats to Excel can be performed by using the Excel template shown above. For copying the threats to export, switch to “Analysis view” as shown in Fig. 36.

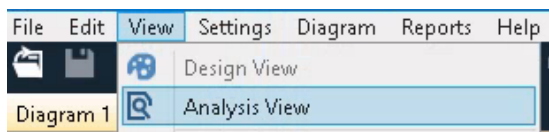


Fig. 36 Switching MTM to Analysis view

The next step is to select all the threats to export. to do so, press Ctrl+A in the “Threat List” panel. Then, right click on the selected threats, and select “Copy Custom Threat Table”, as in Fig. 37.

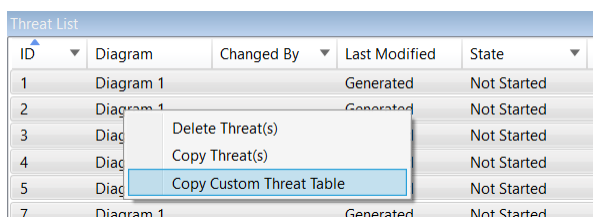


Fig. 37 Copying threat(s) to the clipboard

The following formatting is used for the Excel file that we are going to export to:

ID=\$(ID);Diagram=\$(Diagram);Changed By=\$(Changed By);Last Modified=Generated;State=\$(State);Title=\$(Threat);Category=\$(Category);Description=\$(Description);Justification=\$(Justification);Interaction=\$(Interaction);Elapsed time=\$(Elapsed time);Specialist expertise=\$(Specialist expertise);Knowledge of the item or component=\$(Knowledge of the item or component);Window of opportunity=\$(Window of opportunity);Equipment=\$(Equipment);Impact rating for safety damage=\$(Impact rating for safety damage);Impact rating for financial damage=\$(Impact rating for financial damage);Impact rating for operational damage=\$(Impact rating for operational damage);Impact rating for privacy damage=\$(Impact rating for privacy damage);

The final step is in the Excel file. Simply paste the previously copied content in the first cell (B4) of the “Threats” tab, as shown in Fig. 38 below.

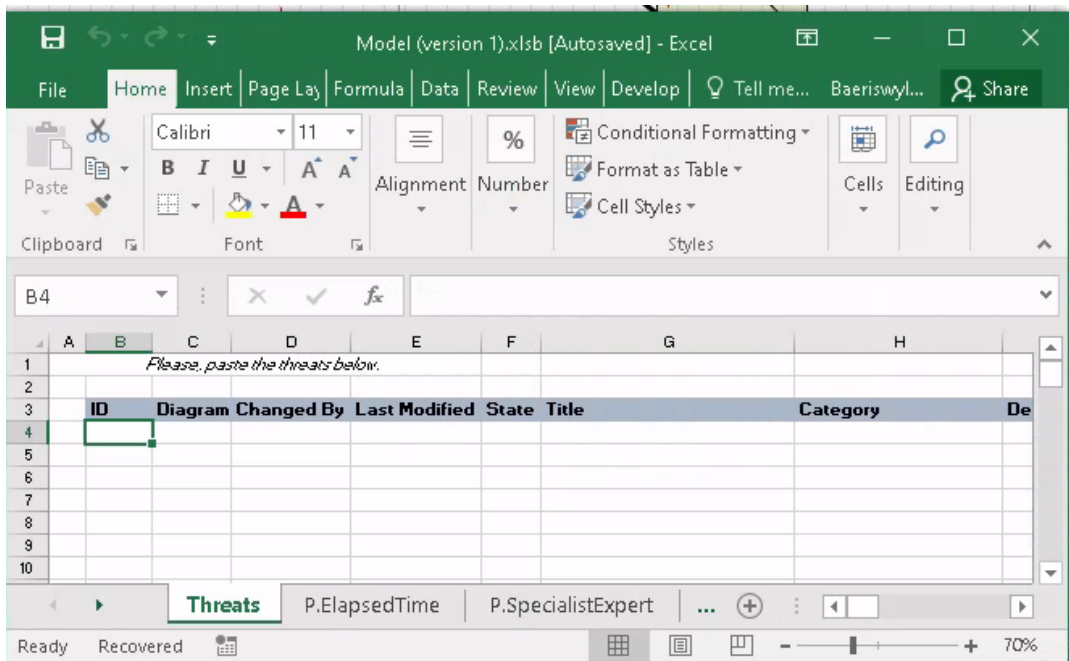
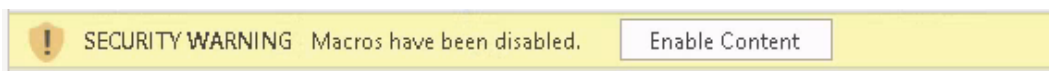


Fig. 38 Setup for pasting data to Excel template

Remark: Please note that macros need to be enabled for the automatic calculation to work.



If everything went well, you should now see that the threats are copied in the Excel sheet, and the automatic field should be filled accordingly. A screenshot in Fig. 39 shows what the fields should look like.

	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI
Impact rating for privacy damage	ET	SE	K	WoO	Eq	Feasibility	Safety Impact	Financial Impact	Operational Impa	Privacy Impact	Safety Risk	Financial Risk	Operational Ris	Privacy Risk		
Major	0	3	0	0	4	7	1	1	1,5	1,5	8	8	11,5	11,5		
Severe	0	0	0	0	0	0	2	2	2	2	2	1	1	1	1	1
Severe	0	0	0	0	0	0	2	2	2	2	2	1	1	1	1	1
Severe	19	6	0	0	7	32	1,5	2	2	2	49	65	65	65	65	65
Severe	0	0	0	0	0	0	2	2	2	2	2	1	1	1	1	1
Severe	0	0	0	0	0	0	2	2	2	2	2	1	1	1	1	1
Negligible	0	0	0	0	0	0	1	1	1,5	0	1	1	1	1	1	1
Major	0	3	0	0	4	7	1	1	1,5	1,5	8	8	11,5	11,5		
Severe	19	6	0	0	7	32	2	2	2	2	65	65	65	65	65	65
Negligible	1	6	0	4	4	15	2	1,5	2	0	31	23,5	31	31	1	1
Negligible	1	6	3	0	7	17	2	1,5	2	0	35	26,5	35	35	1	1
Negligible	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1
Negligible	4	3	0	1	0	8	0	0	1	0	1	1	9	1	1	1

Fig. 39 Screenshot of automatic fields filled when pasting input data

4.4 Human-based results

A preliminary risk assessment based on the tailored methodology is available in annex II.2. This section will focus on how to follow this methodology for a specific threat.

Focus on a specific threat

The studied scenario represents a highly automated vehicle at an intersection controlled by a traffic light. Both the infrastructure and the vehicle are equipped with C-ITS that communicates with SPATEM and MAPEM messages to describe the position and the traffic-light state. This infrastructure is represented in *Fig. 40* below.

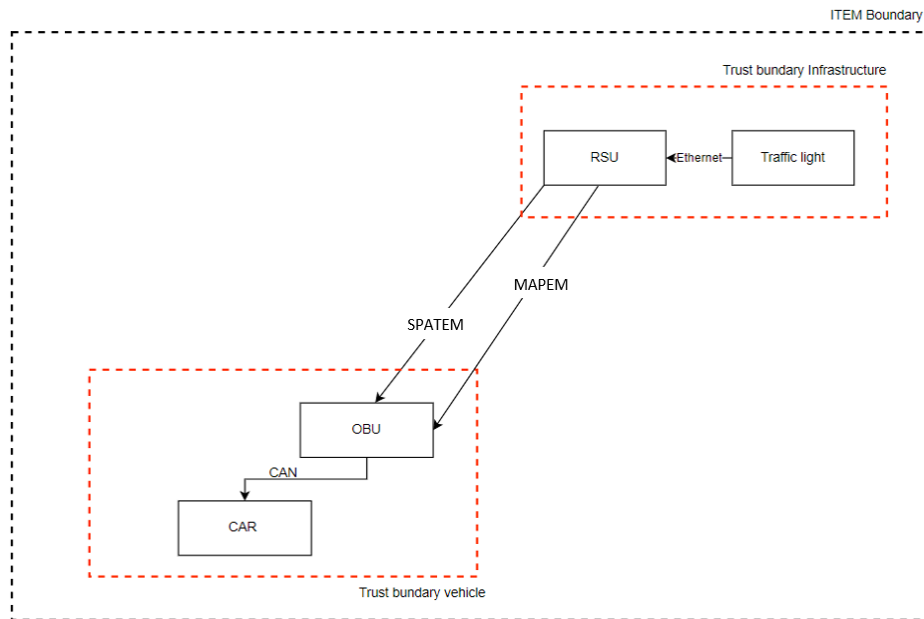


Fig. 40 Dataflow diagram system under consideration

4.4.1 1. Asset definition

The first step is to identify the asset. This is done by analyzing the data flow diagram, *Fig. 40*. This diagram shows the communication between the RSU and the OBU which needs to be protected against external attack. Thus, the **SPATEM message** is the first analyzed asset. The focus is on its integrity because it could lead to a potential incident like: “The vehicle does not stop at the traffic light due to an incorrect SPATEM message”.

4.4.2 2. Threat scenario identification

Based on the asset identification, a potential threat is derived using STRIDE methodology. The threat could come from the **spoofing** of a SPATEM message between the RSU and OBU, leading to loss of integrity in the data communication and thus also to an incident due to the wrong message being sent (the vehicle will not know that the light is red).

4.4.3 3. Impact Rating

The impact rating is divided in four categories: Financial, Operational, Privacy and Safety. Each is evaluated to one of four levels: negligible, moderate, major and severe. The outcome for this specific threat is:

- **Financial: Moderate:** The issue only leads to inconvenient consequences which the stakeholder will be able to overcome with limited resources, such as reputation damage;
- **Operational: Severe:** The issue leads to a wrong message being sent;
- **Safety: Severe:** There are potentially fatal injuries in a car accident;
- **Privacy: Negligeable:** The issue leads to no privacy effect.

The worst impact is a crash involving human safety. Thus, the **highest impact is severe**.

4.4.4 4. Attack path analysis

The attack path from a high-level perspective can be done in two steps:

- **Sniffing communication:** The attacker sniffs the communication to analyze the message structure;
- **Forging new packets:** Based on the analyzed message, new messages are broadcasted with a new modified traffic-light state.

4.4.5 5. Attack feasibility rating

The feasibility of the attack path analyzed above is rated based on five different vectors:

- **Elapsed time: < 1 month:** The attacker will need less than one month to conduct the attack;
- **Expertise: Expert:** An expert knowledge of communication technologies is required to conduct this attack;
- **Knowledge: Public:** There is no required restricted knowledge of the system under consideration. Public knowledge developed on the C-ITS standards to understand ITS-G5 communication is enough;
- **Equipment required: Specialized:** The attacker will only need to acquire a specific modem to analyze the ITS-G5 communication.

The **aggregation** of these five vectors outputs a **medium feasibility**.

4.4.6 6. Risk determination

The combination of the impact rating and attack feasibility gives a **risk value of 4 out of 5**.

4.4.7 7. Risk treatment decision

The **risk will be reduced** by adding a specific **cybersecurity goal**: SPATEM messages shall be authenticated.

4.4.8 Human-based summary

Summary

Risks coming from spoofing, repudiation, denial of service and elevation of privilege have been found during the risk assessment. The risk origin can be split into three main categories: communication based on communication technology, the RSU configuration, and finally the logging of the RSU.

All risks with a level higher than 1 can be reduced through cyber security mechanisms such as message authentication and message freshness or by controlling and segmenting the network so that only certain devices can connect to the RSU network. Only the risk with a level of one has been accepted due to a very low feasibility rating in view of the required time and equipment to conduct the attack.

Conclusion

The human-based approach identified the specific needs of a C-ITS environment as part of a risk analysis, mainly to be able to stay on a high level regarding the equipment used while also focusing on the type of messages sent and the communication channel. Based on these requirements, the risk assessment methodology used for road vehicles has been tailored to integrate specific needs while remaining understandable for the automotive world that might work on it. This approach was chosen to facilitate the integration of automotive stakeholders and other more mature cybersecurity stakeholders that also use similar methodologies.

The preliminary risk analysis showed that the tailored methodology works well for C-ITS environments but required a complete team of mobility and cybersecurity experts to cover all the possible threat sources. This can be a disadvantage due to the number of people required with specific expertise to conduct every C-ITS risk assessment. On the other hand, the diversity of profiles generates opinions that mobility or security experts would perhaps not otherwise consider.

4.5 Tool-based results

This section will present the results of a risk assessment with the tool-based approach described in section 4.3 as applied to the scenario described in section 3.4. The scenario represents a highly automated vehicle at an intersection controlled by a traffic light. Both the infrastructure and the vehicle are equipped with C-ITS that communicates with SPATEM and MAPEM messages to describe the position and the traffic-light state.

These results are the direct output of the Microsoft tool and the automatic calculation made on the Excel sheet, without any intervention on the part of the cybersecurity expert.

4.5.1 1. Asset definition

The asset definition is directly performed inside the C-ITS template. Thus, the only action to perform is the description of the scenario using the stencils available in the template. Elements of the scenario correspond to the implemented stencil, as illustrated in Fig. 41.

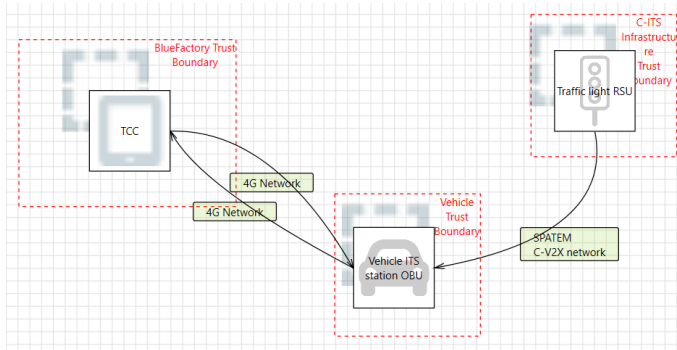


Fig. 41 Overview of realistic scenario

4.5.2 2. Threat scenario identification

Multiple threat scenarios are generated by the model (listed in Tab. 24). However, only the threat closest to the one analyzed in the human-based approach is presented here, in a similar way to 4.4.2.

Masquerading is categorised as a spoofing attack. The following description is attached to it:

“By posing as legitimate nodes in the vehicular network, outsiders can proceed to conduct more types of attacks than they otherwise could, for example forming black holes or fabricating false messages. However, given how easy it is to become part of the network by simply joining it with a working OBU, the masquerading exercise for an outsider becomes analogous to breaking a window to get into a house when the front door is wide open. There is, however, much to be gained by a rogue insider masquerading as another OBU or a RSU. By assuming a false identity, an attacker can create mischief with impunity, such as injecting false messages into the network and deceiving authorities into believing that another node was responsible. With PSOBUs possessing special privileges within the network, and RSUs providing wireline access and LBS information, spoofing such nodes can be the first step in accessing personal user information and possibly compromising privacy. However, because OBUs and RSUs can be identified by their certificate which can be distributed in Certificate Revocation Lists (CRLs) if a node turns rogue, such a deception would be difficult to successfully carry out. With the strong technical difficulty in conducting this attack, despite its high impact on the user and the network due to compromised integrity, the threat is ranked as minor.”

Tab. 24 Description of generated threats

Title	Category	Description
External Entity TCC Potentially Denies Receiving Data	Repudiation	TCC claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Data Flow 4G Communication Network Is Potentially Interrupted	Denial Of Service	An external agent interrupts data flowing across a trust boundary in either direction.
Malware	Denial Of Service	The introduction of malware, such as viruses or worms, into the vehicular network has the potential to cause serious disruptions to its operation. Since the OBUs and RSUs are expected to receive periodic software and firmware updates, this threat is more likely to

		be carried out by a rogue insider than by an outsider. The associated motivation is ranked as moderate because it consists of a disruption in service. Since the threat is theoretically possible, the technical difficulty is a solvable one if countermeasures are not in place. The impact on the user is considered high due to the resulting long-lasting outages.
Misconfiguration	Denial Of Service	Threat faced by WAVE service advertisement (WSA): As with Country String, the potential that the location could be used not simply as information about the Provider but to reconfigure the User introduces a vulnerability. A user that does not know its own location, but that has a map of the geographic regions that different Country Strings apply to, might set its active locale to the Country String indicated by the 2D Location. This is a high threat for devices of this type as this could lead to them having an incorrect channel mapping and being locked out of the system. Note that this attack can be mounted without the attacker even having to generate a WSA: they can obtain a WSA generated by a valid Provider in one location, and forward it to a different location. This wormhole attack will work even if the WSA is signed. Because the result could be for a device to be locked out of the system, we classify attacks based on a false 2D Location as having potentially HIGH impact.
Data Flow SPATEM Network Is Potentially Interrupted	Denial Of Service	An external agent interrupts data flowing across a trust boundary in either direction.
Spamming	Denial Of Service	There is a risk of increased transmission latency due to the presence of spamming messages. The motivation for marketers to acquire a RSU or an OVHI-enabled OBU for this purpose is best rated as moderate. On one hand, it is likely to be very lucrative, but on the other hand, the business is ultimately accountable to its customers who typically resent such a waste of their time and bandwidth. With the technical difficulty rated as low since the marketer is an insider, and with the impact on the user also low because it represents little more than an annoyance, the threat is ranked as minor.
Malware on RSU	Denial Of Service	The introduction of malware, such as viruses or worms, into the vehicular network has the potential to cause serious disruptions to its operation. Since the OBUs and RSUs are expected to receive periodic software and firmware updates, this threat is more likely to be carried out by a rogue insider than by an outsider. The associated motivation is ranked as moderate because it consists of a disruption in service. Since the threat is theoretically possible, the technical difficulty is a solvable one if countermeasures are not in place. The impact on the user is considered high due to the resulting long-lasting outages.
Black Hole	Denial Of Service	A black hole is formed by nodes which fail to propagate messages. Such an attack can only be carried out by rogue insiders, since network outsiders are not expected to repeat messages. The consequences of having a black hole in the network include dropped traffic messages, service requests and replies. With sufficient numbers of rogue nodes colluding to form a black hole past which no messages are propagated, it may be possible for attackers to partition the vehicular network in such a way that legitimate nodes never receive messages. If this scenario succeeds, nodes may be prevented from receiving critical updates to their root certificate lists and CRLs, leaving them vulnerable to masquerading attacks from nodes using expired, revoked or falsified certificates. With significant gains to be made from this attack, its technical difficulty solvable and its tremendous impact on the security of the network, the threat is ranked as critical.
GPS Spoofing	Spoofing	By using a GPS satellite simulator to generate radio signals stronger than those received from the genuine GPS satellite, an attacker can lead nodes to believe they are in a different location than they actually are [13], potentially causing collisions. Also, if GPS time is used to timestamp messages, a spoofing of the GPS clock could result in nodes accepting expired messages as new ones and could thus lead to a successful replay attack. Given the potential gains for an attacker, the solvable technical difficulties involved in this type of attack and its high impact on the network and the users, the threat is ranked as critical.
Masquerading	Spoofing	By posing as legitimate nodes in the vehicular network, outsiders can proceed to conduct more types of attacks than they otherwise

		could, for example forming black holes or fabricating false messages. However, given how easy it is to become part of the network by simply joining it with a working OBU, the masquerading exercise for an outsider becomes analogous to breaking a window to get into a house when the front door is wide open. There is, however, much to be gained by a rogue insider masquerading as another OBU or a RSU. By assuming a false identity, an attacker can create mischief with impunity, such as injecting false messages into the network and deceiving authorities into believing that another node was responsible. With OBUs possessing special privileges within the network, and RSUs providing wireline access and LBS information, spoofing such nodes can be the first step in accessing personal user information and possibly compromising privacy. However, because OBUs and RSUs can be identified by their certificate which can be distributed in Certificate Revocation Lists (CRLs) if a node turns rogue, such a deception would be difficult to successfully carry out. With the strong technical difficulty in conducting this attack, despite its high impact on the user and the network due to compromised integrity, the threat is ranked as minor.
Downgrade attack	Tampering	Using a rogue base station broadcasting at a high-power level, an attacker can force a user to downgrade to either GSM or UMTS. As of the time of this writing, there are no significant, publicly known weaknesses in the cryptographic algorithms used to protect the confidentiality and integrity of the UMTS air interface. Unfortunately, significant weaknesses exist for the 2G GSM cryptographic algorithms used to protect the confidentiality and integrity of the air interface. Examples of broken 2G cryptographic algorithms are A5/1 and A5/2 [15]. Depending on the algorithm negotiated while attaching to the rogue base station, the air interface cryptographic algorithms chosen to protect the air interface may be cryptographically broken, leading to a loss of call and data confidentiality. While GSM is out of scope for this document, real world deployments utilize GSM networks to connect with LTE networks, which bring this into scope.
Radio Jamming Attack	Denial Of Service	Jamming attacks are a method of interrupting access to cellular networks by exploiting the radio frequency channel being used to transmit and receive information. Specifically, this attack occurs by decreasing the signal to noise ratio by transmitting static and/or noise at high power levels across a given frequency band. This classification of attack can be accomplished in a variety of ways requiring a varying level of skill and access to specialized equipment. Jamming that targets specific channels in the LTE spectrum and is timed specifically to avoid detection is often referred to as smart jamming. Broadcasting noise on a large swath of RF frequencies is referred to as dumb jamming.

4.5.3 3. Impact Rating

The impact rating is divided into four categories: Financial, Operational, Privacy and Safety. Each of them is evaluated to one of four levels: negligible, moderate, major and severe. All ratings related to the threats described in the previous subsection are listed in *Tab. 25*. The outcome for this specific threat, tampering, is:

Negligible: For each category, the impact is considered negligible

Tab. 25 Generated impact rating for the realistic scenario

D	Title	Impact rating for safety damage	Impact rating for financial damage	Impact rating for operational damage	Impact rating for privacy damage
1	External Entity TCC Potentially Denies Receiving Data	Severe	Severe	Severe	Severe
2	Data Flow 4G Communication Network Is Potentially Interrupted	Severe	Severe	Severe	Severe

3	Malware	Major	Severe	Severe	Severe
4	Misconfiguration	Moderate	Moderate	Major	Major
5	Data Flow 4G Communication Network Is Potentially Interrupted	Severe	Severe	Severe	Severe
6	Data Flow SPATEM ITS G5 Network Is Potentially Interrupted	Severe	Severe	Severe	Severe
7	Spamming	Moderate	Moderate	Major	Negligible
8	Misconfiguration	Moderate	Moderate	Major	Major
9	Malware on RSU	Severe	Severe	Severe	Severe
10	Black Hole	Severe	Major	Severe	Negligible
11	GPS Spoofing	Severe	Major	Severe	Negligible
12	Masquerading	Negligible	Negligible	Negligible	Negligible
13	Downgrade attack	Negligible	Negligible	Moderate	Negligible
14	Black Hole	Severe	Major	Severe	Negligible
15	Radio Jamming Attack	Moderate	Moderate	Major	Negligible
16	Downgrade attack	Negligible	Negligible	Moderate	Negligible
17	Black Hole	Severe	Major	Severe	Negligible
18	Radio Jamming Attack	Moderate	Moderate	Major	Negligible

4.5.4 4. Attack path analysis

The attack path generated is not very verbose, as it only states the two objects under consideration, namely an OBU and an RSU, linked with the communication, namely V2X.

4.5.5 5. Attack feasibility rating

Based on the attack path described in last subsection, an attack feasibility rating is calculated for the studied threat; all other attack feasibility ratings are listed in *Tab. 26*.

The feasibility of the attack path analysed above is rated on five vectors:

- **Elapsed time: < 1 day:** The attacker will need less than one day to conduct the attack;
- **Expertise: Layman:** A layman's knowledge is the easiest to achieve, and the lowest level of expertise;
- **Knowledge: Public:** There is no required restricted knowledge of the system under consideration. Public knowledge developed on the C-ITS standards to understand C-ITS communication is enough;
- **Equipment required: Standard:** Equipment is easy to acquire and does not need specific modifications to operate.

The **aggregation** of these five vectors outputs the **easiest** level of **feasibility** for the specific studied threat.

Tab. 26 Generated attack feasibility rating for the realistic scenario

ID	Title	Elapsed time	Specialist expertise	Knowledge of the item or component	Window of opportunity	Equipment
----	-------	--------------	----------------------	------------------------------------	-----------------------	-----------

1	External Entity TCC Potentially Denies Receiving Data	<= 1 day	Layman	Public information	Unlimited	Standard
2	Data Flow 4G Communication Network Is Potentially Interrupted	<= 1 day	Layman	Public information	Unlimited	Standard
3	Malware	>6 months	Expert	Public information	Unlimited	Bespoke
4	Misconfiguration	<= 1 day	Proficient	Public information	Unlimited	Specialized
5	Data Flow 4G Communication Network Is Potentially Interrupted	<= 1 day	Layman	Public information	Unlimited	Standard
6	Data Flow SPATEM ITS G5 Network Is Potentially Interrupted	<= 1 day	Layman	Public information	Unlimited	Standard
7	Spamming	<= 1 day	Layman	Public information	Unlimited	Standard
8	Misconfiguration	<= 1 day	Proficient	Public information	Unlimited	Specialized
9	Malware on RSU	> 6 months	Expert	Public information	Unlimited	Bespoke
10	Black Hole	<= 1 week	Expert	Public information	Moderate	Specialized
11	GPS Spoofing	<= 1 week	Expert	Restricted information	Unlimited	Bespoke
12	Masquerading	<= 1 day	Layman	Public information	Unlimited	Standard
13	Downgrade attack	<= 1 month	Proficient	Public information	Easy	Standard
14	Black Hole	<= 1 week	Expert	Public information	Moderate	Specialized
15	Radio Jamming Attack	<= 1 week	Proficient	Public information	Easy	Specialized
16	Downgrade attack	<= 1 month	Proficient	Public information	Easy	Standard
17	Black Hole	<= 1 week	Expert	Public information	Moderate	Specialized
18	Radio Jamming Attack	<= 1 week	Proficient	Public information	Easy	Specialized

4.5.6 6. Risk determination

The combination of the impact rating and attack feasibility gives the **lowest** risk for the studied threat. Other risk values are listed in *Tab. 27*.

Tab. 27 Generated impacts and risks for the generated threats

ID	Title	Safety Risk	Financial Risk	Operational Risk	Privacy Risk
1	External Entity TCC Potentially Denies Receiving Data	1	1	1	1
2	Data Flow 4G Communication Network Is Potentially Interrupted	1	1	1	1
3	Malware	49	65	65	65
4	Misconfiguration	8	8	11,5	11,5
5	Data Flow 4G Communication Network Is Potentially Interrupted	1	1	1	1
6	Data Flow SPATEM ITS G5 Network Is Potentially Interrupted	1	1	1	1
7	Spamming	1	1	1	1
8	Misconfiguration	8	8	11,5	11,5
9	Malware on RSU	65	65	65	65

10	Black Hole	31	23,5	31	1
11	GPS Spoofing	35	26,5	35	1
12	Masquerading	1	1	1	1
13	Downgrade attack	1	1	9	1
14	Black Hole	31	23,5	31	1
15	Radio Jamming Attack	10	10	14,5	1
16	Downgrade attack	1	1	9	1
17	Black Hole	31	23,5	31	1
18	Radio Jamming Attack	10	10	14,5	1

4.5.7 7. Risk treatment decision

The **risk does not need to be mitigated**, as the impacts are very low. The risk treatment decision is not automatically calculated due to its complexity. Thus, other risk treatment decisions are not listed.

4.5.8 Tool-based summary

Summary

All attacks are STRIDE-labelled by design, and feasibility as well as impact ratings are automatically generated.

Conclusion

For this example, the effort invested in template creation facilitated the output of an initial list of threats to be analysed. This shows that the output of the model relies heavily on the quality of the template. One important conclusion from this is that more should be done to create a specific task force involving cybersecurity and mobility experts to produce an exhaustive threat catalogue for C-ITS. The effort is required only once and would undoubtedly be worth the investment. As shown in this subsection, the quality of the template effectively reduces the required amount of expert input at subsequent stages.

It is noteworthy that the results of the tool-based method differ significantly from the human-based approach. This divergence is illustrated by the masquerading attack in the tool-based approach, which represents an outsider's ability to pose as a legitimate node. The tool-based method considers that the behaviour of other nodes will not be affected, resulting only in a small disruption. Even if it is feasible to create a fake green light signal, hiding the legitimate red-light signal is not; vehicles should be able to see the contradiction and continue to operate safely.

4.6 Sum up

Both approaches showed advantages and disadvantages. The human-based approach showed the benefit of having a cybersecurity expert at every step of the risk assessment, namely the ability to tailor threat scenarios to the specific use case and to have a complete analysis of the attack paths, enabling accurate calculation of attack feasibility. However, this approach requires a lot of human effort for each project. In the tool-based approach, on the other hand, once an adequate template is created, a new project can be conducted without the cybersecurity expert. The downside to this approach is that it could lead to generic threats that have to be reviewed after template generation, and to inadequate attack feasibility metrics also caused by generalization during template creation and lack of detail in the attack path step. The ideal solution is therefore a "hybrid approach" that

combines the strengths of the human- and tool-based approaches. The application and implementation of this “hybrid approach” will be described in the next section.

5 Hybrid approach

Previous sections showed the advantages and disadvantages of both the human-based and tool-based methods. The recommended approach is considered to be a “hybrid” one that combines the advantages of each method. This section will show how this hybrid approach works, which part is carried out automatically (tool-based), and which part is done manually (human-based).

5.1 Hybrid approach setup

The automated solutions showed good results for asset definition, threat scenario definition impact rating and attack feasibility rating. Thus, these steps will be performed with the modelling tool. Attack path analysis (step 4) will be performed manually, based on the data-flow diagram defined in the modelling tool, this limitation is due to the actual threat modelling tool, an improvement of this tool will allow to automated this step too. Finally, the risk determination will be calculated automatically on the Excel template developed in the manual approach. *Fig. 42* shows all steps of the risk analysis from asset determination to risk determination.

Data transmission from the modelling tool to the excel template will be done through an executable. This process is illustrated in *Fig. 43*. Cells filled in blue are done through the modelling tool and cells filled in green are done through the Excel template.

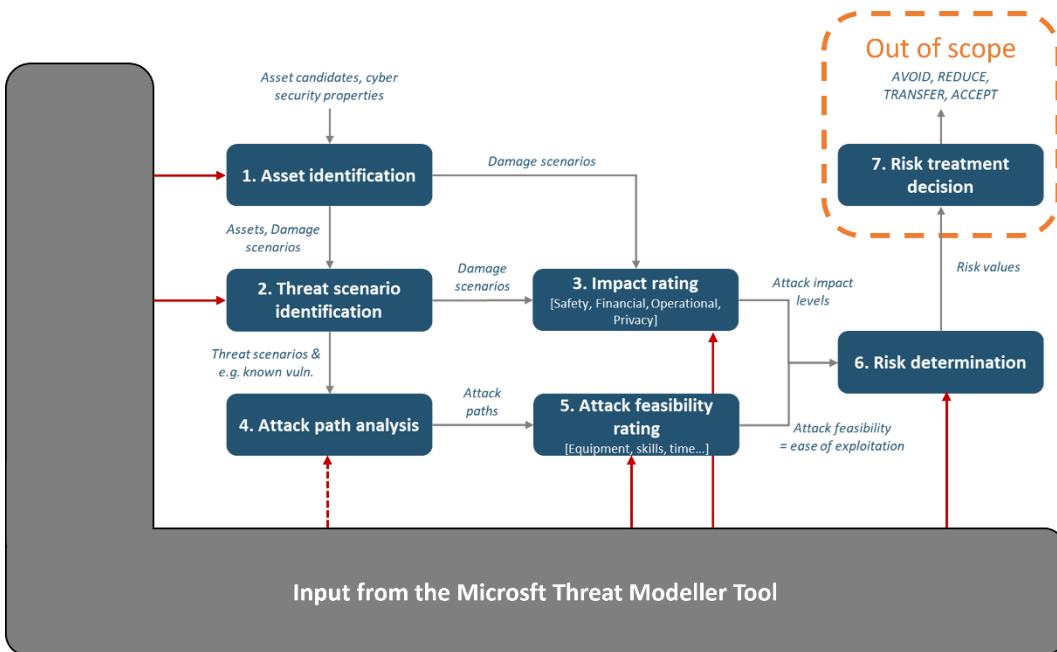


Fig. 42 Graphical representation of which steps are performed automatically and manually

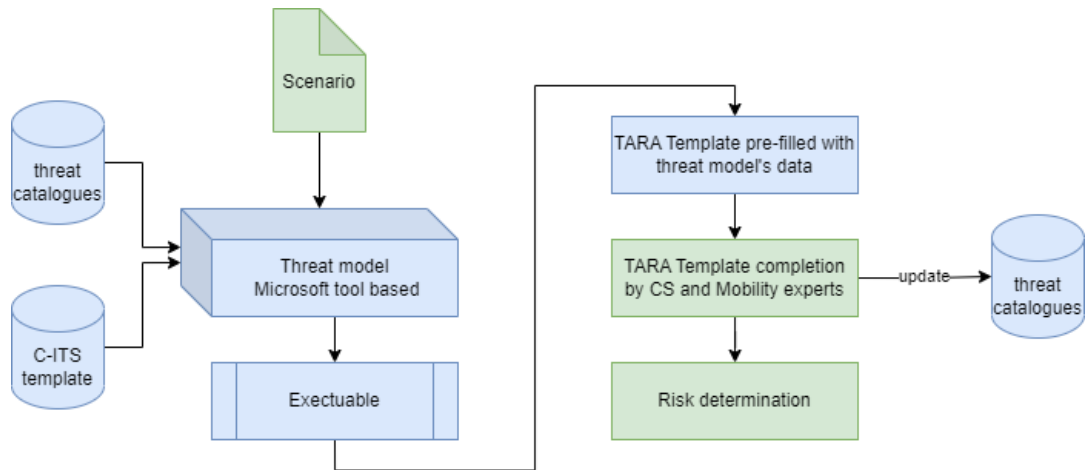


Fig. 43 Hybrid process approach illustration

5.2 Hybrid approach example

The scenario developed in section 3.4, designed to test both the automatic (tool-based) and manual (human-based) approaches, will also be used to evaluate this hybrid approach and to show how it works and its advantages. *Fig. 44* illustrates the scenario with an automated vehicle and a connected traffic light that broadcasts its status with V2X messages.

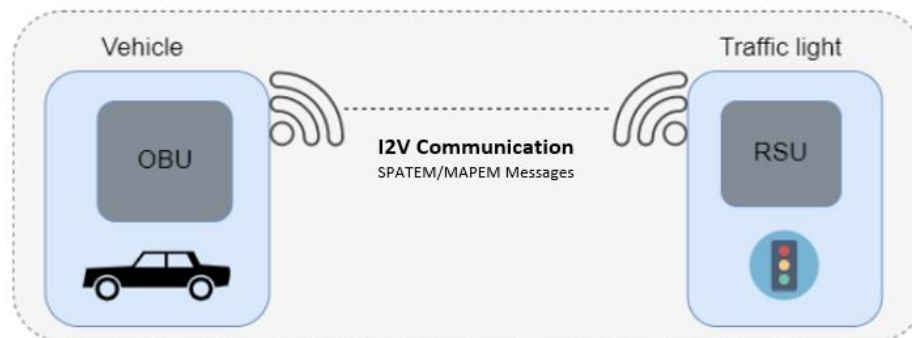


Fig. 44 Illustration of a communication between a traffic light and a vehicle

5.2.1 Threat modeling tool

For this first step, the scenario will be described on the Microsoft threat modelling tool. This task can be understood as drawing the data flow diagram using a predefined template. Only basic knowledge of the tool and no prior cybersecurity experience are required. The execution of this step is described in subsection 4.3 (tool-based approach), and illustrated in *Fig. 45*.

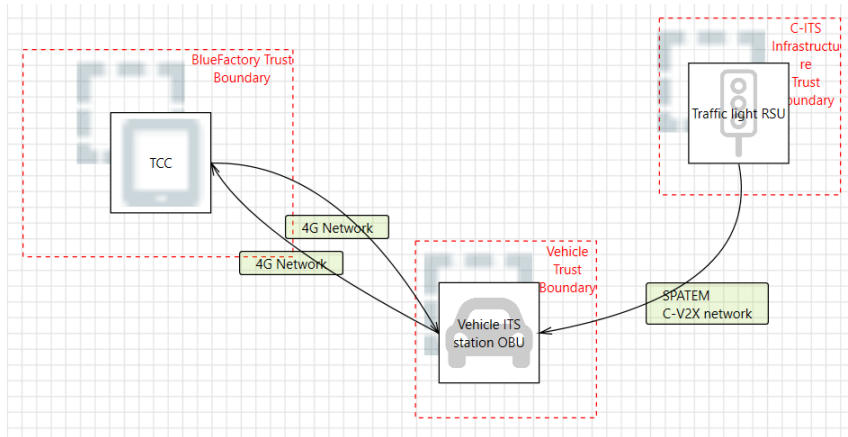


Fig. 45 Example of data flow diagram

5.2.2 Data extraction to Excel template

Once the scenario is modelled on the Microsoft tool, the data can be extracted with a tailored script, that will prefill the Excel template, annex II.3 with the information from the model. An example of a prefilled template is shown in Fig. 46 and Fig. 47. Fig. 46 shows a first list of assets generated by the threat modeler tool. Then based on its possible related threat scenario, coming from the threat catalogue defined by the working group, and their related STRIDE vector are listed in step 2 “2. Threat scenario identification”. Gaps will be filled in the next subsection by a cybersecurity specialist.

Fig. 47 illustrates last four parts of the risk assessments. The main gap in this part is the “attack path analysis”, step 4. This is part is highly dependent on the environment and related implemented hardware, depending on the RSU architecture for example.

Selected Item: v2l and l2v communication																
0. Item traceability		1. Asset identification						2. Threat scenario identification				3. Impact rating				
Function id	Function description	SaC ?	Component / Message	Asset	Cybers-orig		Damage scenario	Safety relevant	Threat scenario ID	STRIDE vector	Impact					
					Confidentiality	Integrity	Availability	Damage scenario description			Financial	Operational	Privacy	Safety	Worst impact - (worst case if controlability used)	Highest impact
				SPATEM C-V2X network					1	Denial Of Service	Moderate	Major	Negligible	Moderate		Major
				SPATEM C-V2X network					2	Denial Of Service	Severe	Severe	Severe	Severe		Severe
				SPATEM C-V2X network					3	Denial Of Service	Severe	Major	Major	Severe		Severe
				SPATEM C-V2X network					4	Denial Of Service	Major	Severe	Negligible	Severe		Severe
				SPATEM C-V2X network					5	Denial Of Service	Moderate	Major	Negligible	Moderate		Major
				SPATEM C-V2X network					6	Denial Of Service	Severe	Severe	Severe	Severe		Severe
				SPATEM C-V2X network					7	Tampering	Negligible	Moderate	Negligible	Negligible		Moderate

Fig. 46 TARA template automatically filled with information coming from the model (steps 1, 2 and 3)

4. Attack path analysis		5. Attack feasibility rating (alternatives to be chosen between A, B or C)							6. Risk determination [Symmetric matrix]			
Attack path id	Attack path	A. Attack potential-based feasibility							Aggregated and total feasibility	Risk criteria		Risk value [0-5]
		Elapsed time	Expertise	Knowledge	Window of opportunity	Equipment required	TOTAL	Impact		Feasibility		
		< 1 week	Layman	Public	Unlimited	Standard	0	High	Severe	High	5	
		<= 3 years	Expert	Public	Unlimited	Bespoke	23	Low	Severe	Low	3	
		< 1 week	Proficient	Public	Unlimited	Specialized	7	High	Severe	High	5	
		< 1 week	Expert	Public	Moderate	Specialized	14	Medium	Severe	Medium	4	
		< 1 week	Proficient	Public	Easy	Specialized	8	High	Severe	High	5	
		< 1 week	Layman	Public	Unlimited	Standard	0	High	Severe	High	5	
		< 1 month	Proficient	Public	Easy	Standard	5	High	Severe	High	5	

Fig. 47 TARA template automatically filled with information coming from the model (steps 4, 5 and 6)

5.2.3 Completion of the TARA template

This is the first step where cybersecurity knowledge is required. The first task is to check the completeness, consistency and correctness of the threat scenario and of its estimated impact as generated by the threat model. This human check is necessary due to possible limitations in the scenario specifications. Once this verification is carried out, template completion can start.

First activity is to fill the “damage scenario”, a small text explaining the possible damage on the C-ITS infrastructure given the C-ITS usage, monitoring, autonomous vehicle... Then based on it step 3, “impact rating” will be finetuned to match the damage scenario. Fig. 48 shows step 1 to 3 filled and reviewed.

Selected items v2i and i2x communication																
0. Item traceability		1. Asset identification					2. Threat scenario identification			3. Impact rating						
Function id	Function description	BUC ?	Component / Message	Asset	Cybers-- wrt			Damage scenario	Threat scenario id	STRIDE vector	Threat scenario description	Impact				Highest impact
					Confidentiality	Integrity	Availability					Financial	Operational	Privacy	Safety	
F01	Communication between RSU > OBU		Message from RSU to OBU	SPATEM C-V2X network		X	The vehicle does not stop on the traffic light due to an incorrect SPATEM	1	Denial Of Service	Spamming	Moderate	Major	Negligible	Severe	Command modification leading to a crash with humans	Severe
F01	Communication between RSU > OBU		Message from RSU to OBU	SPATEM C-V2X network		X	The vehicle does not stop on the traffic light due to an incorrect SPATEM	2	Denial Of Service	Malware on RSU	Severe	Severe	Severe	Severe	Command modification leading to a crash with humans	Severe
F01	Communication between RSU > OBU		Message from RSU to OBU	SPATEM C-V2X network		X	The vehicle does not stop on the traffic light due to missing SPATEM information (traffic light state)	3	Denial Of Service	Misconfiguration	Severe	Major	Major	Severe	Command modification leading to a crash with humans	Severe
F01	Communication between RSU > OBU		Message from RSU to OBU	SPATEM C-V2X network		X	The vehicle does not stop on the traffic light due to missing SPATEM information (traffic light state)	4	Denial Of Service	Black Hole	Major	Severe	Negligible	Severe	Command modification leading to a crash with humans	Severe
F01	Communication between RSU > OBU		Message from RSU to OBU	SPATEM C-V2X network		X	The vehicle does not stop on the traffic light due to missing SPATEM information (traffic light state)	5	Denial Of Service	Radio Jamming Attack	Moderate	Major	Negligible	Severe	Command modification leading to a crash with humans	Severe
F01	Communication between RSU > OBU		Message from RSU to OBU	SPATEM C-V2X network		X	The vehicle does not stop on the traffic light due to missing SPATEM information (traffic light state)	6	Denial Of Service	Data Flow SPATEM C-V2X network is Potentially Interrupted	Severe	Severe	Severe	Severe	Command modification leading to a crash with humans	Severe
F01	Communication between RSU > OBU		Message from RSU to OBU	SPATEM C-V2X network		X	The vehicle does not stop on the traffic light due to missing SPATEM information (traffic light state)	7	Tampering	Downgrade attack	Negligible	Moderate	Negligible	Severe	Command modification leading to a crash with humans	Severe

Fig. 48 TARA template after completion and review by a CS Specialist (steps 1, 2 and 3)

Step 4 (attack path analysis) must be completed with relevant information / step to perform the attack. Then based on it step 5 (attack feasibility rating) will be reviewed to finetune value generated by the model. This fine tuning is required as the feasibility can evolve because of new weaknesses in the system or with the availability of new equipment to perform an attack. A template filled in with steps 4, 5 and 6 is illustrated in Fig. 49.

4. Attack path analysis		5. Attack feasibility rating (alternatives to be chosen between A, B or C)							6. Risk determination [Symmetric matrix]		
Attack path id	Attack path	A. Attack potential-based feasibility							Risk criteria		Risk value [0-5]
		Elapsed time	Expertise	Knowledge	Window of opportunity	Equipment required	TOTAL	Aggregated and total feasibility	Impact	Feasibility	
AP01	i. Detection of a CY2X communication hotspot ii. Spamming the network with tons of unnecessary messages	< 1 week	Layman	Public	Unlimited	Standard	0	High	Severe	High	5
AP02	i. Detection of RSU network ii. Connection as root on the RSU iii. Perform a network-based DoS	<= 3 years	Expert	Public	Unlimited	Bespoke	23	Low	Severe	Low	3
AP03	i. Detection of RSU network ii. Analyse of RSU network configuration iii. Exploit misconfiguration	< 1 week	Proficient	Public	Unlimited	Specialized	7	High	Severe	High	5
AP04	i. Detection of RSU network ii. Analyse of RSU network configuration iii. Set a blackhole for all incoming communication	< 1 week	Expert	Public	Moderate	Specialized	14	Medium	Severe	Medium	4
AP05	i. Detection of RSU network ii. Analyse of radio frequency iii perform a jamming attack on this frequency	< 1 week	Proficient	Public	Easy	Specialized	8	High	Severe	High	5
AP06	i. Detection of RSU network ii. Simulate thousands of connected device using the same frequency iii. The network will be congested iv. New V2X messages will not be sent	< 1 week	Layman	Public	Unlimited	Standard	0	High	Severe	High	5
AP07	i. Detection of RSU network ii. Attacker intercept and manipulate the 4g communication iii The 4g network with switch to 3g or 2g iv. 4g messages security will not work v. The CITS communication will not work	< 1 month	Proficient	Public	Easy	Standard	5	High	Severe	High	5

Fig. 49 TARA template after completion and review by a CS Specialist (steps 4, 5 and 6)

The last steps of the TARA template are filled in automatically with the internal Excel calculations and a risk value is returned. Based on the risk value and cybersecurity knowledge of the user, a risk treatment option can be selected. The complete Excel template is available in annex II.4. Different risk treatment options can then be defined, such as Reducing, Avoiding, Transferring and Accepting the risk, but these decisions are out of scope for the current project.

5.3 Sum up

This example showed why a hybrid approach, simplified in Fig. 50, is the best one. The advantage of the automated (tool-based) part is that no cybersecurity knowledge is required to generate a data flow diagram. This automated generation significantly reduces the time and effort required to list assets, damage scenarios and threat scenarios, and thus also reduces the time that cybersecurity experts need to be involved in the project. In fact, the expert’s knowledge is only required to build the template. Afterwards, the manual (human-based) steps ensure that the generated data is verified and in conformity with the system under consideration. The hybrid approach is not without its disadvantages, however. The main one is the script required to convert the produced data into the right format for the Excel template. But the only solution to avoid this step would be to develop a tailored threat modelling tool that integrates the specific risk analysis.

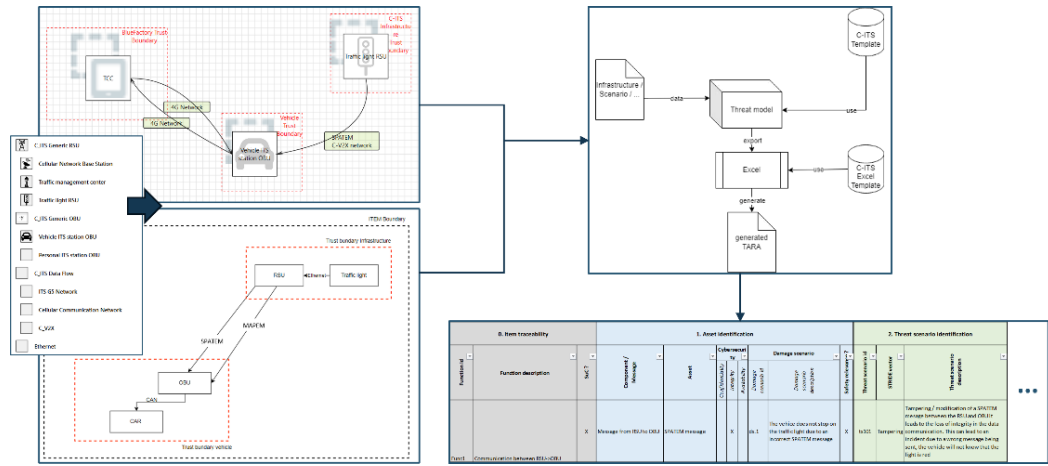


Fig. 50 Hybrid approach's schematic view

6 Conclusion

This research report has focused on cyber risk assessment activities applied to the Cooperative Intelligent Transport Systems (C-ITS) environment. The analysis and findings underscore the critical importance of addressing cybersecurity concerns to ensure the secure and reliable deployment of C-ITS. The research has highlighted the various cyber risk challenges associated with C-ITS, using V2X communications as an example of attack vector / targets. These challenges emphasize the need for comprehensive cybersecurity measures to mitigate risks and protect the integrity, confidentiality and availability of future Swiss C-ITS systems.

Effective risk assessment methodologies and frameworks play a vital role in identifying and evaluating potential cyber threats and vulnerabilities specific to the C-ITS environment. The research has explored existing risk assessment approaches, such as threat modelling using STRIDE methodology, which provide valuable insights into system weaknesses and potential attack vectors. These assessments aid in prioritizing security measures and allocating resources effectively.

Furthermore, the research has emphasized the importance of collaboration and information sharing among stakeholders in the C-ITS ecosystem. Government agencies, industry partners, and cybersecurity experts must work together to establish standardized security frameworks (standard-based approaches), develop secure communication protocols (commonly agreed secure technologies), and promote best practices in secure C-ITS deployment. Cross-sector collaboration enhances the resilience of C-ITS systems against emerging cyber threats and fosters a proactive approach to cybersecurity. This project proposed to formalize that shared knowledge within a threat model template to be maintained continuously in order to keep a realistic view of threats against existing and upcoming C-ITS infrastructure

In conclusion, the successful deployment of C-ITS relies heavily on robust cyber risk assessment activities and proactive security measures. By implementing comprehensive risk assessment methodologies, collaborating across sectors, and prioritizing cybersecurity, countries can address the unique challenges of the C-ITS environment and pave the way for a secure and resilient intelligent transport system that enhances road safety, efficiency, sustainability and data privacy.

6.1 Project valorization

The project's outcomes enabled the execution of additional research concerning C-ITS (Cooperative Intelligent Transport Systems) communications. Primarily focused on practical research initiatives, the implementation of On-Board Units (OBUs) on extensively automated vehicles facilitated the evaluation of attack feasibility. The experimentation was carried out within a private communication laboratory established at ROSAS, enabling systematic assessment of potential vulnerabilities.

6.2 Future perspectives

Future perspectives for this project are split in three main categories: C-ITS technology, threat modeler and project valorization.

6.2.1 Cyber threat analysis model extension

This project has carried out an analysis on how C-ITSs work and on related threats from a high-level of abstraction. Although the scope of C-ITS was restricted to two specific car-to-car and car-to-infrastructure communications (SPATEM & MAPEM) in this project, the actual scope of C-ITS is much wider. Thus, a first perspective for future work is to widen the project's output to include all C-ITS types, including communication between vehicles

and pedestrians, tolls, traffic management and their related threats. A few starting points are listed below for these communication types.

Pedestrians [39]: Multiple research projects have focused on V2P communication, or Vehicle-to-Pedestrian. As the main outputs of those projects show, the device most commonly used by pedestrians to receive messages is the smartphone (and, less frequently, a tag, especially for child safety). The aims of those messages are to ensure the safety of pedestrians on roads shared with other road users.

Bicyclists [40]: V2X technology can be used to alert vehicles about a cyclist coming from a blind spot or to broadcast a bicyclist's speed and positional data. A first project, Bike2CAV, was developed in Salzburg, Austria. This project tested the communication between an onboard unit on the bicycle and other automated vehicles. The potential payload under consideration is the positional data of the bicyclist, which may exhibit a potential variation of up to 50cm.

Vehicles: V2X communication standards define multiple types of messages to improve road efficiency and safety for vehicles and automated vehicles. These messages are sent through direct communication between the vehicles or between vehicles and infrastructure. Examples of safety messages are:

- **BSM** (Basic Safety Message): every connected vehicle broadcasts its current position, position, speed, and acceleration;
- **DENM** (Decentralized Environmental Notification Message): broadcasts information about road hazards or weather conditions in a vehicle's surroundings;
- **RSI**: (Road Sign Information): broadcasts real-time information about speed limits and regulatory signs.

Connected services (Traffic management center, Cooperative management center, Remote operation center): Despite being put aside during the project, this element is an important part of a C-ITS environment. Connected services are responsible for collecting, processing, and managing traffic data from various sources, such as road sensors, surveillance cameras, detection devices, signaling systems, and more. They also communicate with other intelligent transport systems, such as connected vehicles (OBU), smart signage (RSU), and mobile applications, to exchange information and coordinate actions. *Fig. 51* illustrates this management system in a C-ITS environment.

The primary role of the TMC is to monitor real-time traffic conditions and make traffic management decisions to optimize the efficiency, safety, and flow of the road network. This may include managing traffic signals, adjusting signal timings, lane management, controlling recommended routes, coordinating special events, and other traffic management strategies.



Fig. 51 Illustration of a CMS or Traffic Management Control in a C-ITS environment

Fig. 51 illustrates the CMS by a cloud solution, but the communication between RSU and the traffic controller can also be wired. Alternatively, the TMC could be used as an endpoint of a SOC (Security Operations Center). This communication could enable detection of

security incidents at an early phase, with a traffic light remaining green or a speed limit indicator that does not comply with Federal law.

Future use cases: The 5GAA, or 5G Automotive Association, published a roadmap for c-v2x integration until 2030. Future use cases such as automated valet parking will mainly rely on automated driving safety and highly automated capabilities with HD sensor information sharing between vehicles and cooperative maneuvers. The complete roadmap is illustrated in *Fig. 52*.

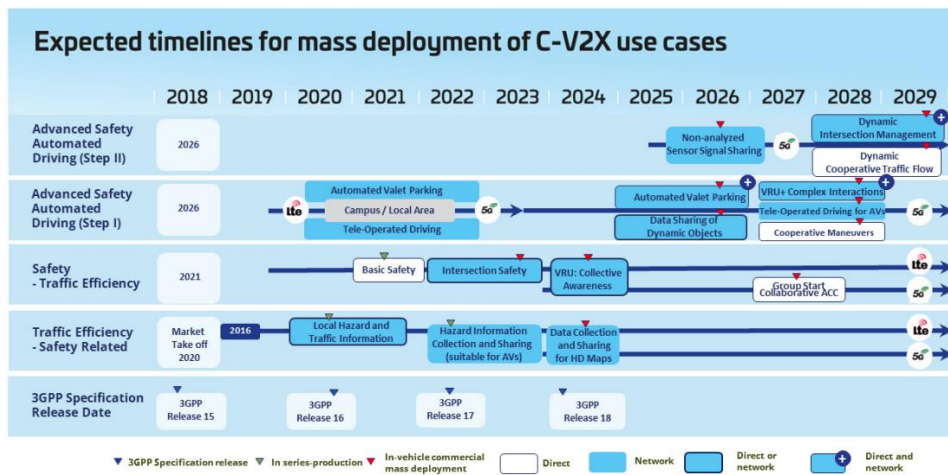


Fig. 52 Roadmap of C-V2X use cases [41]

6.2.2 Cyber threat assessment for Swiss C-ITS – Way forward

This project illustrated five different workstreams to be considered by national authorities in the context of C-ITS analysis and deployment. Those topics are not only cyber security related, but might either be supported or impacted by cyber security consideration.

Standardization and cross-border cooperation: Developing and implementing standardized protocols and frameworks for C-ITS is crucial to ensure interoperability and compatibility across different systems and devices. Countries must collaborate and agree on common standards to enable seamless communication and cooperation between vehicles and infrastructure. From a cyber security perspective, considerations about the potential deployment of PKI (Public Key Infrastructure) or any other security mechanisms for securing C-ITS should be commonly agreed for ensuring a security baseline

- **#1 Way Forward:** Use of cyber threat assessment model for benchmarking C-ITS architecture and technologies, e.g. C-V2X vs ITS-G5 using PKI.

Legal and regulatory framework: Countries need to establish appropriate legal and regulatory frameworks to govern the deployment of C-ITS. This includes defining liability and responsibility in case of accidents or malfunctions, addressing data ownership and privacy concerns, and setting rules for the collection, storage, and usage of C-ITS data. From a cyber security perspective, outputs from this project should be considered as insightful resources for identifying major threats which would require legally binding mitigation measures

- **#2 Way Forward:** Use of threat catalogue, as well as threat assessment model for identifying current and future threats to be considered for “authorizing” C-ITS systems based on Swiss rules

User acceptance and adoption: Encouraging user acceptance and adoption of C-ITS technologies can be a challenge. Public awareness campaigns, educational initiatives, and incentives may be necessary to familiarize users with the benefits of C-ITS and alleviate concerns related to privacy, security, and reliability. From a cyber security perspective,

such project should be used as an argument for demonstrating efforts and considerations made by Swiss authorities towards secure C-ITS

- **#3 Way Forward:** stimulate Swiss cyber security community about C-ITS security concerns, based on initial project results and way forward to secure C-ITS development and deployment

Funding, high-level commitment and collaboration: Implementing secure C-ITS requires significant resources, including financial and human resources. Countries need to secure funding for research and development, infrastructure deployment, and ongoing maintenance. Collaboration between government agencies, private companies, and research institutions is crucial to leverage expertise and resources effectively. From a cyber security perspective, Swiss authorities should define their strategy to tackle cyber security risks applied to upcoming C-ITS environment. Discussions about governance and management of this topic should be considered, including evaluation of potential implementation of cyber security management system on national and/or cantonal level.

- **#4 Way Forward:** Investigate about the needs of formal cyber security management system and advanced strategy for C-ITS related cyber risk handling

Cyber threat assessment improvement: The developed threat model and risk analysis framework facilitates the identification and tracking of cyber risks, from asset determination to risk value and potential treatment decision. However, the process is split in two parts due to current tool limitations. Improvements of such cyber threat assessment tool would maximize efficiency and threat identification quality

- **#5 Way Forward:** Improve the integration of tools for supporting the identification and handling of cyber threats, either using the proposed solutions as a baseline, or migrating to a professional solution as mentioned throughout relevant part of this report

6.2.3 Follow-up project – From proactive approach to reactive methods

Proactive methods such as the one presented throughout this report are key for responding to current known threats. However, cyber security landscape is dynamic and would therefore require complementary reactive methods for handling newly discovered threats and maintaining the security of systems already in operation.

For responding to this need, MB4 research group issued a subsequent research proposal targeting feasibility analysis related to potential future “Security Operation Center” (SOC) to be operated in that purpose (MB4_20_02G_01). In that context, current consortium responded to that project tender and received a preliminary approval from FEDRO.. Fig. 53 below conceptually illustrates an overview about collaborative proactive and reactive methods.

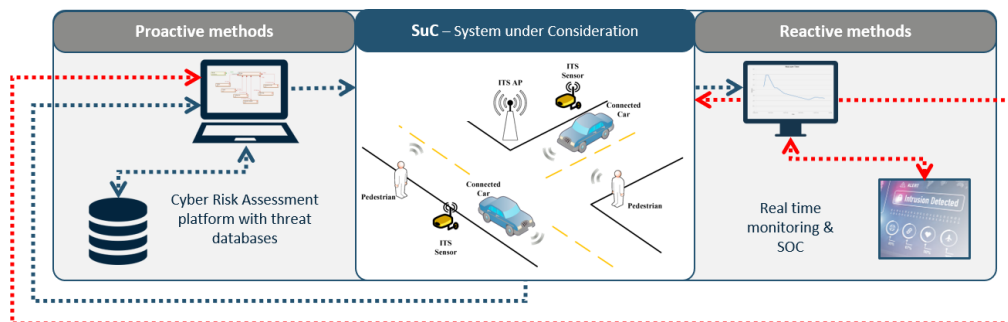


Fig. 53 Proactive method follow-up project

Annexes

I	STRIDE categories	88
II	External annexes.....	89
II.1	Excel template for tool-based approach	89
II.2	Completed TARA following human-based approach	89
II.3	TARA following hybrid approach.....	89
II.4	Completed TARA following hybrid approach	89

I STRIDE categories

This annex lists the different categories and gives an example related to a C-ITS.

Spoofting

A spoofing attack consists of usurping the identity of a person or a program to gain an illegitimate advantage. Applied to C-ITS it can be an unauthorized RSU that sends wrong information about a traffic light to surrounding OBUs.

Tampering

The intentional but unauthorized modification of parameters exchanged between a client and a server. Applied to C-ITS it can be a modification of an ITS-G5 frames to indicate that a lane is free when it is not.

Non-Repudiation

Non-repudiation happens when an action has been assigned to another person on a log-file. From an attacker perspective related to C-ITS. The attacker can modify the list of authorized RSU in a certain area and then modify the logs to look like the modification have been done by an authorized user.

Information disclosure

It happens when there is a data leak. The leak can be intentional or unintentional the result will be the same sensitive data can be exposed to unauthorized person. Applied to C-ITS it could result in a leak of all vehicles that go through a certain intersection with their actual speed.

DoS : Denial of Service

DoS happens when an or multiple attackers flood the network to make the system or a part of it temporarily or definitely unavailable. A DoS attack to a C-ITS infrastructure could result in flooding a RSU linked to a traffic light. Thus, it will not be able to transmit its current state to the OBU located in a certain area.

Elevation of Privilege

Elevation of privilege is the act of exploiting a flaw in the configuration of the OS or in a software application to gain elevated access to normally non-authorized data. In a C-ITS perspective it can be the RSU application that receive the messages from the OBU access to the application that can modify the priority in an intersection. In this case it is a horizontal privilege escalation. An example of vertical privilege escalation is from this application that receive the message from the OBU access to the root level and uninstall the complete OS or corrupt it.

II External annexes

II.1 Excel template for tool-based approach

The template is available in “TARA_Template_ToolBased.xlsx”.

II.2 Completed TARA following human-based approach

The TARA after the human-based approach in “TARA_MB4_HumanBased.xlsx”

II.3 TARA following hybrid approach

The TARA after the automatic generation is available in “TARA_MB4_Hybrid.xlsx”

II.4 Completed TARA following hybrid approach

The completed TARA is available in “TARA_MB4_Hybrid_Filled.xlsx”

Glossar

Begriff	Bedeutung
3GPP	3rd Generation Partnership Project (3GPP)
ANSSI	Agence nationale de la sécurité des systèmes d'information / French National Agency for the Security of Information System (ANSSI)
API	Application Programming Interface (API)
C2I	Car-to-Infrastructure (C2I)
CAM	Cooperative Awareness Message (CAM)
CE	Community Edition (CE)
CEN /TC	European Committee for Standardization (CEN) /Technical Committees (/TC)
CENELEC	European Committee for Electrotechnical Standardization (CENELEC)
CES	Clean Energy Standard (CES)
CIA	Confidentiality, Integrity and Availability (CIA)
C-ITS	Cooperative Intelligent Transport Systems and Services (C-ITS)
CRL	Certificate Revocation List (CRL)
CRUD	Creating, Reading, Updating, Deleting (CRUD)
C-V2X	Cellular Vehicle-to-Everything (C-V2X)
DENM	Decentralized Environmental Notification Message (DENM)
DFD	Data Flow Diagrams (DFD)
DoS	Denial-of-Service (DoS)
E/E	Electrical/Electronic (E/E)
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité / Expression of Needs and Identification of Security Objectives (EBIOS)
ECIES	Elliptic Curve Integrated Encryption Scheme (ECIES)
EE	Entreprise Edition (EE)
EEA	European Economic Area (EEA)
eNB	Evolved Node B (eNB)
ETSI	European Telecommunications Standards Institute (ETSI)
EU	European Union (EU)
EVITA	E-safety vehicle intrusion protected applications (EVITA)
GDPR	General Data Protection Regulation (GDPR)
GSM	Global System for Mobile Communications (GSM)
I2V	Infrastructure-to-Vehicle (I2V)
ICT	Information and Communications Technology (ICT)
IDX	Internet Data Exchange (IDX)
IEC	International Electrotechnical Commission (IEC)
IEEE	Institute of Electrical and Electronics Engineers (IEEE)
ISO /TR /SAE	International Organization for Standardization (ISO) /Technical Reports (/TR) /Society of Automotive Engineering (/SAE)
IT	Information Technology (IT)

ITS	Intelligent Transport Systems and Services (ITS)
-S	-Station (-S)
-SU	-Station Unit (-SU)
-G5	-5 GHz (-G5)
ITU	International Telecommunication Union (ITU)
IVIM	Infrastructure-to-Vehicle Information Message (IVIM)
LBS	Location-Based Service (LBS)
LOS	Line-Of-Sight (LOS)
LTE	Long Term Evolution (LTE)
MAPEM	MAP Extended Message (MAPEM)
MTMT	Microsoft Threat Modelling Tool (MTMT)
NFAP	National Frequency Allocation Plan (NFAP)
OBU	On Board Unit (OBU)
OEM	Original Equipment Manufacturer (OEM)
OT	Operational technology (OT)
OVHI	OBU to Vehicle Host Interface (OVHI)
OWASP	Open Worldwide Application Security Project (OWASP)
PASTA	Process of Attack Simulation and Threat Analysis (PASTA)
PII	Personal Identifying Information (PII)
PKI	Public Key Infrastructure (PKI)
PRR	Packet Reception Rate (PRR)
RF	Radio Frequency (RF)
RO	Risk Origins (RO)
RSU	Road-Side Unit (RSU)
SaaS	Software as a Service (SaaS)
SCOOP	Système Coopératif (SCOOP)
SDL	Secure Development Lifecycle (SDL)
SFOP	Safety impact, Financial impact, Operational impact and/or Privacy impact (SFOP)
SFR	Security Functional Requirement (SFR)
SNV	Swiss Association for Standardization (SNV)
SPATEM	Signal Phase And Timing Extended Message (SPATEM)
SREM	Signal Request Extended Message (SREM)
SSEM	Signal request Status Extended Message (SSEM)
SSO	Single Sign-On (SSO)
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege (STRIDE)
TARA	Threat Analyses and Risk Assessment (TARA)
TCC	Teleoperation Control Center (TCC)
TMC	Transportation Management Center (TMC)
TMT	Threat Modelling Tool (TMT)
TO	Target Objektive (TO)
TOE	Target Of Evaluation
TTT	Transport and Traffic Telematics (TTT)
TVRA	Threat, Vulnerability And Risk Assessment (TVRA)

UMTS	Universal Mobile Telecommunications System (UMTS)
UNECE	United Nations Economic Commission for Europe (UNECE)
UX	User Experience (UX)
V2I	Vehicle-to-Infrastructure (V2I)
V2V	Vehicle-to-Vehicle (V2V)
V2X	Vehicle-to-Everything (V2X)
VAST	Visual, Agile, Simple Threat (VAST)
VMS	Variable Message Sign (VMS)
WSA	WAVE Service Advertisement (WSA)
XiL-lab	Everything-in-the-Loop Laboratory (XiL-Lab)
YAML	Yet Another Markup Language (YAML)

Bibliography

Regulations

- [1] United Nations Economic Commission for Europe UNECE (2021), „Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system”, Addendum 154 – UN Regulation No. 155, <https://unece.org>
- [2] The European parliament and the council of the European union EU (2016), „Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)”, REGULATION (EU) 2016/679, <https://eur-lex.europa.eu>

Standards

- [3] European Committee for Standardization CEN (1991), „Intelligent transport systems – Cooperative ITS”, CEN/TC 278/WG 16
- [4] International Organization for Standardization ISO (2020), „Intelligent transport systems – Station and communication architecture”, ISO 21217:2020
- [5] Institute of Electrical and Electronics Engineers IEEE (2010), „Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments”, IEEE 802.11p-2010
- [6] European Commission (2019), „supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems”, 2010/40/EU
- [7] International Organization for Standardization ISO (2022), „Information security, cybersecurity and privacy protection”, ISO/IEC 27001:2022
- [8] International Organization for Standardization ISO (2018), „Information technology — Security techniques — Information security risk management”, ISO/IEC 27005:2018
- [9] International Organization for Standardization ISO (2019), „Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices”, ISO/TS 21177:2019
- [10] International Organization for Standardization ISO (2019), „Intelligent transport systems — Communication profiles for secure connections between trusted devices”, ISO/TS 21185:2019
- [11] Institute of Electrical and Electronics Engineers IEEE (2022), „Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages”, IEEE 1609.2-2022
- [12] International Organization for Standardization ISO (2021), „Cooperative intelligent transport systems (C-ITS) — Guidelines on the usage of standards — Part 3: Security”, ISO/TR 21186-3:2021
- [13] International Organization for Standardization ISO (2021), „Road vehicles — Cybersecurity engineering”, ISO/TR 21434:2021
- [14] European Telecommunications Standards Institute ETSI (2017), „Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)”, ETSI TS 102 165-1
- [15] European Telecommunications Standards Institute ETSI (2018), „Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services”, ETSI TS 103 301

Documentation

- [16] Tmoney (Accessed 19.01.2023), „C-ITS”
- [17] SecurityWeek (Accessed 19.01.2023), „Tesla Car Hacked Remotely From Drone via Zero-Click Exploit”
- [18] DW (Accessed 19.01.2023), „Germany's military-run transport fleet hacked”
- [19] Q-Free (Accessed 19 01 2023), „C-ITS ON-BOARD UNIT (OBU)”
- [20] C-ITS (Accessed 19.01.2023), „About C-ITS”
- [21] Shagdar, O., Tsukada, M., Kakiuchi, M., Toukabri, T., & Ernst, T. (2012), „Experimentation towards IPv6 over IEEE 802.11p with ITS Station Architecture”
- [22] Mireles, Rui, Mate Boban, Peter Steenkiste, Ozan K. Tonguz, and Joao Barros (2010), „Experimental Study on the Impact of Vehicular Obstructions in VANETs”
- [23] Rakesh Shrestha, Seung Yeob Nam, Rojeena Bajracharya, Shiho Kim (2020), „Evolution of V2X Communication and Integration of Blockchain for Security Enhancements”

-
- [24] The engine of broadband wireless innovation NGMN Alliance (2018), „**V2X White Paper**”
-
- [25] Federal Office of Communications OFCOM (Accessed 19.01.2023), „**ofcomnet – Frequency Allocation Plan**”
-
- [26] Electronic Communications Committee ECC (2020), „**Use of the band 5855-5875 MHz for Intelligent Transport Systems (ITS)**”
-
- [27] Electronic Communications Committee ECC (2019), „**Harmonised use of the 63.72-65.88 GHz frequency band for Intelligent Transport Systems (ITS)**”
-
- [28] EVITA (2008), „**E-safety vehicle intrusion protected applications**”, <https://evita-project.org/>
-
- [29] Project SCOOP (2016), „**Système Coopératif (SCOOP), Présentation du projet**”, <https://www.scoop.developpement-durable.gouv.fr>
-
- [30] Project SCOOP Seminar (2019), „**Seminar – 20th and 21st November 2019**”, <https://www.scoop.developpement-durable.gouv.fr>
-
- [31] ANSSI Guide (2019), „**EBIOS RISK MANAGER**”, <https://www.ssi.gouv.fr>
-
- [32] Daniel Cuthbert (March 16, 2023), „**What is Threat Modeling and How Does It Differ from Risk Assessment?**”, <https://www.pivotpointsecurity.com>
-
- [33] Open Web Application Security Project - OWASP (Accessed 13.04.2023), „**OWASP Threat Dragon**”, <https://owasp.org/www-project-threat-dragon/>
-
- [34] Paul Saitta, Brenda Larcom and Michael Eddington (July 13th, 2005), „**Trike v.1 Methodology Document**”, <https://www.octotrike.org>
-
- [35] Joseph Longo, Robin Schulman (Accessed 24.04.2023), „**Threat Modeling**”, <https://about.gitlab.com/>
-
- [36] Tony UcedaVélez (November 23, 2021), „**What is PASTA Threat Modeling?**”, <https://versprite.com/>
-
- [37] Threatmodeler (August 12, 2019), „**STRIDE, VAST, TRIKE, & MORE: WHICH THREAT MODELING METHODOLOGY IS RIGHT FOR YOUR ORGANIZATION?**”, <https://threatmodeler.com/>
-
- [38] SecV2IComm (Accessed 26.05.2023), „**SecV2IComm – Secured Vehicle-to-Infrastructure Communication**”, <https://www.heia-fr.ch/>
-
- [39] Parag Sewalkar and Jochen Seitz (January 17, 2019), „**Vehicle-to-Pedestrian Communication for Vulnerable Road Users: Survey, Design Considerations, and Challenges**”, <https://www.mdpi.com/>
-
- [40] Adam Hill (May 10, 2023), „**Austrian Bike2CAV V2X project could mark turning point in cyclist safety**”, <https://www.itsinternational.com/>
-
- [41] 5GAA Automotive Association (November 21, 2022), „**A visionary roadmap for advanced driving use cases, connectivity technologies, and radio spectrum needs**”, <https://5gaa.org/>
-

Projektabschluss



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement, des transports,
de l'énergie et de la communication DETEC
Office fédéral des routes OFROU

RECHERCHE DANS LE DOMAINE ROUTIER DU DETEC

Version du 09.10.2013

Formulaire N° 3 : Clôture du projet

établi / modifié le : 27.06.2023

Données de base

Projet N° : MB4_20_02C_01

Titre du projet : Cyber Threat Analysis Model for Cooperative Intelligent Transport System

Echéance effective : 30.06.2023

Textes :

Résumé des résultats du projet :

This research initially examined international literature to define the basic elements to analyze in terms of technology, security, regulations, and research status. Based on these elements, certain choices were made for the project's continuation:

- Technology: The research group decided to focus its efforts on V2X communications used between vehicles and road infrastructure. In Switzerland, this segment of C-ITS aims to be covered by the use of the C-V2X protocol. With access to C-ITS equipment (OBU and RSU) using the C-V2X and ITS-G5 protocols, the research group implemented a scenario involving connected traffic lights communicating their status and position to an autonomous vehicle. The vehicle adjusts its maneuvers based on this data. This scenario was used as the basis for the proof-of-concept to illustrate the feasibility of a real cybersecurity attack that could be prevented by proactively addressing these risks.
- Security: To identify threats and quantify the inherent risks in V2I (respectively I2V) communications, two choices were made:
 - For system/scenario modeling, Microsoft's open-source software "Microsoft Threat Modeling Tool" was used.
 - For identifying threats relevant to the modeled scenario, a specific template for C-ITS was developed using Microsoft's open-source software "Microsoft Threat Modeling Tool."
 - For risk analysis, the "Threat Analysis and Risk Assessment" (TARA) methodology proposed in the recent ISO/SAE 21434:2021 standard was used.

To assess the added value of such a threat model and its application to a C-ITS system, a parallel "traditional" risk analysis procedure was carried out manually, primarily based on expert judgment. These two approaches, tool-based and expert judgment-based, were compared to extract their advantages, disadvantages, and potential limitations. In summary, the tool-based approach has the main advantage of providing a certain level of automation, enabling the rapid generation of an extensive catalog of threats to consider. This automation is facilitated by the use and maturity of the C-ITS template developed as part of the project, which will continuously evolve to reflect the dynamic nature of the cyber threat landscape.

The expert judgment-based (human-based) approach, on the other hand, has the advantage of not introducing false positives into the threat catalog (e.g., existing generic threats that are not applicable to the specific system). However, the effort and expertise required for its application are significantly higher, making its viability critical in systems that aim to continuously evolve.

These findings led the research group to describe a "hybrid" approach that combines the advantages of both alternatives to maximize threat identification using the tool while minimizing the occurrence of false positives and adjusting risk criteria based on expert judgments. In addition to these aspects, this approach reduces the involvement of cybersecurity experts during the cyber risk analysis phase by integrating their knowledge into the C-ITS template, which can be used by potential non-experts.

In conclusion, the hybrid approach proposed by the research group proves to be pragmatic and provides a solid framework for proactive threat identification and analysis. It is evident that such an analysis cannot be exhaustive, and reactive approaches should also be considered to provide a management framework for the future detection of new threats and vulnerabilities. The evolution of technologies and attack methods will introduce new threats, and their handling will be decisive in maintaining a secure C-ITS environment in Switzerland.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement, des transports,
de l'énergie et de la communication DETEC
Office fédéral des routes OFROU

Atteinte des objectifs :

A preliminary threat catalogue based on heterogeneous sources (incl. standards, regulations, guidance, public databases and other research projects) has been created for responding the objectives of getting a identification of potential security vulnerabilities related to C-ITS.

In addition to this theoretical knowledge, an environment for modelling C-ITS environment and simulating cyber threats have been identified and tailored to the specificities of such mobility ecosystems. This tool, in conjunction with tailored templates developed by the research group, provides the capability to identify existing and potential future threats related to mobility concepts, architectures and technologies.

For supporting the analysis and interpretation of cyber threats, a complete "Threat Analysis and Risk Assessment" methodology has been proposed for enhancing risk quantification and enabling subsequent treatment decisions

As a summary, project results are fulfilling predefined objectives with some additional values raising from practical experiences and attacks performed in the context of side projects for validating results consistency

Déductions et recommandations :

Project has led to the following recommendations and considerations:

- It is strongly recommended to initiate the creation of cyber threat models related to innovative mobility concepts (incl. C-ITS) before any other considerations about implementation, in order to integrate cyber security as a major pillar of it (Security-by-design objective)
- It would be recommended to use such threat catalogue (and related cyber threat assessment methodology) for defining Swiss strategy against cyber threats across mobility sector. This might support the development of potential future legal and regulatory framework for secure C-ITS (similar to UN ECE R155 threats for Road Vehicles homologation).
- Threat catalogues and systematic cyber threat assessment approach should be communicated throughout Swiss mobility sector for education and awareness purpose.
- It is recommended to use such threat catalogue (and related cyber threat assessment methodology) as a knowledge baseline for developing reactive methods and potential related Security Operation Centers

Publications :

None

Chef/cheffe de projet :

Nom : Marty

Prénom : Kilian

Service, entreprise, institut : CertX SA

Signature du chef/de la cheffe de projet :



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement, des transports,
de l'énergie et de la communication DETEC
Office fédéral des routes OFROU

RECHERCHE DANS LE DOMAINE ROUTIER DU DETEC

Formulaire N° 3 : Clôture du projet

Appréciation de la commission de suivi :

Evaluation :

The research has explored existing risk assessment approaches, such as threat modelling using STRIDE methodology, for V2V and V2I communications. This project proposed to formalize a threat model template to be maintained continuously in order to keep a realistic view of threats against existing and upcoming C-ITS infrastructure. The research project objectives have been achieved.

Mise en oeuvre :

The threat catalogue and the threat assessment methodology could be used for the design of the swiss cyber-management C-ITS (e.g. for the swiss national PKI infrastructure).

Besoin supplémentaire en matière de recherche :

The Cyber threat analysis model could be extended to V2X (Vehicle to Everything). Real-time aspects could also be considered.

Influence sur les normes :

ISO 21217 - definition of the general architecture of ITS stations
GEN ISO/TR 21186-3 - security standard covers both broadcast and unicast communications
ISO/SAE 21434 - cybersecurity standard applied to road vehicles.
ISO/TR 21186-3:2021 - guidelines on security applicable in Intelligent Transport Systems (ITS) related to communications and data access.

Président/Présidente de la commission de suivi :

Nom : Ndzana

Prénom : Bertrand

Service, entreprise, institut : DETEC - OFROU

Signature du président/ de la présidente de la commission de suivi :