Ilona Loskin

TARA+AD: THREAT ANALYSIS AND RISK ASSESSMENT FOR AUTOMATED DRIVING

CYBERSECURITY OF ROAD VEHICLES

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2023

ABSTRACT

Loskin, Ilona
TARA+AD: Threat Analysis and Risk Assessment for Automated Driving – Cybersecurity of Road Vehicles
Jyväskylä: University of Jyväskylä, 2023, 154 p.
Information Systems Science, Master's Thesis
Supervisors: Hämäläinen, Timo; Siponen, Mikko

Cybersecurity of road vehicles has become a genuine matter as vehicles are not manufactured anymore as plain mechanical devices but containing numerous amounts of computers and millions of lines of code. The intelligent and safety-critical vehicular systems are prone to cyberattacks just like any other information system. It is evident that the vehicles need to be protected. A joint global working group prepared a new, international standard to cover the cybersecurity engineering in the automotive industry. The standard is called ISO/SAE JWG 21434 Road vehicles - Cybersecurity engineering. The new cybersecurity engineering standard defines the minimum criteria for cybersecurity of road vehicles which is also a demand by the United Nations Economic Commission for Europe (UNECE). The cybersecurity engineering standard gives requirements and recommendations what a security risk analysis of road vehicles should contain. The standard does not provide instructions how to perform the analysis. This research study targeted to find a threat analysis and risk assessment method which covers the requirements and recommendations of the cybersecurity engineering standard. Such singular method did not exist, thus a new analysis framework named TARA+AD (Threat Analysis and Risk Assessment for Automated Driving) was derived from the best features of two existing security risk analysis methods. The research method used was design science which aims to produce an artifact to resolve real-life problems. The artifact, TARA+AD, and the study was evaluated by using a Design Science Research Method (DSRM) process model. The new framework was tested by executing a use case related to vehicular communication which is the easiest interface to be attacked. The results were satisfactory as the new TARA+AD analysis framework solved the issue with performing a cybersecurity engineering standard compliant security risk analysis.

Keywords: cybersecurity of road vehicles, automated driving, threat analysis and risk assessment, ISO/SAE JWG 21434, design science research, intelligent vehicle, vehicular communication

TIIVISTELMÄ

Loskin, Ilona
TARA+AD: Uhkien analysointi ja riskien arviointi autonomisessa ajossa – Maantieajoneuvojen kyberturvallisuus
Jyväskylä: Jyväskylän yliopisto, 2023, 154 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaajat: Hämäläinen, Timo; Siponen, Mikko

Maantieajoneuvojen kyberturvallisuudesta on tullut todellinen asia, sillä ajoneuvoja ei valmisteta enää pelkkinä mekaanisina laitteina, vaan ne sisältävät lukuisia määriä tietokoneita ja miljoonia koodirivejä. Älykkäät ja turvallisuuskriittiset ajoneuvojärjestelmät ovat alttiita kyberhyökkäyksille kuten kaikki muutkin tietojärjestelmät. On selvää, että ajoneuvoja on suojeltava. Yhteinen globaali työryhmä valmisteli uuden kansainvälisen standardin kattamaan autoteollisuuden kyberturvallisuustekniikan. Standardin nimi on ISO/SAE JWG 21434 Road vehicles - Cybersecurity engineering (suomeksi: ISO/SAE JWG 21434 Maantieajoneuvot - Kyberturvallisuustekniikka). Uusi kyberturvallisuustekniikkastandardi määrittelee maantieajoneuvojen kyberturvallisuuden vähimmäiskriteerit, jota myös Yhdistyneiden kansakuntien Euroopan talouskomissio UNECE vaatii. Kyberturvallisuustekniikan standardi antaa vaatimuksia ja suosituksia, mitä tieliikenteen ajoneuvojen turvallisuusriskianalyysin tulee sisältää. Standardi ei anna ohjeita analyysin suorittamiseen. Tämän tutkimuksen tavoitteena oli löytää uhkien analysointi- ja riskien arviointimenetelmä, joka kattaa kyberturvallisuustekniikan standardin vaatimukset ja suositukset. Tällaista yksittäistä menetelmää ei ollut saatavilla, joten uusi analyysikehys nimeltä TARA+AD (Threat Analysis and Risk Assessment for Automated Driving) (suomeksi: uhkien analysointi ja riskien arviointi autonomisessa ajossa) johdettiin kahden olemassa olevan turvallisuusriskianalyysimenetelmän parhaista ominaisuuksista. Tutkimusmenetelmänä oli suunnittelutiede, jonka tavoitteena on tuottaa artefakti, eli jokin tuotos ratkaisemaan tosielämän ongelmia. Artefakti, TARA+AD, ja tutkimus arvioitiin Design Science Research Method (DSRM) -prosessimallilla (suomeksi: suunnittelutieteellinen tutkimusmenetelmä). Uutta viitekehystä testattiin suorittamalla ajoneuvoviestintään liittyvä käyttötapaus, sillä ajoneuvoviestintä on helpoin käyttöliittymä hyökkäyksille. Tulokset olivat vakuuttavia, sillä uusi TARA+AD -analyysikehys ratkaisi ongelman tarjoamalla kyberturvallisuustekniikan standardin mukaisen turvallisuusriskianalyysin.

Asiasanat: maantieajoneuvojen kyberturvallisuus, autonominen ajo, uhkien analysointi ja riskien arviointi, ISO/SAE JWG 21434, suunnittelutieteellinen tutkimus, älykäs ajoneuvo, ajoneuvoviestintä

TERMS AND DEFINITIONS

Term	Description	References
4G/LTE	Fourth generation of broadband cellular network technology / Long Term Evolution	Shen, X., Fantacci, R., & Chen, S. (2020). Internet of vehicles [scanning the issue]. *Proceedings of the IEEE, 108*(2), 242-245.
ACC	Adaptive Cruise Control	Lu, M., Wevers, K., & Van Der Heijden, R. (2005). Technical feasibility of advanced driver assistance systems (ADAS) for road traffic safety. *Transportation Planning and Technology, 28*(3), 167-187.
ACsIL	Automotive Cybersecurity Integrity Level	SAE. (2016c). J3061-1: Automotive Cybersecurity Integrity Level (ACsIL). *Society for automotive engineers*.
AD	Automated Driving	SAE. (2016a). J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. *Society for automotive engineers*.
ADAS	Advanced Driver Assistance Systems	Lu, M., Wevers, K., & Van Der Heijden, R. (2005). Technical feasibility of advanced driver assistance systems (ADAS) for road traffic safety. *Transportation Planning and Technology, 28*(3), 167-187.
ADS	Automated Driving System	SAE. (2016a). J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. *Society for automotive engineers*.
AI	Artificial Intelligence	General knowledge
Analysis template	MS Excel spreadsheet used for TARA+AD security risk analysis in practise.	Research study -based terminology
Artifact	"*Artifacts may include constructs, models, methods, and instantiations. They may also include social innovations or new properties of technical, social, or informational resources. In short, this definition includes any designed object with an embedded solution to an understood research problem.*"	Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems, 24*(3), 45-77.

(continues)

TERMS AND DEFINITIONS (continues)

ASIL	Automotive Safety Integrity Level	ISO, I. (2018). 26262: Road vehicles-Functional safety. *International Standard ISO/FDIS*, 26262.
Automotive Ethernet	Ethernet-based network communications protocol	Smith, C. (2016). *The Car Hacker's Handbook: A Guide for the Penetration Tester*. No Starch Press.
BRA	Binary Risk Analysis	Sapiro, B. (2011) Binary Risk Analysis. *Creative Commons License, 1*.
BT	Bluetooth	General knowledge
C-V2X	Cellular Vehicle-to-Everything	Alalewi, A., Dayoub, I., & Cherkaoui, S. (2021). On 5G-V2X use cases and enabling technologies: A comprehensive survey. *IEEE Access, 9*, 107710-107737.
CACS	Comprehensive Automobile Traffic Control System	Matsumoto, S., Mikami, T., Yumoto, N., & Tabe, T. (1979). Comprehensive automobile traffic control system. *J. of IECE, 62*(8), 870-887.
CAL	Cybersecurity Assurance Level	ISO/SAE, (2020). 21434: Road vehicles-Cybersecurity engineering. *International Standard ISO/Society for automotive engineers SAE*.
CAN	Controller Area Network	Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., ... & Kohno, T. (2011, August). Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *USENIX Security Symposium* (Vol. 4, pp. 447-462).
Car	Vehicle in US	General knowledge
CIA	Confidentiality, Integrity and Availability model	SAE. (2016b). J3061: Cybersecurity guidebook for cyber-physical vehicle systems. *Society for automotive engineers*. ISO/SAE, (2020). 21434: Road vehicles-Cybersecurity engineering. *International Standard ISO/Society for automotive engineers SAE*.

(continues)

TERMS AND DEFINITIONS (continues)

Comparison Matrix	MS Excel spreadsheet used for checking how well the chosen security risk analysis methods cover the requirements and recommendations from the cybersecurity engineering standard.	Research study -based terminology
CPS	Cyber-physical Systems	Baheti, R., & Gill, H. (2011). Cyber-physical systems. *The impact of control technology, 12*(1), 161-166.
CPVS	Cyber-physical Vehicle Systems	Bradley, J. M., & Atkins, E. M. (2015). Optimization and control of cyber-physical vehicle systems. *Sensors, 15*(9), 23020-23049.
DIS	Draft International Standard version	https://en.wikipedia.org/wiki/International_Organization_for_Standardization
DREAD	Damage Potential, Reproducibility, Exploitability, Affected Users and Discoverability	Macher, G., Armengaud, E., Brenner, E., & Kreiner, C. (2016b). Threat and risk assessment methodologies in the automotive domain. *Procedia computer science, 83*, 1288-1294.
DS	Design Science	Simon, H. A. (1996). The sciences of the artificial. MIT Press. *Cambridge, MA*.
DSR	Design Science Research	Vaishnavi, V., Kuechler, W., & Petter, S. (2004/2019). Design science research in information systems. *January, 20*, 2004.
DSRC	Dedicated Short-Range Communication	Smith, C. (2016). *The Car Hacker's Handbook: A Guide for the Penetration Tester*. No Starch Press.
DSRM	Design Science Research Method	Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems, 24*(3), 45-77.
(E/E) systems	Electrical and/or electronic systems	ISO, I. (2018). 26262: Road vehicles-Functional safety. *International Standard ISO/FDIS*, 26262.
ECU	Electronic Control Unit	Charette, R. N. (2009). This car runs on code. *IEEE spectrum, 46*(3), 3.

(continues)

TERMS AND DEFINITIONS (continues)

ETSI	European Telecommunications Standards Institute	ETSI (2010). *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis* (Report TS 102 165-1 V4.2.x). European Telecommunications Standards Institute.
EVITA	E-Safety Vehicle Intrusion Protected Applications	Ruddle, A., Ward, D., Weyl, B., Idrees, S., Roudier, Y., Friedewald, M., ... & Wolf, M. (2009). Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios. *EVITA project*.
ERGS	Electronic Route Guidance System	Dong, W. (2011, September). An overview of in-vehicle route guidance system. In *Australasian Transport Research Forum* (Vol. 2011).
FCA	Forward Collision Avoidance	Lu, M., Wevers, K., & Van Der Heijden, R. (2005). Technical feasibility of advanced driver assistance systems (ADAS) for road traffic safety. *Transportation Planning and Technology, 28*(3), 167-187.
FDIS	Final draft international standard	https://en.wikipedia.org/wiki/International_Organization_for_Standardization
FlexRay	High-speed network communications protocol	Smith, C. (2016). *The Car Hacker's Handbook: A Guide for the Penetration Tester*. No Starch Press.
FuSa	Functional Safety	ISO, I. (2018). 26262: Road vehicles-Functional safety. *International Standard ISO/FDIS*, 26262.
General instructions	MS Word document used for elaborating the general guidance of the activities of the TARA+AD security risk analysis framework.	Research study -based terminology
GNSS	Global Navigation Satellite Systems	Onishi, H., Wu, K., Yoshida, K., & Kato, T. (2017). Approaches for vehicle cyber-security in the US. *International Journal of Automotive Engineering, 8*(1), 1-6.
GPS	Global Positioning System	General knowledge
GSM	Global System for Mobile Communications	General knowledge

(continues)

TERMS AND DEFINITIONS (continues)

Hacker	In this study used in the use case; a person who steals company equipment and tries to intrude to company systems by pretending to be an employee or uses his/her own equipment and utilizes malicious programs to infiltrate the company systems.	Research study -based terminology
HARA	Hazard Analysis and Risk Assessment	ISO, I. (2018). 26262: Road vehicles-Functional safety. *International Standard ISO/FDIS*, 26262.
Hazard	"*Potential source of harm caused by malfunctioning behaviour of the item.*"	ISO, I. (2018). 26262: Road vehicles-Functional safety. *International Standard ISO/FDIS*, 26262.
HEAVENS	HEAling Vulnerabilities to ENhance Software Security and Safety	Lautenbach, A., & Islam, M. (2016). HEAVENS–HEAling Vulnerabilities to ENhance Software Security and Safety. *The HEAVENS Consortium (Borås SE)*.
HLC	High Level Controller	Virtual Vehicle (2020b). *Item Definition - "SPIDER"*. (Project: SPIDER, Version: V1.0). Virtual Vehicle, 1.7.2020.
HW	Hardware	General knowledge
ICA	Intersection Collision Avoidance	Lu, M., Wevers, K., & Van Der Heijden, R. (2005). Technical feasibility of advanced driver assistance systems (ADAS) for road traffic safety. *Transportation Planning and Technology, 28*(3), 167-187.
IEC	International Electrotechnical Commission	https://www.iec.ch/homepage
IS	Information Systems	General knowledge
IoT	Internet of Things	Wortmann, F., & Flüchter, K. (2015). Internet of things. *Business & Information Systems Engineering, 57*(3), 221-224.
IoV	Internet of Vehicles	Rahim, M. A., Rahman, M. A., Rahman, M. M., Asyhari, A. T., Bhuiyan, M. Z. A., & Ramasamy, D. (2021). Evolution of IoT-enabled connectivity and applications in automotive industry: A review. *Vehicular Communications, 27*, 100285.
ISO	International Organization for Standardization	https://www.iso.org/home.html

(continues)

TERMS AND DEFINITIONS (continues)

ISO 26262	Functional Safety	ISO, I. (2018). 26262: Road vehicles-Functional safety. *International Standard ISO/FDIS*, 26262.
ISO/SAE JWG 21434	Road vehicles - Cybersecurity engineering	ISO/SAE, (2020). 21434: Road vehicles-Cybersecurity engineering. *International Standard ISO/Society for automotive engineers SAE*.
IT	Information Technology	General knowledge
ITS	Intelligent Transportation System	Smith, C. (2016). *The Car Hacker's Handbook: A Guide for the Penetration Tester*. No Starch Press.
LiDAR	Light Detection and Ranging	Here: Virtual Vehicle (2020b). *Item Definition - "SPIDER"*. (Project: SPIDER, Version: V1.0). Virtual Vehicle, 1.7.2020.
MoRA	Modular Risk Assessment	Angermeier, D., Beilke, K., Hansch, G., & Eichler, J. (2019). Modeling security risk assessments.
MSTMT	Microsoft Threat Modeling Tool	https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool
NHTSA	US National Highway Traffic Safety Administration	https://www.nhtsa.gov/
OBD	On-Board Diagnostics	Charette, R. N. (2009). This car runs on code. *IEEE spectrum, 46*(3), 3.
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation	Alberts, C. J., Behrens, S. G., Pethia, R. D., & Wilson, W. R. (1999). *Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, Version 1.0*. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.
Operator Panel	In this study, the user interface program to operate the SPIDER robot vehicle.	Research study -based terminology
PASTA	Process for Attack Simulation and Threat Analysis	UcedaVelez, T., & Morana, M. M. (2015). *Risk Centric Threat Modeling: process for attack simulation and threat analysis*. John Wiley & Sons.
PLS	Physical Layer Security	Furqan, H. M., Solaija, M. S. J., Hamamreh, J. M., & Arslan, H. (2019). Intelligent physical layer security approach for V2X communication. *arXiv preprint arXiv:1905.05075*.

(continues)

TERMS AND DEFINITIONS (continues)

Requirements' elaboration	MS Word document used for elaborating the requirements, recommendations, and terms of the cybersecurity engineering standard.	Research study -based terminology
RFID	Radio Frequency Identification	Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and microsystems, 77*, 103201.
Road vehicles	Passenger cars, trucks, buses, trailers, and motorcycles, excluding mopeds.	ISO, I. (2018). 26262: Road vehicles-Functional safety. *International Standard ISO/FDIS*, 26262.
ROS	Robot Operating System	Virtual Vehicle (2020b). *Item Definition - "SPIDER"*. (Project: SPIDER, Version: V1.0). Virtual Vehicle, 1.7.2020.
SAE	Society of Automotive Engineers	https://www.sae.org/
SAE J3016	Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems	SAE. (2016a). J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. *Society for automotive engineers*.
SAE J3061	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems	SAE. (2016b). J3061: Cybersecurity guidebook for cyber-physical vehicle systems. *Society for automotive engineers*.
SAHARA	Security Aware Hazard Analysis and Risk Assessment	Macher, G., Sporer, H., Berlach, R., Armengaud, E., & Kreiner, C. (2015, March). SAHARA: a security-aware hazard and risk analysis method. In *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)* (pp. 621-624). IEEE.
SARA	Security Automotive Risk Analysis	Monteuuis, J. P., Boudguiga, A., Zhang, J., Labiod, H., Servel, A., & Urien, P. (2018, May). Sara: Security automotive risk analysis method. In *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security* (pp. 3-14).

(continues)

TERMS AND DEFINITIONS (continues)

SINA	Security in Networked Automotive Systems	Schmidt, K., Tröger, P., Kroll, H. M., Bünger, T., Krueger, F., & Neuhaus, C. (2014). Adapted development process for security in networked automotive systems. *SAE International Journal of Passenger Cars-Electronic and Electrical Systems, 7*(2014-01-0334), 516-526.
SPIDER	Smart PhysIcal Demonstration and Evaluation Robot	https://www.v2c2.at/spider
STRIDE	Spoofing Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege	Microsoft Corporation. (2005). The STRIDE Threat Model.
STRIDE(LC)	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege, Linkability, Confusion.	Monteuuis, J. P., Boudguiga, A., Zhang, J., Labiod, H., Servel, A., & Urien, P. (2018, May). Sara: Security automotive risk analysis method. In *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security* (pp. 3-14).
SW	Software	General knowledge
SysML	Systems Modeling Language	https://sysml.org/
TARA	Threat Analysis and Risk Assessment	SAE. (2016b). J3061: Cybersecurity guidebook for cyber-physical vehicle systems. *Society for automotive engineers*.
TARA+	Controllability-aware Threat Analysis and Risk Assessment	Bolovinou, A., Atmaca, U. I., Sheik, A. T., Ur-Rehman, O., Wallraf, G., & Amditis, A. (2019, June). TARA+: Controllability-aware Threat Analysis and Risk Assessment for L3 Automated Driving Systems. In *2019 IEEE Intelligent Vehicles Symposium (IV)* (pp. 8-13). IEEE.
TARA+AD	Threat Analysis and Risk Assessment for Automated Driving	Research study -based terminology
TARA by MITRE corporation	Threat Assessment & Remediation Analysis by MITRE corporation	Wynn, J., Whitmore, J., Upton, G., Spriggs, L., McKinnon, D., McInnes, R., ... & Clausen, L. (2011). *Threat assessment & remediation analysis (tara): Methodology description version 1.0* (No. MTR110176). MITRE CORP BEDFORD MA.
TARA Intel	Threat Agent Risk Assessment	Rosenquist, M. (2009). Prioritizing information security risks with threat agent risk assessment. *Intel Corporation White Paper*.

(continues)

TERMS AND DEFINITIONS (continues)

THROP	Threat and Operability Analysis	SAE. (2016a). J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. *Society for automotive engineers*.
TVRA	Threat, Vulnerability and Risk Assessment	ETSI (2010). *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis* (Report TS 102 165-1 V4.2.x). European Telecommunications Standards Institute.
UC	Use case	General knowledge
UNECE	United Nations Economic Commission for Europe	https://unece.org/
V2C	Vehicle-to-Cloud	RGBSI (2020). *Driving Change: The Future of Mobility* (Whitepaper). Rapid Global Business Solutions, Engineering Solutions.
V2D	Vehicle-to-Device	RGBSI (2020). *Driving Change: The Future of Mobility* (Whitepaper). Rapid Global Business Solutions, Engineering Solutions.
V2G	Vehicle-to-Grid	RGBSI (2020). *Driving Change: The Future of Mobility* (Whitepaper). Rapid Global Business Solutions, Engineering Solutions.
V2I	Vehicle-to-Infrastructure	Smith, C. (2016). *The Car Hacker's Handbook: A Guide for the Penetration Tester*. No Starch Press.
V2N	Vehicle-to-Network	RGBSI (2020). *Driving Change: The Future of Mobility* (Whitepaper). Rapid Global Business Solutions, Engineering Solutions.
V2P	Vehicle-to-Pedestrian	Harding, J., Powell, G., R., Yoon, R., Fikentscher, J., Doyle, C., Sade, D., Lukuc, M., Simons, J., & Wang, J. (2014, August). *Vehicle-to-vehicle communications: Readiness of V2V technology for application*. (Report No. DOT HS 812 014). Washington, DC: National Highway Traffic Safety Administration.
V2V	Vehicle-to-Vehicle	Smith, C. (2016). *The Car Hacker's Handbook: A Guide for the Penetration Tester*. No Starch Press.

(continues)

TERMS AND DEFINITIONS (continues)

V2X	Vehicle-to-Everything	Rahim, M. A., Rahman, M. A., Rahman, M. M., Asyhari, A. T., Bhuiyan, M. Z. A., & Ramasamy, D. (2021). Evolution of IoT-enabled connectivity and applications in automotive industry: A review. *Vehicular Communications, 27*, 100285.
VANET	Vehicular ad hoc network	Alalewi, A., Dayoub, I., & Cherkaoui, S. (2021). On 5G-V2X use cases and enabling technologies: A comprehensive survey. *IEEE Access, 9*, 107710-107737.
Vehicle	Term *vehicle* chosen over term *car* in the study, as vehicle is more standard in Europe.	Research study -based terminology
WiFi	Wireless networking technology	General knowledge
WiFi AP	WiFi Access Point	Virtual Vehicle (2020b). *Item Definition - "SPIDER"*. (Project: SPIDER, Version: V1.0). Virtual Vehicle, 1.7.2020.

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

Road vehicles have been mass-produced through the past 80 years as mechanical devices. Only until a couple of decades ago the direction of the development focused to make vehicles to contain numerous amounts of computers and myriad lines of code. Along the development appeared also new kind of threats such as cyberattacks to vehicles' safety-critical systems. (Koscher et al., 2010; Charette, 2009; Checkoway et al., 2011.) If the cybersecurity of the transportation domain follows the trends of the internet, we might be able to witness cyberattacks in the automotive domain. The motivation for hacking a vehicle is seen mostly as an attempt to gain financial benefit with chip tuning or odometer rollback. The possible further step causing harm or even an accident to the passengers, might get easier to take. (Weimerskirch & Gaynier, 2015.)

The research study examines background theories of functional safety and related cybersecurity standards, technical reports, and guidebooks of road vehicles. The target is to gather requirements for a security risk analysis validated with a chosen security risk analysis method. Automotive domain is highly regulated by different standards thus standards are a vital part of the study while investigating the requirements and metrics for the solution concept creation (ISO, 2021).

The study discusses what kind of interfaces there are between a vehicle and the outside world that can be attacked by the means of hijacking, cyberattacking, disturbing and infiltrating. The main interface for attacks is related to vehicular communication, both internal and external. (Doms et al., 2018.)

The research study was originated from an Austrian research center called Virtual Vehicle Research Gmbh (later: Virtual Vehicle) focusing on road vehicle technology in the automotive domain. The study was conducted as per the assignment from Virtual Vehicle.

1.1 Backgrounds and Motivations

The world of today is digitalizing everyday life functions increasingly in different domains like IT, healthcare, automotive, maritime and avionics. Not only have we smaller scale of IoT (Internet of Things) products like smartphones, smart wristbands, and smart blood pressure meters, but the development is broadening into bigger scale as well with cyber-physical systems (CPS) (Farooq, Waseem, Mazhar, Khairi & Kamal, 2015; Wortmann & Flüchter, 2015; Baheti & Gill, 2011). In the future there will be driverless self-driving vehicles. The concern with independently navigating and moving vehicles lands to safety and security issues which are among the primary priorities to investigate in this new evolving technology. (Schoitsch, Schmittner, Ma & Gruber, 2016.) Automated driving is part of the future and connected with cyber-physical systems and IoT in the automotive domain. Automated driving as a concept is based on the definition of ADS (Automated Driving System) levels (SAE, 2016a). The five ADS levels describe vehicular operations which are monitored and executed either by a human driver or a driverless system. (SAE, 2016a; Litman, 2017; Doms et al., 2018.)

Road vehicles like cars, trucks, buses, trailers, and motorcycles, contain embedded micro-processors which are integrated in Electronic Control Units (ECUs) and software that has millions of lines of code which work together with vehicle's functions like brakes (Charette, 2009). This kind of system in the vehicle must be safe in the sense that any failure in the system shall never lead to harm people. There are safety and security risks in such systems and all the derived measures can only be used for risk reduction because systems can never be 100% secure or 100% safe. (Smith & Simpson, 2010; Sommerville, 2016; Ebert, 2017.) The ambition is to make the systems as secure and safe as possible. Functional safety standard (ISO 26262) covers road vehicles' functional safety and provides requirements and recommendations for the entire product lifecycle covering management, development, production and further on operation and decommissioning. (ISO, 2018.)

The automotive domain is already affected by cyberthreats; thus, a joint global working group has prepared a new, international standard to cover the cybersecurity engineering in the automotive industry. The new standard is based on another cybersecurity related guidebook (SAE, 2016b). One of the main objectives of the new cybersecurity engineering standard is to define the minimum criteria for cybersecurity of road vehicles which is also a demand by the UNECE (United Nations Economic Commission for Europe) (UNECE, 2021a). Another major target of the new standard is to harmonize and unify the terminology across the automotive industry and provide a process framework for cybersecurity engineering. (Akram, 2019; ISO/SAE, 2020.)

One of the essential features of road vehicles which can be breached is communication. Automated driving requires secure communication between different instances like other vehicles and infrastructure such as buildings,

traffic lights and traffic signs. Without communication a vehicle cannot perform automated driving operations. The vehicular communication systems have evolved from Bluetooth, GSM, and WiFi (Wolf, Weimerskirch & Paar, 2006) to Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) technologies. (Smith, 2016.) It is essential to investigate the different vehicular communication systems and technologies to address the interfaces where a cyberbreach could occur.

1.2 Research Objectives

The prime objective of the research study is to discover an automotive compatible security risk analysis method which meets the assignment's expectations and fulfils the requirements of the cybersecurity engineering standard. To accomplish the prime objective, an evaluation of existing risk analysis method approaches for the required needs is carried out. The main point is if any existing approach can fulfil the needs or should some of the approaches be improved.

The second objective of the study is to validate that the chosen security risk analysis method meets the set criteria from the cybersecurity engineering standard. There are specific requirements defined in the new standard and the study aims to evaluate if the existing risk analysis methods could be utilized to reflect those requirements. The purpose is to evaluate the elaborated approach including the method and identifying the impact on functional safety of a vehicle.

The study aims to publish the results concerning the security risk analysis to provide up-to-date information how to implement cybersecurity engineering in early design phases and which method is the most suitable for the security risk analysis.

1.3 The Scope of the Research

The main scope of the study is to explore the security impact on road vehicle safety and the negative effects on human life, loss of reputation, financial losses, legal violations, loss of intellectual property, damaging critical infrastructure and so on. The target is to evaluate methods for security risk analysis in early road vehicle design phase and elaborate the impact of cybersecurity on functional safety in the automotive domain. The chosen security risk analysis method will be validated with a use case execution and evaluation.

The focus of the study is on automated driving where a licensed human driver is not required inside the vehicle. This scenario covers the levels 4 and 5 of the five automated driving levels defined in the automation level technical report SAE J3016. (SAE, 2016a; Litman, 2017; Doms et al., 2018.)

A human aspect in the study is outlined to cover the safety of human lives when designing the security features of road vehicles. The focus is on the system-level features and what kind of impact there can be if a cyberattack occurs. Different human created cyberattack scenarios are to be defined and discussed in the study.

In addition to technical report SAE J3016 which covers the definition of automated driving, another set of standards and a guidebook are discussed in the study concerning functional safety (ISO 26262) and cybersecurity (SAE J3061 and ISO/SAE JWG 21434). The focus is on the interface outside the vehicle but not the outside world which is defined by other standards.

The development of driverless, independent, and high-level of driving autonomy vehicles transporting human passengers is already happening. Such vehicles have full autonomy without any human interaction. However, this topic is quite distant in the future to be covered in the research study thus it is out of scope. The scenarios of a hacker inside a vehicle manipulating or influencing the vehicle's safety features are excluded from the study as well as threatening behaviour and harmful actions of an incautious driver. The study focuses only into early development phases of road vehicles and does not discuss the human behaviour aspect. Hardware and software levels of the functional safety standard ISO 26262 are out of scope as the study focuses only on system level (functional/technical). Ethics of automated driving and independent vehicles is also out of scope as it would be too wide to be covered efficiently.

1.4 Research Problems

The new standard ISO/SAE 21434 concerning cybersecurity engineering of road vehicles was released in early 2020 and as such, there was no previous studies concerning a security analysis of the brand-new standard when the study was conducted. The new standard has been developed since 2016 by experts from ISO (International Organization for Standardization) and SAE (Society of Automotive Engineers) organizations involving different companies and manufacturers, thus all members have their own interest what should be defined in the standard. (Schmittner, Griessnig & Ma, 2018.) The study is conducted for the initial version of the standard and can be revised in possible later versions.

ISO/SAE 21434 aims to provide a starting point and an official reference for vehicular cybersecurity. The standard defines a common terminology so that different operators in the automotive domain can better understand each other. The standard gives the minimum criteria for cybersecurity in a vehicle and defines security assurance levels for metrics and analysis purposes. With the new cybersecurity engineering standard, the vehicle manufacturers can

make sure their products are sufficiently secured when driving on the roads. (Akram, 2019.)

The cybersecurity engineering standard does not provide an exact schema how to perform a security risk analysis from start to end as one entity. The guidance gets shattered when instructions and suggestions are spread into different sections and annexes. The standard indicates that TARA, Threat Analysis and Risk Assessment (SAE, 2016b) framework is the basis of the security risk analysis, but very few TARA based methods are mentioned. This leads to the research problem: how to make a TARA based and cybersecurity engineering standard compliant security risk analysis for road vehicles. The solution requires a security risk analysis method with detailed instructions, and an equivalent tool to perform the analysis in a comprehensive manner.

The research questions proposed in the study are:

Research Question #1:
Which existing risk analysis methods cover the requirements regarding security risk analysis in the standard ISO/SAE JWG 21434?

Research Question #2:
How could a standard compatible security risk analysis method look like in the early design phase?

Research question 1 aims to discover the potential risk analysis methods in the automotive domain from the documentation of the standards and in the academic literature. Research question 2 aims to provide the best possible risk analysis method and related tool which will fulfil the requirements of the cybersecurity engineering standard.

1.5 Research Methodology and Results

The design of the study contains three parts: 1) finding a security risk analysis method which meets the requirements of the cybersecurity engineering standard (*Comparison of the different TARA approaches*), 2) modelling of the cybersecurity engineering standard compliant analysis framework together with a security risk analysis template (*Elaboration of the new approach*), and 3) use case creation and execution with the derived security risk analysis template (*Application of the specific approach for the UC*). The chosen research method is Design Science (DS) (Simon, 1996) as the study targeted to produce an artifact (March & Smith, 1995) to solve the research problem. The chosen evaluation approach for the study is Design Science Research Method (DSRM) created by Peffers et al. (2007). The DSRM process model was used to describe and evaluate the study's progress and outcome.

A new analysis framework was developed as the artifact: TARA+AD. The AD stands for Automated Driving which refers to the automated driving features (SAE, 2016a). TARA+AD follows the exact form and sequence of the cybersecurity engineering standard's (ISO/SAE, 2020) requirements and recommendations. The necessary parts of SARA (Monteuuis et al., 2018) and TARA+ (Bolovinou et al., 2019) methods are matched to the cybersecurity engineering standard. TARA+AD acts as a framework providing a larger concept and guidance how to perform a security risk analysis instead of being a method that gives steps how to perform a certain task (Vaishnavi et al., 2004/2019).

TARA+AD analysis framework addresses the need for threat and risk analysis required by the cybersecurity engineering standard. The framework is illustrated with a diagram of the analysis flow and related activities, tasks, and sub-tasks. The framework provides general instructions and an analysis template for the actual security risk analysis. The general instructions and analysis template are company confidential, but the information used to these products is public and can be gathered for a tool creation by any instance.

1.6 The Structure of the Research Study

The study consists of four main sections gathering the related chapters under them. The sections and related chapters are presented in the following figure (figure 1).

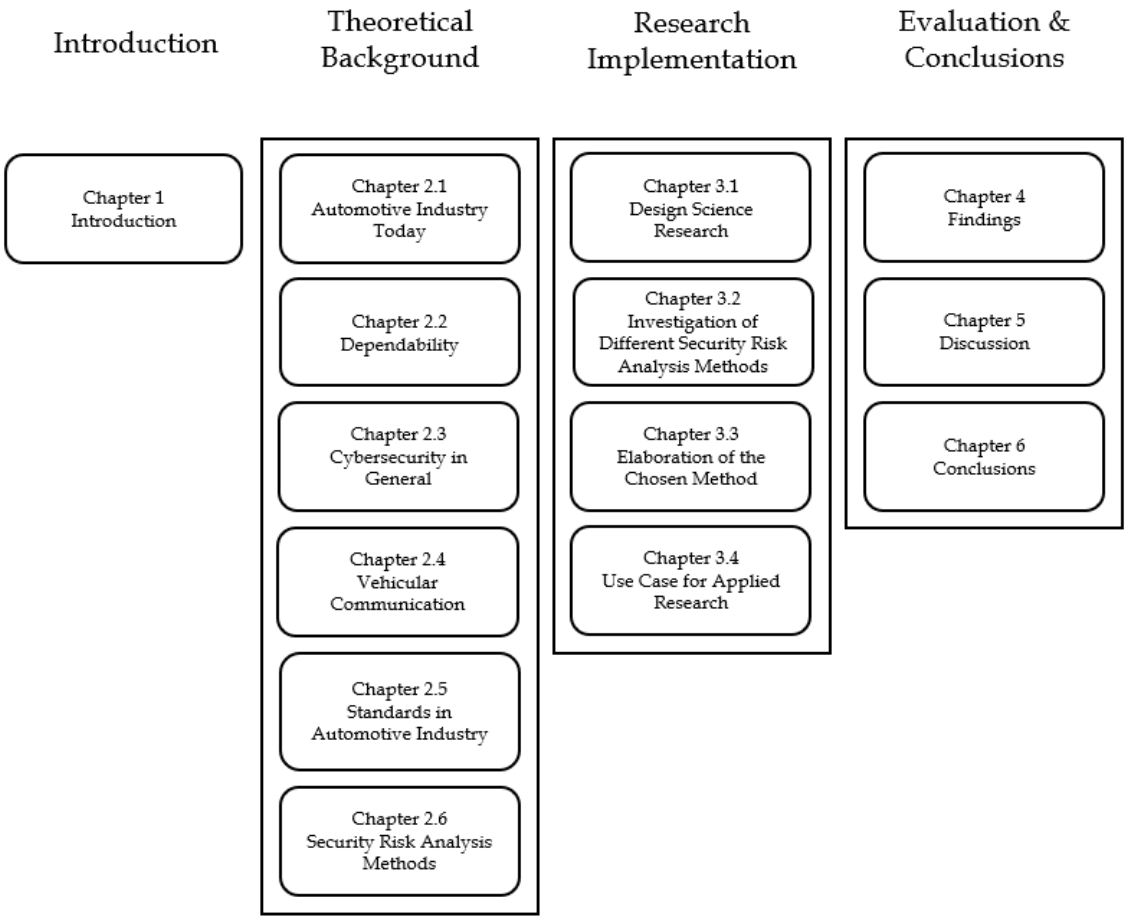

FIGURE 1 The structure of the research study

Introduction presents the background of the study and the motivation for the research. Research objectives and the scope are discussed, and research problems along with research questions are elaborated. Research methodology and results are presented, and the structure of the study is illustrated and shortly described.

Theoretical Background discusses the main concepts of the study. Dependability is strongly related to Information Technology domain. As automotive industry is following the path of the internet, the basics of Cybersecurity, Internet of Things, Cyber-Physical Systems and Cyber-Physical Vehicle Systems are elaborated. Vehicular communication discusses the interfaces of internal and external communication technologies that can be breached. The other half of the chapter elaborates how the chosen standards are referenced in the study and what are the key standards related to automotive cybersecurity. A short introduction to security risk analysis methods is given.

Research Implementation discusses how the research was conducted and what methodology was used. The design science research chapter describes the

different approaches how to define and evaluate design science research and introduces the concept of an artifact. The rest of the chapters focus on the investigation and evaluation of different security risk analysis methods, elaboration of the chosen method and the creation of the new approach. For the evaluation of the new approach, a use case is created and executed, and the outcome is presented.

Evaluation & Conclusions consists of three chapters. Chapter 4 titled *Findings* presents the principles of the DSRM (Design Science Research Method) process model, how the data was gathered, analysed, and further elaborated to meet the set targets. The results are examined from three aspects: 1) the comparison of the different security risk analysis methods, 2) the implementation part consisting of elaboration of the new approach, and 3) the application of the new approach with the use case. The artifact is presented, examined, and justified.

Chapter 5 titled *Discussion* reflects the research problems and answers the research questions. The findings are discussed, and the implications to research and to practice are argued.

Chapter 6 titled *Conclusions* discusses the summary of the study and the contribution, presents the limitations of the study, and proposes further research topics.

2 THEORETICAL BACKGROUND

This chapter discusses the automotive industry today and the related concepts of functional safety, cybersecurity, dependability, and vehicular communication. The study-centric standards in the automotive domain are elaborated and the related standard referencing procedure is presented. Finally, a brief introduction to security risk analysis methods is given.

2.1 Automotive Industry Today

Vehicles manufactured today are not anymore plain mechanical devices but intelligent and automated computational instruments on wheels. How can then automated driving be protected from hardware and software failures in view of safety and security? The question is worth studying as cyber-physical systems (CPS) such as self-driving road vehicles are being developed in increasing amounts. (Schoitsch et al., 2016.) One of the targets is to ensure the safety and security issues of these cyber-physical systems. A major area of CPS is the automated driving which has been evolving for the past few years. The studies related to automated driving and cybersecurity are thus very new. There exists different warning systems, parking aids and lane-keeping programs for vehicles and the fully automated driving is predicted to be real in the next 10 or 20 years. (Anderson et al., 2014; Hars, 2016.)

One aspect that emerges when discussing about the safety and security of automated driving is the impact of cybersecurity to functional safety. Functional safety means failures derived from hardware, system and software which can cause injuries and loss of human lives. The general approach of functional safety is to ensure that the car electronics are safe. In practice this means that the steering works, acceleration is under control and brakes brake. The functional safety and cybersecurity in the automotive domain have been researched by Burton, Likkei, Vembar & Wolf (2012), Czerny (2013) and Glas et al. (2015). Burton et al. (2012) discusses the existence of a third kind of source

causing hazards on top of hardware faults and software failures. The third source being malicious attacks and manipulation of the vehicles' electrical/electronic (E/E) control systems. Czerny (2013) addresses that the automotive systems have been classified as embedded systems, but the terminology is moving to the direction of calling these systems as cyber-physical automotive systems because of cybersecurity involvement. Vehicles, like passenger cars, have programmed systems which can be or are in connection with IoT (Internet of Things), and both external and internal networks. This exposes the systems under hacking and malicious attacks causing the vehicle having functional safety and security issues. The consequences of security issues have different effects of financial, operational, safety and privacy matters. The consequences can mean loss of reputation and damage to critical infrastructure, but also posing threat to human life. (Glas et al., 2015.) The three studies indicate that the vehicular networks, both internal and external, are the most potential interfaces for cyberattacks.

2.2 Dependability

Dependability at its simplest definition is making something reliable and trustworthy. Dependability, and security, are discussed when dealing with computing and communication systems thus it applies to vehicles with automated driving capabilities. Automated driving refers to a transportation mode of a vehicle with less manual interaction from the driver. Automated driving requires intelligent vehicles which contain system algorithms that understand the environment around and can act accordingly. (Bishop, 2000; Kyriakidis, Happee & de Winter, 2015.) Intelligent vehicles have dependable systems which aim to avoid service failures and gain trust. The attributes of a dependable system are reliability, availability, safety, integrity, and maintainability. Security plays a key role together with dependable systems. Security holds the attributes of confidentiality, availability, and integrity which are often called as CIA, and security aims to protect authorized access only. The threats to dependability and security are faults, errors, and failures. (Avizienis, Laprie, Randell & Landwehr, 2004; Jonsson, 2006.)

Dependability in the study context is related to system protection and preventing different failures in view of vehicular cybersecurity. While Chemweno, Pintelon, Muchiri and Van Horenbeek (2018) and kamal Kaur, Pandey and Singh (2018) discuss the ever-growing utilization of technology in the societies and different industries in their studies concerning risk assessment of dependability, Macher et al. (2021) address the concern of dependability in the automotive domain. All scholars agree on fault prevention, fault tolerance, fault removal and fault forecasting of critical systems and evaluate and apply existing security risk analysis methods. Security risk analysis methods are discussed further in the study.

2.3 Cybersecurity in General

Modern-day world is highly digitalized in all segments of human life, societies, infrastructure, education, business, military, and governments in the post-industrialized countries (Cavelty, 2015; Costigan & Hennessy, 2016). Humankind is largely dependent on information technology and the internet. Computers, smartphones, tablets, wearable devices, and household appliances are all connected. Anything that is connected, can be breached. (Singer & Friedman, 2014; Jang-Jaccard & Nepal, 2014; Cavelty, 2015.) Cybersecurity as a concept can be described with various definitions. Craigen, Diakun-Thibault and Purse (2014) argue in their study about defining cybersecurity that the definitions can be often uninformative and subjective. Singer and Friedman (2014) note that common people might often think that cybersecurity is something that only IT experts understand. Cybersecurity is however everyman's business. A rough portrayal of cybersecurity is humans with machines attacking humans protecting machines (Craigen et al., 2014). When cybersecurity gets compromised, it means that the confidentiality, integrity, and/or availability of information and communication systems is jeopardized. An example of such cybersecurity breach is unauthorised access into secured network or phishing sensitive information like passwords via email. (Shaikh & Siponen, 2023.)

The core of cybersecurity is about risk management, vulnerability patching and system resilience improvement. Cybersecurity concerns today road vehicles as they contain computational technology and are connected e.g., via smartphones. (Lehto & Neittaanmäki, 2015.) Carry-in devices are not the only threat to automotive cybersecurity. Global Navigation Satellite Systems (GNSS) and emerging communication technologies like Vehicle-To-Vehicle (V2V) are a matter of concern. (Onishi, Wu, Yoshida & Kato, 2017.) The most potential interfaces of road vehicles to be breached are discussed further in the study in vehicular communication section.

2.3.1 Internet of Things (IoT)

Internet of Things aka IoT is a term used when products and services are connected to internet, and they can be reached and controlled over the internet (Wortmann & Flüchter, 2015). Examples of IoT are smart domestic appliances such as refrigerators which keep track of the food supplies and washing machines that can be controlled with a mobile app (Pa et al., 2015). Another set of IoT devices are products monitoring and enhancing health such as wearable technologies and blood sugar censors (Farooq et al., 2015). IoT does not narrow only to individuals' use of technology, but in larger scale as well. Surveillance drones are utilized to provide data to city planners and energy resources are gathered into a microgrid for better controllability. Different industries are using robots which are connected and can be controlled remotely. Even road

vehicles are seen today as a part of IoT since they hold code in, use IoT-based sensors and have external network interfaces for communication. (Lehto & Neittaanmäki, 2015; Hassan, 2019.) An example of an IoT automotive application is the iDrive, an intelligent informatics system from BMW which provides driving directions, monitoring of vehicle location, and information of the road conditions (Uden & He, 2017). Another example is a wireless OBD-II dongle which enables vehicle owners to remotely perform functions to their vehicle via mobile apps. The functions are basically monitoring and diagnostics and e.g., controlling the seat-belt warnings and disabling remote unlocking. (Wen, Chen & Lin, 2020.)

The evolution of IoT in automotive applications is divided into five different eras: Research and Development Era 1966-1995, Embedded Era 1995-2002, Infotainment Era 2007-2012, V2X (Vehicle-to-Everything) Era 2012-2020, and New Mobility Era from 2020 onwards (estimation). During the Research and Development Era, there were great ideas but no sufficient technology for implementation. Embedded Era provided with embedded modules wireless communication possibilities for vehicle users to communicate with telematics service providers by using e.g., mobile phones. Infotainment Era was the turning point when third-party content, and software and app providers joined the automotive industry by providing vehicular information and entertainment applications. V2X Era describes vehicles as smart devices with their multiple sensors and embedded technology and services enabling communication with other smart devices and infrastructure around. New Mobility Era is about autonomous self-driving vehicles and possibly a rivalry between software providers and carmakers concerning who dominates the automotive industry. (Krasniqi & Hajrizi, 2016; Rahim et al., 2021.) The recent IoT technologies are presented in the following table (table 1) from Infotainment Era to New Mobility Era.

TABLE 1 IoT vehicular technology from Infotainment Era to New Mobility Era by Rahim et al. (2021, 3)

Infotainment Era 2007-2012	**V2X Era 2012-2020**	**New Mobility Era 2020 -**
Monitor/display for entertainment facility in vehicle	Eco-navigation	Autonomous vehicle
BlackBerry's QNX tool	Smart charging and charging safety by V2H and V2G	Autonomous shared vehicle
Real-time vehicle navigation systems	Ride-sharing	Self-driven shared vehicle
Vehicle cockpit	Collision and accident avoidance	Vehicular environment by LTE
Wireless internet access in the car	Pedestrians safety alerts from the vehicle	NB-IoT and LoRa for vehicular connectivity

(continues)

Table 1 (continues)

Data streaming to the vehicle with the help of USB and Bluetooth connectivity	Smart traffic management	
Speech-recognition interface for car	Traffic congestion avoidance alert	
	Internet of Vehicle technology	

Cybersecurity concerns IoT in the automotive applications as all connected devices need to be protected against attacks and misuse. For the study, it is relevant to acknowledge the dimensions of IoT in the automotive domain. From the IoT spectrum, especially V2X communication is elaborated further in the study.

2.3.2 Cyber-Physical Systems (CPS)

Cyber-Physical Systems (CPS) are systems which include both physical and computational components and these components are closely integrated with each other. A cyber-physical system is connected to a network, and it has same principles as IoT, but CPS holds higher capabilities with mission-critical applications, thus it is used more in vehicular industry like cars and space shuttles. (Baheti & Gill, 2011; Onishi et al., 2017.) Cyber-physical systems have reached a variety of different domains in the economic society and modern industry. The real-time applications and services are utilized in energy industry like power, gas and water, medical health care, military, agriculture, manufacturing systems, smart cities, and in transportation such as intelligent transportation systems (ITS) and autonomous vehicles. (Ding, Han, Ge & Wang, 2020; Yaacoub et al., 2020.)

The architecture of CPS is divided into three main layers by Yaacoub et al. (2020). The first layer is called Perception Layer and it collects data and information with sensors, aggregators, actuators, RFID (Radio Frequency Identification) tags and GPS. The second layer is Transmission Layer, and its objective is to transmit data and information via clouds, internet, access points, WiFi, routers, switches and with Zigbee, a wireless mesh network. The third layer is the Application Layer for data and information analysis, and for decision making. The Application Layer contains smart solutions like smart waste management, smart vehicles, smart transportation and traffic control, smart infrastructure and street lighting, and smart power managements. (Yaacoub et al., 2020.)

2.3.3 Cyber-Physical Vehicle Systems (CPVS)

Just like IoT, CPS has expanded into automotive domain as mentioned above, and the Cyber-Physical Vehicle Systems (CPVS) are increasing and being

widely researched. Bradley and Atkins (2015) describe humans being cyber-physical systems fundamentally where the mind represents the cyber, and body the physical subsystems. The analogue refers to advanced CPVS which exploits the resources of cyber and physical entities. The humans have symbiosis how the mind and body works together, but CPVS's cyber and physical parts are only partially aware of each other or even completely unaware. This dilemma has been under heavy research how to improve the awareness with path planning, control theory and real-time system theory. (Bradley & Atkins, 2015.)

Bradley and Atkins (2015) have divided the architecture of CPVS into three layers: 1) the reactive, control or acting layer (low-level), 2) the execution, guidance, or sequencing layer (intermediate), and 3) the planning or deliberation layer (high-level). The first layer consists of physical actuators which are controlled in low-level, and which utilize feedback control techniques. The second layer acts as an assistant or a middleman between the first and third layer by translating the high-level plans of third layer to first layer so that the first layer can make the required actions with the given reference trajectories or sequences. The third layer contains the algorithm for planning and scheduling tasks and actions. (Bradley & Atkins, 2015.)

A typical example of CPVS is an intelligent electric vehicle in which the cyber is represented by the controller, and the physical part is formed by the human driver, the vehicle, and the environment (Lv, Xing, Zhang & Cao, 2020). As intelligent vehicles are becoming more and more autonomous and connected to different networks, they need to communicate with other vehicles and non-vehicle entities for safe and secure transportation. The development of automotive systems is shifting to a mode of systems of systems instead of isolated entities, and this requires vehicular communication between vehicles and other related parties. (Macher et al., 2021.) The next section discusses the different vehicular communication types and technologies.

2.4 Vehicular Communication

Vehicular communication types can be divided into internal or external. Internal communication can be seen as the communication between different elements and systems inside the vehicle and external communication happens when the vehicle connects and communicates with the world and infrastructure outside. (Doms et al., 2018.)

The search of different cybersecurity breach interfaces and related technology is pointed to vehicular communication in many studies. The focus is on the cyberattacks from outside the vehicle. Vehicular communication forms the main interface for possible hijacks, disturbance, and infiltration of a vehicle. As an example, a hacker (a person), outside the vehicle causes safety hazard to the driver and possible passenger(s) if manipulating the safety features of some communication system with a malware. The communication types are identified being in-vehicle, telematics, infotainment, and vehicle-to-everything.

(Wolf, Weimerskirch & Wollinger, 2007; Zhao, 2002; Wolf et al., 2006; Smith, 2016; Rahim et al., 2021.) This section introduces the very basic functions of a vehicle and discusses what the vehicular communication interfaces are which can be attacked from outside.

2.4.1 In-Vehicle Communication

Vehicular communication can be seen as internal or external depending on the function in question. Internal communication or in-vehicle communication refers to communication between different nodes inside the vehicle itself. The main basic elements and systems forming the in-vehicle communication are ECUs, CAN and OBD. ECU stands for Electronic Control Unit, and ECU embodies an independent computer or a microprocessor in a vehicle. ECUs coordinate and monitor different elements and functions in a vehicle such as vehicle's body components (windows, dashboard, lights, wipers, mirrors, doors, roof and so on) and the driver's comfort (air conditioning, cruise control, seats, air bags and so on). (Koscher et al., 2010; Keskin, 2009; Charette, 2009.) CAN stands for Controller Area Network, and it is the protocol for internal network of a vehicle which connects ECUs with serial buses and enables them to communicate. As an example, ECUs communicate through CAN so that the vehicle knows when to brake or accelerate. (Checkoway et al., 2011; Han, Weimerskirch & Shin, 2014.)

The physical interface to a vehicle's internal system is the OBD-port. OBD stands for On-Board Diagnostics, and it is the central gateway and the interface for diagnostics while its physical port is the gate to a CAN bus that connects different ECUs. From outside the vehicle one can communicate from OBD-port and read the diagnostics of the vehicle and reset parameters. Via OBD-port one can connect to different ECUs and use read, write, and delete functions. (Smith, 2016.) It is worth to mention that there are future technologies such as FlexRay and automotive Ethernet which are evolving high-speed network communication protocols. CAN is seen as a midrange protocol whereas FlexRay and automotive Ethernet are considered as high-end protocols. (Smith, 2016.)

2.4.2 External Vehicle Communication

Telematics, infotainment, and vehicle-to-everything (V2X) are today's interfaces from the vehicle to the outside world (Zhao, 2002; Smith, 2016; Rahim et al., 2021). Infotainment provides entertainment features such as music, movies, games, and newscasts, but also information features such as GPS services to the vehicle's driver and passengers (Wolf et al., 2006). Telematics focuses to provide navigation and location-based features related to safe driving, such as control of vehicle speed and notification of vehicle collision (Zhao, 2002; Checkoway et al., 2011). In addition to telematics and infotainment, vehicle-to-everything, V2X is an evolving technology which is applied especially to automated driving. V2X

incorporates different technologies related to connected vehicular communication with other vehicles, road infrastructure, pedestrians, and networks. (Rahim et al., 2021.)

Telematics and Infotainment

Telematics, a concept combined from the words telecommunications and informatics (Nora & Minc, 1980), refers to any system or a device in the vehicle that communicates wirelessly and offers navigation and location-based services to the vehicle driver and third parties. Telematics system sends, receives, and stores information that can be utilized in addition to vehicle owner by vehicle manufacturers, car service, police, or insurance companies. Telematics offer safety and communication features such as crash warning, maintenance notifications, theft detection and emergency calls. (Zhao, 2002; Checkoway et al., 2011.)

Infotainment gets its name from the words information and entertainment, and by its name, it focuses to provide information and entertainment features to the driver and passengers. Infotainment features have been thought as premium content in vehicles, but vehicle manufacturers have started to build in more infotainment features as standard features. Infotainment features are GPS, WiFi, Bluetooth, radio, newscasts, movies, music, games, hands-free calling and so on. (Wolf et al., 2006.)

Vehicle-to-Everything Communication (V2X)

Vehicle-to-everything is an overall term for vehicle's connected communication technologies. According to a whitepaper by Rapid Global Business Solutions (2020), there are seven types of vehicle connectivity. Such technologies are vehicle-to-vehicle communication (V2V), vehicle-to-infrastructure communication (V2I), vehicle-to-pedestrian communication (V2P), vehicle-to-network communication (V2N), vehicle-to-cloud communication (V2C), vehicle-to-device communication (V2D), and vehicle-to-grid communication (V2G) (RGBSI, 2020). The applications and goals of V2X consists of road safety, traffic management, comfort and infotainment, and autonomous driving (Sedar, Kalalas, Vázquez-Gallego, Alonso & Alonso-Zarate, 2023). V2X communication is seen as more advanced concept than Telematics as V2X has further developed technology and it provides a larger scale of features (Harding et al., 2014). V2X is not however a mainstream technology today, it is still under development (Wang, Shao, Ge & Yu, 2019).

Vehicle-to-everything communication technology can be seen evolving since the 1960s when the Electronic Route Guidance System (ERGS) was developed by the US Federal Highway Association. The ERGS was intended to provide route guidance via an in-vehicle unit which enabled interaction between the system and the users. (Dong, 2011.) During the 1970s in Tokyo Japan, private corporations together with two government research institutes deployed a project called Comprehensive Automobile Traffic Control System

(CACS). This FR (radiofrequency) communication based dynamic and interactive system took the route guidance into the next level with additional functions which saved total travel time. (Matsumoto, Mikami, Yumoto & Tabe, 1979; Dong, 2011; Alalewi, Dayoub & Cherkaoui, 2021.)

After several decades later, the V2X technology started to evolve in bigger steps during the Infotainment Era 2007-2012 (see chapter 2.3.1) introduced by Krasniqi and Hajrizi (2016). In 2007 Wolf et al. studied the potential attacks on automotive software and how the software can be protected. In their study the concepts vehicle-to-vehicle communication and vehicle-to-infrastructure communication were presented. (Wolf et al., 2007.) In 2014 the US National Highway Traffic Safety Administration (NHTSA) published a report of the readiness of vehicle-to-vehicle communication technology for road safety applications and listed potential use cases. The report discussed the V2V and V2I communications and introduced a new communication type; vehicle-to-pedestrian (V2P). According to the report, V2X acronym meant vehicle-to-other such as bicycles. (Harding et al., 2014.) In 2016 Craig Smith used a term vehicle-to-anything in his car hacking book to describe V2X. That time V2X comprehended V2V, V2I and V2P. In general, the discussion of V2X concerned mainly the V2V communication technology. (Smith, 2016.)

Despite the terminology evolution, the technology behind V2X is the same concerning V2V and V2I today. The technology is used in vehicle communication to inform and warn drivers about safety and traffic situations. The goal is to make transportation safer and reduce vehicular accidents. The V2I communication technology is part of the Intelligent Transportation System, ITS, which is a dynamic mesh network that connects not only vehicles to each other, but also roadside devices such as traffic lights. V2V and V2I technology uses dedicated short-range communication protocol, DSRC, which is a wireless communication system working as one- or two-way from a vehicle to a vehicle or a roadside device. The DSRC can be thought as a built-in radio in a vehicle operating in 5.8 - 5.9 GHz band telling other vehicles its position, direction, and speed. (Smith, 2016; RGBSI, 2020; Zhou, Xu, Chen & Wang, 2020.) DSRC together with V2V and V2I technologies is predicted to be installed in 60% of all vehicles by 2029 in the US (Bayless et al., 2016). V2V and V2I provide a 360-degree representation in which vehicles register other vehicles and roadside devices regarding long distance or in urban scenarios where buildings may cover the view around a corner. The features that this kind of communication can offer are different violation warnings such as red light, stop sign or railroad crossing. Another set of such features provide assisting in intersection movement and turning left, as well as warnings of objects in blind spot and lane changing. (Harding et al., 2014; RGBSI, 2020.) The V2V and V2I technology is designed to consider cybersecurity threats which makes it a pioneer in the automotive industry as typically cybersecurity has been considered only afterwards designing vehicle related systems and protocols (Smith, 2016).

Vehicle-to-pedestrian communication (V2P) used to focus on sensors in a vehicle to prevent crashes with pedestrians. A new approach by NHTSA (US

National Highway Traffic Safety Administration) suggested that carry-on devices like mobile phones interact with the vehicle's crash prevention system by using the DSRC frequencies like V2V and V2I. (Harding et al., 2014.) The challenge with the approach is that not everyone carries mobile phones with them, like small children, nor everyone agrees to use such technology. There needs to be other means in parallel to cover all types of pedestrians which makes the V2P the most challenging communication type to cover. (Sewalkar & Seitz, 2019; RGBSI, 2020; Teague, 2021.) V2P covers all kinds of Vulnerable Road Users (VRUs) which contain pedestrians, motorized two-wheelers, and cyclists. A lot of investigation and research is happening to cover the different VRUs. For cyclists and motorized two-wheelers (MTWs) smart helmets together with smartphones are proposed. The helmet warns the bicycle or MTW rider of approaching vehicle after the smartphone has transmitted cloud-based position data. For pedestrians, a tag could be placed into bags, backpacks, wheelchairs and so on for vehicles to notice the cautionary object. (Sewalkar & Seitz, 2019.) Even augmented reality interfaces are proposed to protect the VRUs (Pratticò, Lamberti, Cannavò, Morra & Montuschi, 2021).

Vehicle-to-network communication (V2N), vehicle-to-cloud communication (V2C), vehicle-to-device communication (V2D), and vehicle-to-grid communication (V2G) are the newest types of vehicular communication. Some of them could be considered as extensions to the existing vehicular communication types. Vehicle-to-network for example extends V2V and V2I by communicating with data centers, road infrastructure, cellular and IT networks, other vehicles, and even pedestrians. With this kind of networking, the vehicle can get real-time traffic information and improved driving directions. (RGBSI, 2020; Elagin, Spirkina, Buinevich & Vladyko, 2020; Teague, 2021.) Vehicle-to-cloud boosts V2N by offering cloud-based data exchange and providing broadband cellular mobile networks for V2N access. With this technology, vehicles' software can be updated with OTA (over-the-air), vehicle diagnostics are transmitted, and the preferences of a driver are saved. Even the smart home appliances can be contacted via the cloud. (Rangarajan, Verma, Kannan, Sharma & Schön, 2012; RGBSI, 2020.) With vehicle-to-device (V2D), it is possible to exchange information between vehicles and any smart devices like smartphones and tablets via Bluetooth to connect with the vehicle's infotainment system for instance. The technology also enables communication with smart traffic cones and Smart-Canes, which are electronic devices used together with walking sticks by visually impaired people. Even vehicles themselves can be addressed as smart devices in a sense. (Al-Fuqaha, Kwigizile & Oh, 2018; RGBSI, 2020.) Vehicle-to-grid (V2G) is a technology that targets to contribute into sustainable development and fights the climate change. This happens by using electric vehicles as part of renewable energy systems to support the electrification of the transportation and to balance the electricity consumption especially in times of energy crisis. The idea of V2G is to use electric vehicles in bidirectional way with different smart grids. The electric vehicles have charging and discharging functions, which makes them like

batteries on wheels. The different types of electric vehicles are battery electric vehicles (BEV), plug-in hybrid vehicles (PHEV) and hydrogen fuel cell vehicles (HFCEV). The electric vehicle can be connected and utilized in smart home grid, smart parking lot grid, and even in national power grid. The different grids both feed and obtain energy from the electric vehicle. The innovations around the V2G makes it a ground-breaking technology. (Liu, Chau, Wu & Gao, 2013; Tan, Ramachandaramurthy & Yong, 2016; RGBSI, 2020.)

Vehicle-to-everything communication technology is targeted specifically for connected vehicles with high automation capabilities as well as autonomous driving since without communication, one cannot perform the needed actions. Environment perception is the key element as vehicles are always aware of the surroundings, vehicle speeds and so on. More information is needed of the environment to act upon with the vehicle functionality and reacting. Buildings and crossings, in-vehicle systems and far away situations must be known early enough to react in time. Further on, a fully automated and independent vehicular functionality requires communication with road operator in case of vehicle fleets as an example. (Schoitsch et al., 2016; Gurumurthy, Kockelman & Loeb, 2019.)

Based on the examined literature, V2X technology is seen as the most liable and open, in a negative sense, interface for possible cyberattacks. Some scholars think that the hardware of a vehicle is the most important asset to be secured against cyberattacks. Luckily it is stated that V2X technology software development focuses on the early design phase to take cyberattacks into consideration. (Smith, 2016; Schoitsch et al., 2016.)

Internet of Vehicles (IoV) and V2X Cybersecurity Threats

Internet of vehicles (IoV) is producing a lot of discussion in the academia, and the definition varies among the scholars. Some say it equals to V2X (Ji et al., 2020), others think IoV as a convergence of IoT (Internet of things) and mobile internet (Sadiku, Tembely & Musa, 2018), while IoV is also considered representing a certain case of IoT (Nahri, Boulmakoul, Karim & Lbath, 2018). Nevertheless, the definitions describe the essentials of the IoV which are similar with IoT: smart vehicles connected to other smart vehicles, to pedestrians with smart devices, to smart parking lots and to smart roadside infrastructure through a network. The IoV network uses sensors, software, embedded hardware, and V2X communication technology for the connection establishing and data exchange. (Sadiku et al., 2018; Alalewi et al., 2021; Rahim et al., 2021.) The evolution path of IoV starts with VANETs, vehicular ad hoc networks which are part of ITS (Intelligent Transportation Systems). VANETs use wireless networking technology like WiFi, DSRC and 4G/LTE (Long Term Evolution) and is expanding towards newer cellular technology. The C-V2X, cellular vehicle-to-everything is using 5G mobile technology and it is arriving alongside DSRC. (Zhou et al., 2020; Shen, Fantacci & Chen, 2020; Alalewi et al., 2021.) The ambition of IoV technology is to make transportation more safe, efficient, fast, and autonomous whilst improving the vehicle maintenance and

lifecycle, and reduce destructive environmental impact (Zhou et al., 2020; Duan et al., 2020).

V2X, as any communication technology, has vulnerabilities and is a target for cybersecurity attacks. Since vehicles are connected through IoV, the wireless network invites intruders in increasing numbers as V2X is getting publicity and popularity. People's safety is threatened not only physically, but also privacy and data security are jeopardized. (Villarreal-Vasquez, Bhargava & Angin, 2017; Sedar et al., 2023.) Looking through the research field, it is certain that there exists different levels of classification of the cybersecurity threats of V2X. Some scholars define only few types of threats, like Ivanov, Maple, Watson and Lee (2018): jamming, spoofing and meaconing, and Furqan, Solaija, Hamamreh and Arslan (2019): eavesdropping, spoofing and jamming. Marojevic (2018), Alnasser, Sun and Jiang (2019), Wang, Shao, Ge and Yu (2019), and Sedar et al. (2023) classify the threats based on cybersecurity attributes. The listing of the threats by attributes can be seen in table 2 (table 2).

TABLE 2 Threats based on cybersecurity attributes by Marojevic (2018), Alnasser et al. (2019, 21), Wang et al. (2019, 4) and Sedar et al. (2023, 341)

Marojevic (2018)	Alnasser et al., (2019)	Wang et al., (2019)	Sedar et al., (2023)
Identification, Authenticity, and Integrity Fake nodes False information Fake certificates	**Availability** Blackhole and Greyhole attacks Flooding attack Jamming attack Coalition and platooning attacks	**Authentication** Sybil attack GPS spoofing/position faking attack Node impersonation attack	**Authentication** Sybil Impersonation GPS spoofing Free-riding
Availability Fake certificates RF congestion Jamming	**Data integrity** Alter or inject false messages attack Replay attack GPS spoofing attack	**Availability** DoS attack DDoS attack Jamming attack Black hole attack	**Availability** Denial-of-service (DoS) Jamming Flooding Spamming Malware

(continues)

Table 2 (continues)

Confidentiality and Privacy Fake nodes RF replay	**Confidentiality** Eavesdropping attack Location tracking	**Data Integrity** Masquerading attack Replay attack	**Confidentiality** Eavesdropping Traffic analysis Man-in-the-middle
Non-Repudiation and Accountability Malfunctioning UE	**Authenticity** Certificate replication attack Sybil attack Masquerading attack or impersonation attack	**Confidentiality** Eavesdropping attack Traffic analysis attack	**Integrity and data trust** Message modification Replay Masquerade Illusion
	Non-repudiation Fake identity node in message transmission attack	**Non-repudiation** Loss of events traceability	**Privacy** Location tracking Identity revealing
		Real-time constraints Timing attack	

Lu, Zhang, Ni and Fang (2019), and Ghosal and Conti (2020) define threats based on cybersecurity attributes, but also by specific cases like HW, SW and networking technology, and they outline security issues or security challenges and requirements. The threats listed by Lu et al. (2019), and Ghosal and Conti (2020) are in table 3 (table 3).

TABLE 3 Threats based on cybersecurity attributes, specific cases, and networking technology by Lu et al. (2019), and Ghosal and Conti (2020, 13)

Lu et al. (2019)	Ghosal and Conti (2020)
Trust attacks in 5G V2X systems Bad Mouth Attacks Conflicting Behavior Attacks Blackhole Attacks Sybil Attacks	**Security Challenges for V2X** Dynamic Network Topology Network Scalability Heterogeneity Communication Latency Data Priority Adoption to Future Platforms Attack Prevention User's Trust and Privacy

(continues)

Table 3 (continues)

Security Issues in 5G V2X Confidentiality Authenticity Integrity Availability	**Security Requirements for V2X** Authentication Message Integrity Access Control Message Confidentiality Availability Privacy and Anonymity
Security Attacks in 5G V2X Eavesdropping Message Forgery Jamming Impersonation Replay Attacks MITM (man-in-the-middle) Attacks Sybil Attacks	**Attacks based on Behavioral Patterns** **Selfish Attacks:** Message Spoofing Attack Traffic Analysis/Movement Tracking Attack Eavesdropping Repudiation **Malicious Attacks:** Message Replay Attack Sybil Attack Denial of Service (DoS) Attack Malicious Code Attack Black Hole Attack
Attacks on Network Edge Location Spoofing DoS Attacks Fake Attacks	**Attacks on Hardware (H/W) and Software (S/W)** Location Disclosure Attack Denial of Service (DoS) Attack Spoofing and Forgery Attack Man in the Middle (MiM) Attack Tampering Hardware Brute Force Attack
Attacks on 5G Core Networks Hijacking Attacks Saturation Attacks Link Fabrication Attacks Unauthorized Slice Accesses	**Attacks on Infrastructure** Session Hijacking Attack Distributed Denial of Service (DDoS) Attack Unauthorized Access Tampering Hardware Masquerade Attack Repudiation Attack
Attacks on Data Network/Internet DoS Attacks Malware Injection	**Attacks on Privacy** Identity Revealing Attack Location Tracking
Privacy Issues in 5G V2X Identity Privacy Content Privacy Contextual Privacy Location Privacy	**Data Trust Attacks** Masquerade Attack Replay Attack Message Tampering Attack Hidden Vehicle Attack (GPS spoofing) Illusion Attack (false data)

(continues)

Table 3 (continues)

Privacy Attacks in 5G V2X	
Packet Analysis Attacks	
Packet Tracing Attacks	
Linkage Attacks (Correlation Attacks)	
Movement Tracking Attacks	
Identity Revealing Attacks	
Collusion Attacks	
Inference Attacks	
Deanonymization/Reidentification Attacks	

Sharma, You and Guizani (2020) have taken the cybersecurity threat defining into a highly detailed level. They have gathered a respectful 25 item list of different attack and threat methods and included examples of the related attack types. The exhaustive list of the attacks is presented in table 4 (table 4).

TABLE 4 Cybersecurity attacks, threats, and types by Sharma et al. (2020, 5)

Attacks and Threats	**Types**
Authentication and Authorization Attacks	Brute Force, Weak Validation, Access violation, Session control, Broken Authentication, ACL Modification
Malicious Node Attacks	Black-Hole Attacks, Grey-Hole Attacks, Sink Hole Attacks
Certificate Forgery	Replication, Duplication, Modification, Alteration
Channel Interference	Noise, Jamming, Signal Storming, Covert and overt channels
Cipher text / Plain Text Attacks	Known and Chosen
Data Deletion, Data Disclosing, Data Forgery and Distributions	Replication, Duplication, Modification, Alteration
De-Synchronization Attacks	TCP De-Synchronization, DNS poisoning, Port identification, ICMP attacks
DoS and DDoS Attacks	UDP Flood, SYN Flood, Ping of Death
Access Attacks	Eavesdropping, Impersonation, Man-in-the-Middle, Masquerade Attack
Fabrication Attacks	Falsified Information Injection, Falsified Sensor readings and Misinterpretations
GPS/MAP Modifications	-
Terminals Attacks	Hidden Terminals and Exposed Terminals
Key Exploitation	-
Message Modification and Tampering	Content Modification and Header Modification, SQL Injections, Code obfuscation
Network Stalking and Penetration Attacks	Sniffing, Forensics, Spoofing, Spamming
Reprogramming Attacks	Cloning attacks, Code obfuscation, XSS-scripting
Resource Depletion Attacks	-

(continues)

Table 4 (continues)

Routing Attacks	Topology-based, Resources-based, Traffic-based
Service based network Prevention and Session Hijacking	-
Side Channel Attacks	Cache attack, Timing attack, Power-monitoring attack and Electromagnetic attack, Acoustic attack
Zero-day	Exterior and Interior
Sybil Attacks	-
Timing Attacks	Message Connect, Service-Access based, Range-based, Replay Attacks
Tunneling Attacks	ICMP, DNS, Port, HTTP
Vehicle Health Disruption	Vehicle Configuration Alterations, Vehicle capturing, Firmware and Vehicle Software Modification, Trajectory Alteration

Most of the above-mentioned scholars have proposed approaches how to secure the V2X communication from intrusion and violation attempts. Furqan et al. (2019) proposes cryptography-based and PLS-based (physical layer security) solutions for eavesdropping, spoofing, and jamming. In addition to cryptography-based solutions, Alnasser et al. (2019) introduces behavior-based/trust-based and identity-based solutions for attacks concerning different cybersecurity attributes. Sedar et al. (2023) divides the defence mechanism taxonomy into two branches: proactive security and reactive security. Proactive security consists of cryptography-based, physical layer security (PLS) and privacy preservation. Reactive security holds signature-, anomaly- and context-based solutions from which the latter two are entity and data centric focusing on behavioral and trust (entity-centric), and plausibility and consistency (data-centric) solutions. Ghosal and Conti (2020) classify security approaches into three categories: Symmetric Key Cryptography, Privacy Preservation and Message Authentication.

The protective and preventive measures are taking place yet more needs to be done and investigated for the securing of V2X communication technology. The regulation and standardization of cybersecurity in the automotive domain is crucial and efforts are made to ensure the protection of vehicles from misbehavior attacks. (Sedar et al., 2023.) The next chapter introduces the security related standards in the automotive industry.

2.5 Standards in Automotive Industry

As the automotive industry is highly regulated by different standards, it is necessary to express the importance of the given standards and how they should be referenced. The standards can be even considered as laws and the contents of the standards must be referenced as originally stated. To manage

this necessity, each section taken from an automotive standard, technical report or guidebook is marked in the text in *cursive* and appropriate reference is used accordingly. The chosen standards, a technical report and a guidebook for the study and their referencing procedure are presented in the following table (table 5) and elaborated further in this chapter.

TABLE 5 Referencing procedure of the selected standards

Code	**Name**	**Name used in the study**	**Description**	**Link to public material**
ISO 26262	Functional Safety	Functional safety standard	Functional safety standard covers the critical safety definitions for electronic and electrical safety-related systems of road vehicles. The standard is crucial when new vehicles are designed, and it is an important part of the overall safety and security of road vehicles.	https://www.iso.org/search.html?q=ISO%2026262&hPP=10&idx=all_en&p=0&hFR%5Bcategory%5D%5B0%5D=standard
SAE J3016	Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems	Automation level technical report	SAE J3016 covers the definitions of different automation levels of road vehicles. The technical report is needed when discussing the differences between automated driving and autonomous vehicles.	https://www.sae.org/standards/content/j3016_201401/

(continues)

Table 5 (continues)

SAE J3061	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems	Cybersecurity guidebook	The first guidebook defining cybersecurity of road vehicles. The basis of new standard ISO/SAE JWG 21434. Defines TARA framework and lists related methods for security risk analysis.	https://www.sae.org/standards/content/j3061_201601/
ISO/SAE JWG 21434	Road vehicles - Cybersecurity engineering	Cybersecurity engineering standard	The new standard designed specifically for cybersecurity of road vehicles. The basis of requirements and recommendations how to ensure new vehicles are cybersecurity compatible.	https://www.iso.org/standard/70918.html

The standards, a technical report and a guidebook chosen to the study are within the automotive domain in the areas of functional safety, cybersecurity, automated driving levels and performing a security risk analysis. The full names and the publishing years of the standards, a technical report and a guidebook can be seen in the following figure (figure 2). The cybersecurity engineering standard is marked with dotted line as the version used for the study was a draft.

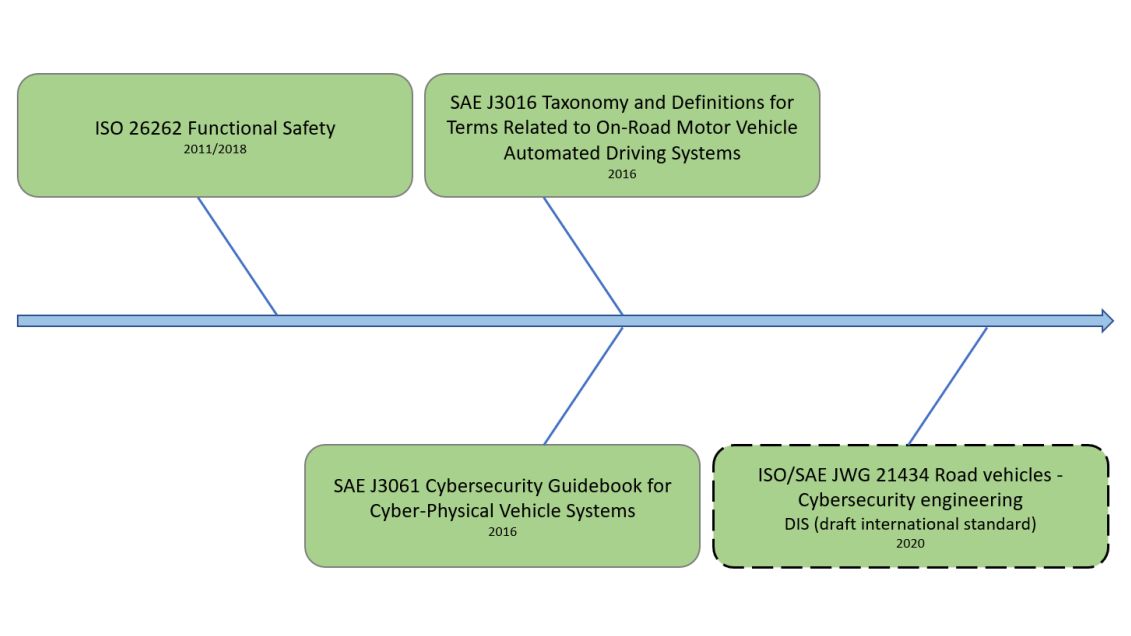

FIGURE 2 Standards related to the study

The cybersecurity guidebook and the cybersecurity engineering standard are providing guidelines and recommendations what methodologies should be used when making a security risk analysis. But they do not offer specific technology or what tools could be used for the analysis. The user would need to know what to use in practise. Also, reading a standard or a technical report requires related technical knowledge and usually applying a use case to test the guidelines in practise. Having a use case eases the direction of the study and discussion when having an example in the process-based approach. The use case for the study is presented in chapter 3.4.

The standards can be very wide in size and content, thus the study outlines its focus only on the system level, and to be more precise, to vulnerabilities in the system interface level. Vulnerabilities and possible intrusions in hardware and software level are scoped out. Only software intensive systems are considered.

2.5.1 ISO 26262 – Functional Safety

The Functional Safety aspect in road vehicles is defined by the International Organization for Standardization (ISO). The standard is the basis and the cornerstone of all safety-related systems including one or more electrical and/or electronic (E/E) systems in road vehicles like passenger cars, trucks, buses, trailers, and motorcycles, excluding mopeds. Human safety is in the scope of functional safety in all abstraction levels: system (functional/technical), hardware and software. The study focuses on the vulnerabilities in the system interface level as cybersecurity could have an impact on functional safety. It is

essential to identify any interaction points and harmonize the derived measures. (ISO, 2018.)

Functional safety standard is large. The standard was created in 2011 and updated in 2018. The standard consists of 12 separate parts in dedicated documents including about 800 pages altogether. The massiveness of the standard can be seen in the following figure (figure 3).

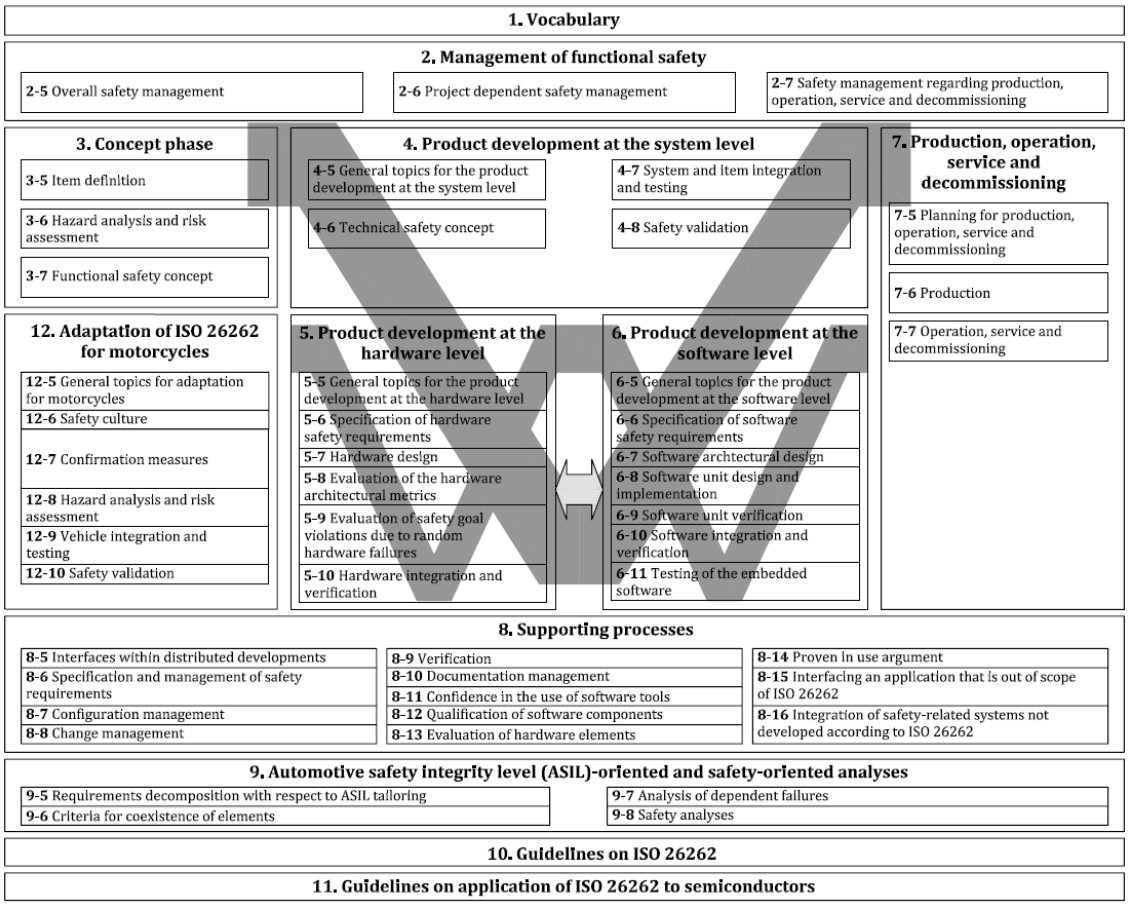

FIGURE 3 Overview of the Functional Safety standard (ISO, 2018:3, vii)

Many other standards are related to functional safety, and they need to be acknowledged and respected. The functional safety standard is derived from IEC 61508 general industry functional safety standard. IEC stands for International Electrotechnical Commission, and the 61508 standard name is *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*. The functional safety principle by IEC 61508 is to assure that the performed action is done correctly in the automatic protection system or that the failure of the performed action happens safely or predictably. The functional safety standard is also influenced by other safety standards, quality standards and assessment models, and automotive design standards. (Martin & Winkler, 2018.) Standards are not direct laws, but they act like one. Other standards provide basis to do such attributes in functional safety standard which then comes on top of some other standards. It is a very standardized and

chained world in automotive area as there needs to be guidelines and requirements to manufacture and ensure safe vehicles. (ISO, 2018.)

Functional safety standard does not cover cybersecurity aspect, but it has a substantial interaction with cybersecurity. The scenario between safety and security is quite tricky as security cannot be covered without safety aspect. The two qualities, safety and security have been treated separately in the automotive domain (Macher, Armengaud, Brenner & Kreiner, 2016b). It is necessary to manage the cybersecurity aspect with other appropriate standards. What is essential for the cybersecurity perspective from the functional safety standard, is the section *6.4.3 Classification of hazardous events* in part 3, the concepting phase. (ISO, 2018.) The cybersecurity engineering standard requires that safety related impacts must be derived from the classification of hazardous events in the functional safety standard (ISO/SAE, 2020). The classes of safety related impacts are presented in the following figure (figure 4).

	Class			
	S0	**S1**	**S2**	**S3**
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

FIGURE 4 Safety related impacts (ISO, 2018:3, 8)

Another meaningful matter within functional safety standard is the ASIL (*Automotive Safety Integrity Levels*) that classifies hazards. ASIL is linked to the safety related impacts mentioned earlier. ASIL is formed by making a risk analysis of possible hazards from the perspective of three classifications: *severity (S)*, *probability of exposure (E)* and *controllability (C)*. For the study, the controllability is highlighted. The controllability factor means the controllability by the driver and not the system, and the concept is elaborated further in the study.

The ASILs formed are ASIL A, B, C and D where ASIL D is presenting the worst-case scenario like fatal injury in the class *severity (S)* (see figure 4). Each ASIL is indicating the criticality of a given failure mode. ASIL degrees are categorized per each failure mode in the following way (ISO, 2018; Martin & Winkler, 2018):

- ”++” The method is **highly recommended**
- “+“ The method is **recommended**
- “o“ The method has **no recommendation for or against** its usage

An example of the usage of ASIL in System level can be seen in the following figure (figure 5).

Methods		ASIL			
		A	B	C	D
1a	Requirement-based test[a]	++	++	++	++
1b	Fault injection test[b]	+	+	++	++
1c	Back-to-back test[c]	o	+	+	++

[a] A requirements-based test denotes a test against functional and non-functional requirements.

[b] A fault injection test uses special means to introduce faults into the system. This can be done within the system via a special test interface or specially prepared elements or communication devices. The method is often used to improve the test coverage of the safety requirements, because during normal operation safety mechanisms are not invoked.

[c] A back-to-back test compares the responses of the test object with the responses of a simulation model to the same stimuli, to detect differences between the behaviour of the model and its implementation.

FIGURE 5 Example of ASIL used in System level (ISO, 2018:4, 20)

2.5.2 SAE J3016 Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems

Automation level technical report is defined by Society of Automotive Engineers (SAE) in 2014 and updated in 2016. The technical report classifies different terms and definitions related to driving automation, like ADS (*Automated Driving System*) and explains the levels of the driving automation. The levels as per the technical report are (SAE, 2016a):

- 0 - No Driving Automation
- 1 - Driver Assistance
- 2 - Partial Driving Automation
- 3 - Conditional Driving Automation
- 4 – High Driving Automation
- 5 – Full Driving Automation

The levels are illustrated in the following figures (figure 6; figure 7).

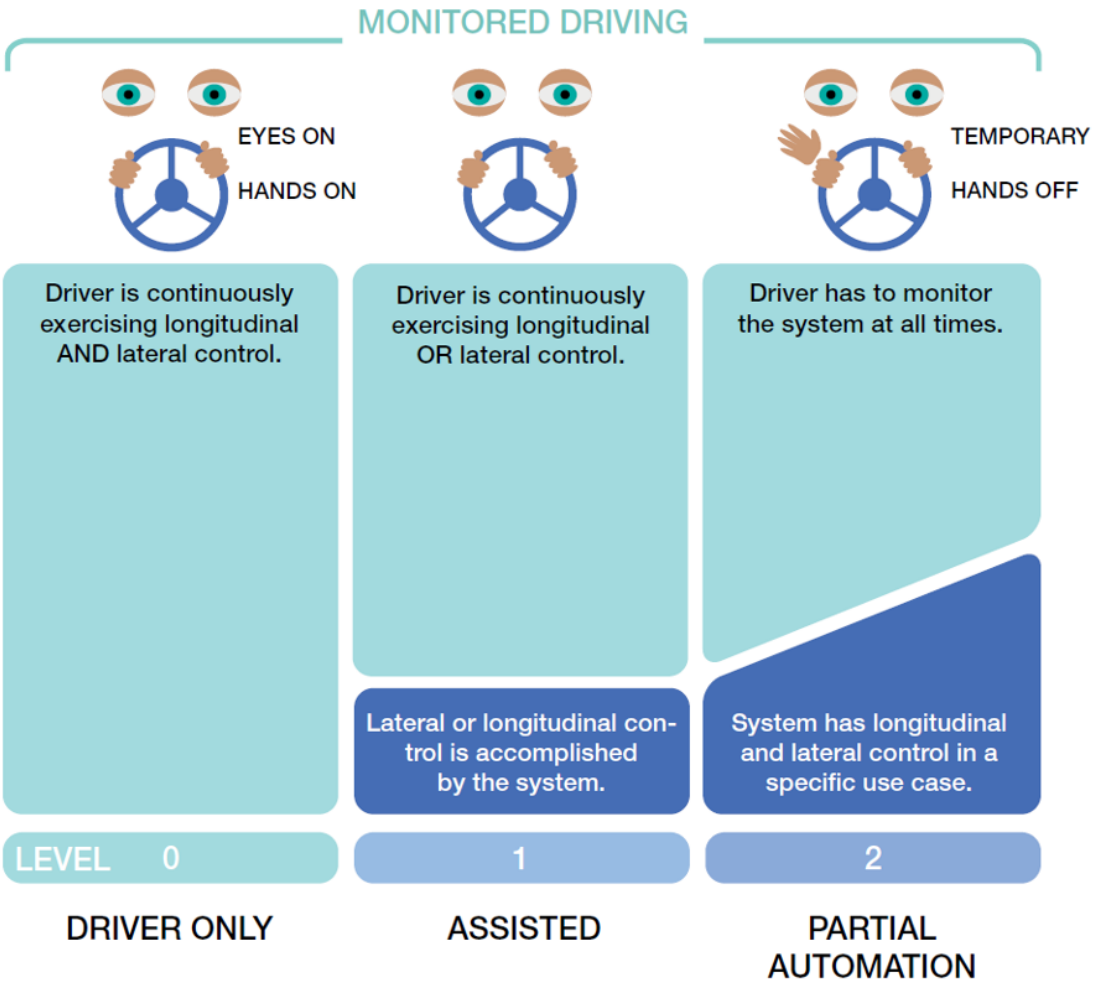

FIGURE 6 Vehicle automation levels, monitored driving (Doms et al., 2018, 15)

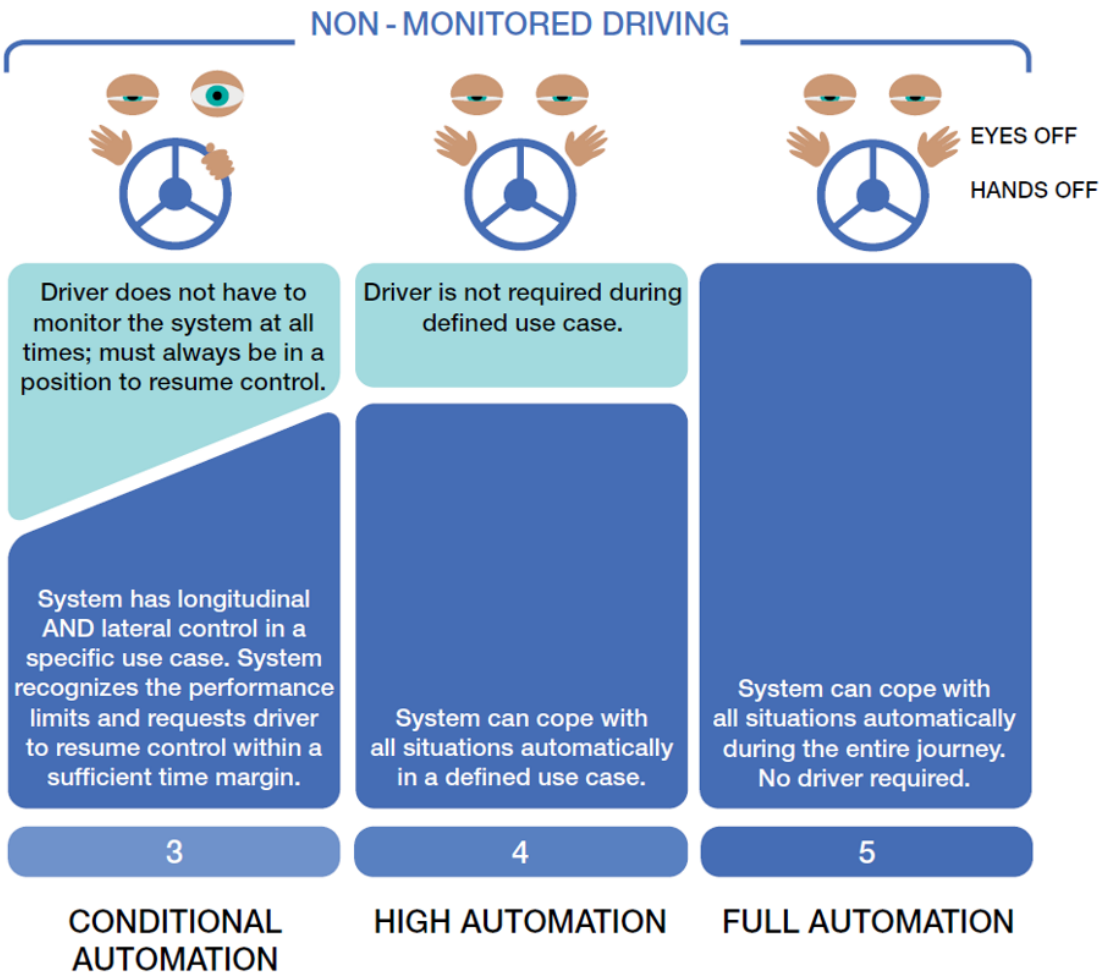

FIGURE 7 Vehicle automation levels, non-monitored driving (Doms et al., 2018, 15)

The study focuses on the levels 4 and 5 without a designated driver inside the vehicle concerning the autonomous driving. Levels 4 and 5 of the five automated driving levels are considered as driverless operations. Before ADS, there were ADAS (*Advanced Driver Assistance Systems*) which are helping the driver in different ways. The ADAS functions are for example adaptive cruise control (ACC), forward collision avoidance (FCA) and intersection collision avoidance (ICA) (Lu, Wevers & Van Der Heijden, 2005). The levels 1 and 2 are mainly ADAS related with the driver assistance features, and levels 3-5 are ADS based on the higher automation and independent vehicle-driven features (Guo et al., 2019).

The automation level technical report is in relation to the study by its nature of modern vehicles becoming more automated, and by some of the chosen security risk analysis methods. The methods are taking automated driving into consideration in their framework and use cases. As the future is preparing for more and more automation in driving, the automation levels bring insight for the definition.

2.5.3 SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

The predecessor of the vehicular cybersecurity is the cybersecurity guidebook created by SAE in 2016. The guidebook was developed to provide high-level principles how cybersecurity threats can be recognized and evaluated in the automotive domain. The guidebook also gives high-level advice how cybersecurity-aware systems can be designed. As mentioned earlier, the guidebook does not provide the tools and the technology how to deal with the cybersecurity threats or how to design the systems. With the given security risk analysis method recommendations, the automotive organizations can develop their own internal security risk management processes. (SAE, 2016b; Macher, Armengaud, Brenner & Kreiner, 2016a.)

In the cybersecurity guidebook, the impacts of the cybersecurity threats are explored from the aspects of *privacy*, *financial* and *operational* whereas the *safety* aspect is derived from the functional safety standard (SAE, 2016b). All the impact categories (*safety, privacy, financial* and *operational*) are crucial factors in the study for the investigation of the potential security risk analysis method.

The cybersecurity guidebook is enormously fundamental for the study, as it introduces the backbone framework for the security risk analysis: TARA (*Threat Analysis and Risk Assessment*). Macher et al. (2016a) made a thorough review of the different security risk analysis methods recommended in the cybersecurity guidebook. The chosen methods by Macher et al. (2016a) are presented in the study in chapter 3.2 in table 9 (see table 9).

2.5.4 ISO/SAE JWG 21434 – Road vehicles - Cybersecurity engineering

The primary and crucial standard for the study is the cybersecurity engineering standard which provides the requirements and recommendations what to include to a security risk analysis. The standard recommends using TARA compatible methods. For the vehicular cybersecurity aspect, the standard gives guidelines what to define but not how to define it exactly. It is the framework and guideline provider, but it is up to the organizations how to apply the guidelines to company specific cybersecurity processes and what TARA compatible security risk analysis methods to use. (ISO/SAE, 2020.)

It is essential to mention, that the cybersecurity engineering standard has become a demand for vehicle homologation and that makes the standard very important in the vehicle development. An upcoming cybersecurity regulation called *UN Regulation No. 155 - Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system* states that any vehicle needs to comply with cybersecurity engineering standard (UNECE, 2021a). The regulation is defined by the working party of UNECE World Forum for Harmonization of Vehicle Regulations (WP.29) (UNECE, 2021b). UNECE is the United Nations Economic Commission for Europe which promotes the pan-European economic integration (UNECE, 2021c).

The cybersecurity engineering standard development was initiated in 2016 and the draft international standard version (DIS) was released in early 2020 which is the version used in the study. The final draft international standard (FDIS) version was published in April 2021, but the changes compared to the DIS version were so minimal that there was no need to switch using the FDIS version. (ISO/SAE, 2020.)

The standard is based on the cybersecurity guidebook which uses terminology from the past. Terminology is a major issue to be addressed through the new cybersecurity standard. The standard harmonizes the terms across the automotive domain so different stakeholders can share the same understanding of the different concepts. (Akram, 2019; ISO/SAE, 2020.)

The predecessor guidebook of cybersecurity could not provide the same to vehicular cybersecurity what the functional safety standard provides to vehicular safety. Thus, it was important to create a more suitable and comprehensive standard to address cybersecurity in the automotive domain. The cybersecurity guidebook however was an important steppingstone in the development of vehicular cybersecurity. (Schmittner et al., 2018.)

The cybersecurity engineering standard was targeted to follow the similar approach with risk assessment as the functional safety standard does with its ASIL hazard classification (Schmittner et al., 2018). SAE started to develop *Automotive Cybersecurity Integrity Level* (ACsIL) in 2016 to synchronize ASIL with cybersecurity, but the extension has been on hold ever since (SAE, 2016c). For the cybersecurity aspect, another kind of workaround was created by the cybersecurity engineering standard: *Cybersecurity Assurance Level* (CAL). The CALs from 1 to 4 are equivalent to ASIL A, B, C and D. With the CAL, the required security level can be defined and the related criteria. (Akram, 2019; ISO/SAE, 2020.)

The requirements chosen to the security risk analysis were selected from the sections *8.3 Asset identification* to *8.8 Risk determination* as they were directed from the requirement *[RQ-09-05] Perform risk analysis* in section *9.4 Cybersecurity goals*. The requirement *[RQ-09-05]* consists of the analysis of an item involving asset identification, threat scenario identification, impact rating, attack path analysis, attack feasibility rating, and risk determination. All in accordance with the sections from 8.3 to 8.8. The initial selection process of the requirements for the security risk analysis did not consider sections from *9.3 Item definition* to *9.5 Cybersecurity concept* as those requirements were related to either earlier or later design and concept phases. Also, *8.9 Risk treatment decision* was not taken into the requirements selection as it was interpreted to belong to a later concepting phase and not to the performing of the security risk analysis itself. (ISO/SAE, 2020.) However, during the research and development of the security risk analysis method, the selection of the requirements was extended. The extension of the requirements is described in chapter 3.3.2. The initially chosen sections for the security risk analysis are marked with a red square in the following figure (figure 8).

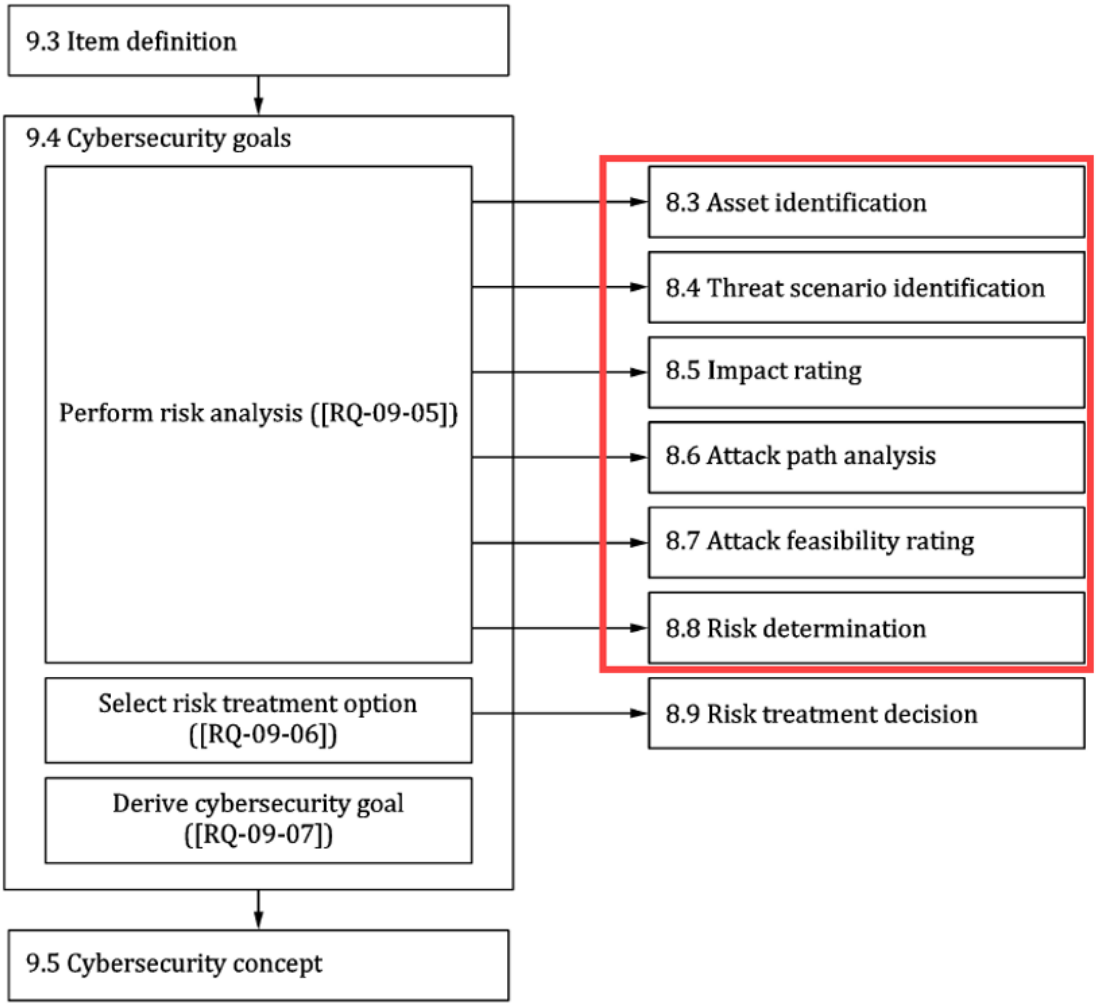

FIGURE 8 Chosen sections for security risk analysis (ISO/SAE, 2020, 80)

2.6 Security Risk Analysis Methods

Once the relevant sections and their requirements were decided from the cybersecurity engineering standard, the investigation of different security risk analysis methods could be started. It was acknowledged, that some methods regarding security risk analysis existed, like TARA, SAHARA and STRIDE, but there was no certainty if those methods could be used to reflect the requirements in the cybersecurity engineering standard. The research by Macher et al. (2016a) provided good insight what methods should be examined and considered. The elaboration of the investigation of security risk analysis methods is described in chapter 3.2 and beyond.

In general, the early security risk analysis is needed to tackle possible issues in the later vehicle lifecycle development phases. Just like safety, cybersecurity should be taken into consideration and be incorporated into early design phases of road vehicles to ensure safe and secure transportation. (SAE,

2016b.) It is important to define possible threat and damage scenarios, discover attack paths, measure attack impacts and feasibilities, and calculate the risks (ISO/SAE, 2020). All these matters were examined while investigating the security risk analysis methods to find the most promising method for further elaboration and development in the study.

2.7 Chapter Summary

This chapter discussed how the automotive industry has changed during the past decades and what it is today. Functional safety and dependability were explained and how they relate to automated driving. Cybersecurity was introduced generally and the related concepts, Internet of Things (IoT), Cyber-Physical Systems (CPS), and Cyber-Physical Vehicle Systems (CPVS) were elaborated. Vehicular communication section described the anatomy of in-vehicle communication and the types of external vehicle communication: Telematics and Infotainment, and Vehicle-to-Everything Communication (V2X). The external vehicular communication part also presented knowledge about Internet of Vehicles (IoV) and highlighted the importance of understanding the V2X cybersecurity threats. The automotive standards related to the study were assembled and the referencing procedure was clarified. Each standard was introduced, and their relevancy was justified. Finally, a short introduction to security risk analysis methods was given.

3 RESEARCH METHODS

This chapter discusses how the study was designed and executed, and what methodology was chosen to conduct the research. The study was implemented in several phases, and part of the phases contained iteration. Each phase is elaborated thoroughly.

The research design evolved to consist of three parts. First part was to investigate and compare the existing TARA compatible (SAE, 2016b) security risk analysis methods and to find the one which meets the cybersecurity requirements of the cybersecurity engineering standard (ISO/SAE, 2020). This part was called *Comparison of the different TARA approaches*. Second part contained the modelling of a new security risk analysis method based on the chosen analysis method and the requirements of cybersecurity engineering standard. The modelling was aimed to be carried out with SysML (Systems Modeling Language) (SysML.org, 2023) or MSTMT (Microsoft Threat Modeling Tool) (Microsoft, 2022). This part was called *Elaboration of the new approach*. Third part focused on use case creation and execution to test the applicability of the derived security risk analysis method and evaluate the use case with SPIDER, a robot vehicle (Virtual Vehicle, 2020b). This part was called *Application of the specific approach for the UC*. The research method used was Design Science (DS) (Simon, 1996) as the target was to make an IT artifact that solves the problem with a real-life solution, in this case, a security risk analysis method (March & Smith, 1995).

The outcome of the three parts met the expectations, even though plans were adjusted and iterated several times. During the first part of the research, it was acknowledged that from the pool of existing security risk analysis methods, there was not a single feasible method to meet the needed requirements of the cybersecurity engineering standard. Hence, a hybrid of two most adequate security risk analysis methods were used to create a new framework for the cybersecurity risk analysis aspect. The second part of the research was conducted by using Microsoft Office tools, Word, Excel, and PowerPoint. The SysML and MSTMT were found too time consuming and laborious in relation

to the demand from Virtual Vehicle and to the given schedule of the allocated project. The result of the second part was an Excel file, a spreadsheet, created specifically for Virtual Vehicle's internal usage of making a security risk analysis for use cases concerning cybersecurity of road vehicles. The third part was fulfilled by creating and actualizing a use case for the SPIDER robot vehicle. The use case was executed on paper as COVID-19 pandemic had outbursts during the implementation phase.

3.1 Design Science Research

Design Science Research (DSR) originates from the sciences of the artificial by Herbert Simon (1996) and from the engineering discipline. Simon (1996) considered design science to be research about how things could be. The purpose of DSR is to create something new with innovative artifacts to solve real-world problems. (vom Brocke, Hevner & Maedche, 2020.)

Scholars have different approaches to define design science research. One of the well-known researchers are March and Smith (1995) who compare the characteristics of natural science and design science in their study concerning research in the information technology domain. They argue that activities from both disciplines are required to make sure the relevancy and effectiveness is realized in technology-oriented IT research. The required research activities are to build, evaluate, theorize, and justify. Natural science (biological, physical, behavioral, and social) focuses on understanding reality and its activities are discovery and justification. Design science is technology-oriented, and it aims to create new solutions or alternatives as products which will avail human purpose with value or utility. In other words, design science aims to solve real world problems. The types of design science products are constructs, models, methods, and implementations, which are targeted to be valuable and innovative in nature. A typical product in IT research is an artifact which is practical rather than notional. The basic activities of design science research are to build and evaluate where building activity is for artifact creation and evaluation examines the artifact's performance. March and Smith (1995) created a research framework specified for information technology with a matrix containing the research activities and outputs adapted from design and natural sciences. (March & Smith, 1995.) The framework is presented in figure 9 (figure 9).

Research Activities

Research Outputs	Build	Evaluate	Theorize	Justify
Constructs				
Model				
Method				
Instantiation				

FIGURE 9 Research framework by March and Smith (1995, 255)

The research outputs (constructs, models, methods, and instantiations) are the artifacts from design science research, and they address tasks. The build and evaluate research activities are from design science and they improve performance. The theorize and justify activities are taken from natural science research and they propose and test theories. The cells in the framework contain the research efforts and have different objectives. The objectives are presented in figure 10 (figure 10). A design science study can include multiple cells but doesn't cover every unit, however. (March & Smith, 1995.)

Research Activities

Research Outputs	Build	Evaluate	Theorize	Justify
	Objectives: Bringing value or utility to a community of users. Artifact has utility for an important task. Tasks provide significant improvement like better performance.	**Objectives**: Developing metrics and comparing the performance of artifact for specific tasks.	**Objectives**: Explaining why and how the effects came about, i.e., why and how the constructs, models, methods, and instantiations work. Unifying the known data (observations of effects) into viable theory: explanations of how and why things happen.	**Objectives**: Performing empirical and/or theoretical research to test the theories posed. Posed and justified theories can provide direction for the development of additional and better technologies.
Constructs		• Characteristics: Completeness, simplicity, elegance, understandability, and ease of use. ➢ Example: Data modelling formalisms (logical structure of data).	➢ Example: How the constructs used in human-computer interaction affect performance.	
Model		• Characteristics: Fidelity with real world phenomena, completeness, level of detail, robustness, and internal consistency. ➢ Example: Mathematical models developed for database design problems.	➢ Example: Positing that a model used for design purposes is true, or as complicated as developing an explanatory model of an IT phenomena. ➢ Example: Adapting theories from base disciplines or developing new, general theories to explain how or why IT phenomena work.	
Method		• Characteristics: Operationality, efficiency, generality, and ease of use. ➢ Example: The ability to perform the intended task or the ability of humans to effectively use the method if it is not algorithmic.	➢ Example: Formal and mathematical theorizing with logical proofs being used for justification or behavioral, explaining why or how a method works in practice.	
Instantiation		• Characteristics: Efficiency and effectiveness of the artifact and its impacts on the environment and its users. ➢ Example: CASE tools.	➢ Example: Developing more general theories or as the specialization of an existing general theory.	

FIGURE 10 The objectives of the research activities (March & Smith, 1995)

The view of the design science research process by March and Smith (1995) is technology oriented whereas Vaishnavi, Kuechler and Petter (2004/2019) consider the process being both technology and information systems oriented. Vaishnavi et al. (2004/2019) lean strongly towards knowledge building through design in DSR (Design Science Research). They argue that developing artifacts for real world problems incorporates two important activities: 1) creating new knowledge with an artifact, and 2) the analysis of the artifact's performance. The knowledge actualizes as theories, constructs, models, methods, and techniques, all targeting to create artifacts which fill the research gap in question and are novel in nature. The artifacts are considered simply objects or processes. The design science research itself uses design, analysis, reflection, and abstraction for creating the missing knowledge. (Vaishnavi et al., 2004/2019.) Vaishnavi et al. (2004/2019) introduce Design Science Research Process Model (DSR Cycle) with five process steps: awareness of problem, suggestion, development, evaluation, and conclusion. Similar elements appear in many other DSR process models, like in the research framework (see figure 9) created by March and Smith (1995). (Vaishnavi et al., 2004/2019.)

Hevner, March, Park and Ram (2004) have a business and management related view concerning design science in information systems (IS) research. They define IS discipline forming of design science and behavioral science, a subset of natural sciences. Both paradigms are inseparable in IS as both concern people, organizations, and technology. Behavioral science research seeks the truth with theory, and design science research pursues utility with artifacts. Hevner et al. (2004) created a conceptual framework to illustrate IS research in view of behavioral and design sciences. The framework is presented in figure 11 and it is quite self-explanatory (figure 11). The IS research contains two phases where theory development and justification are addressed by behavioral science, and artifact building, and evaluation are directed by design science. The environment contains people, organizations and their related technologies defining the problems, opportunities, tasks, and goals. This so-called problem area is feeding business needs to IS research ensuring relevance to the research. The knowledge base contains foundations and methodologies which are the raw material for IS research. The foundational elements support the develop/build phase in the IS research whereas methodologies focuses on the justify/evaluate phase with guidelines. Applying the foundations and methodologies with applicable knowledge bring rigor to the IS research. (Hevner et al., 2004.)

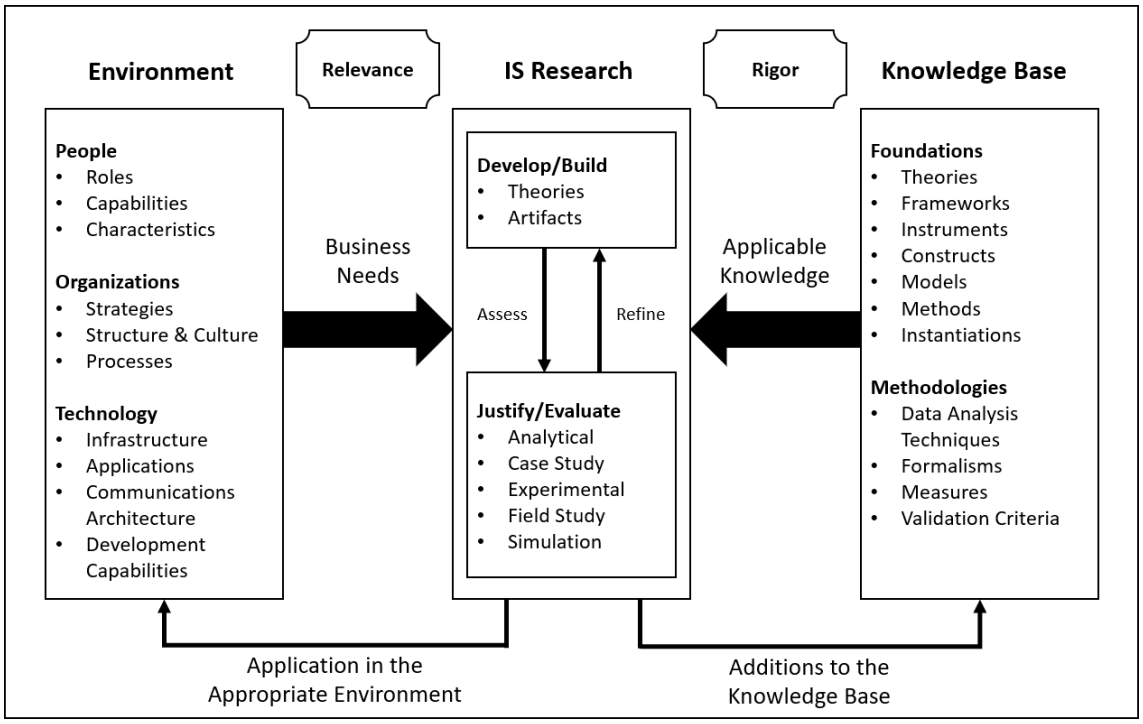

FIGURE 11 Information Systems Research Framework (Hevner et al., 2004, 80)

Another meaningful output from Hevner et al. (2004) are the seven guidelines for design science in IS research. The guidelines are presented in table 6 (table 6). The elements of the guidelines can be found in the Design Science Research Method (DSRM) process model created by Peffers, Tuunanen, Rothenberger and Chatterjee (2007). Peffers et al. (2007) focus purely into information systems domain in their design science research process. They created the DSRM process model to ease, increase and unify the design science research in IS domain with the help of a feasible methodology (Peffers et al., 2007).

TABLE 6 Design Science Research Guidelines (Hevner et al., 2004, 83)

Guideline	Description
Guideline 1: Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.

(continues)

Table 6 (continues)

Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Peffers et al. (2007) used seven representative studies as sources and gathered design science related components from them for the DSRM process model. From the seven studies, Hevner et al. (2004) had the most influence on constructing the DSRM process model. Peffers et al. (2007) defined three objectives for the concepting of the DSRM solution creation: "(1) provide a nominal process for the conduct of DS research, (2) build upon prior literature about DS in IS and reference disciplines, and (3) provide researchers with a mental model or template for a structure for research outputs." (Peffers et al., 2007, 50). The DSRM process model is presented in figure 12 (figure 12). The model consists of six activities:

1. Problem identification and motivation
2. Define the objectives for a solution
3. Design and development
4. Demonstration
5. Evaluation
6. Communication

The process is iterative and typically activities between 2 and 5 are being repeated until a feasible solution is developed. The starting points of the research are illustrated below the activities. Any of the first four activities can be the entry point for the study. (Peffers et al., 2007.) The DSRM process model will be elaborated in detail in chapter 4 Findings, when discussing the outcome of the study.

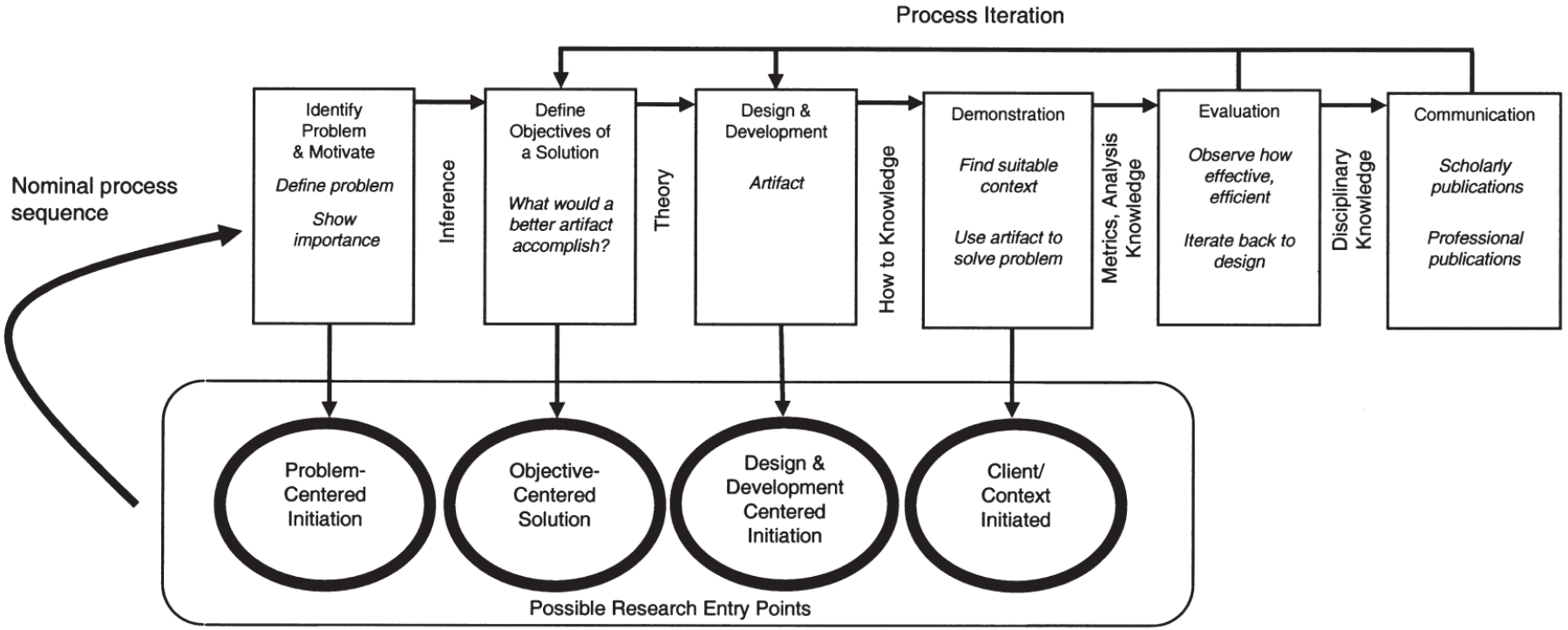

FIGURE 12 DSRM Process Model (Peffers et al., 2007, 54)

3.2 Investigation of Different Security Risk Analysis Methods

The investigation of security risk analysis methods started from TARA, SAHARA and STRIDE methods as recommended by Virtual Vehicle as they had been using these methods in their research projects. The basic knowledge of risk analysis existed on these certain methods; thus, the methods formed the initial starting point. Another TARA method created by Intel corporation (Rosenquist, 2009) was discovered from the academic literature and it was chosen to be analysed together with the three initially chosen methods.

The first set of methods to be analysed can be seen in table 7 (table 7). The order of methods is listed as per priority and not in alphabetical order. The most important method to be evaluated was TARA as it represents pure security. SAHARA is the second to be evaluated as it represents the vehicular hazard analysis presented by the functional safety standard (ISO, 2018). STRIDE is evaluated before TARA Intel as TARA Intel was discovered later in the process. Further on, the new methods found during the investigation process are listed in a random order.

TABLE 7 First set of security risk analysis methods

Security risk analysis method	**Description**
TARA	Threat Analysis and Risk Assessment (SAE, 2016b)
SAHARA	Security Aware Hazard Analysis and Risk Assessment (Macher, Sporer, Berlach, Armengaud & Kreiner, 2015)
STRIDE	Spoofing Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (Microsoft Corporation, 2005)
TARA Intel	Threat Agent Risk Assessment (Rosenquist, 2009)

The examination process was started with TARA as it was introduced in the initial standard concerning vehicular cybersecurity. When studying TARA, it appeared to be more of a framework and a high-level guidance instead of an actual security risk analysis method itself. TARA provided general background information, and metrics and technical facts what to consider when making security risk analysis. Specific measures are defined in other standards by ISO and SAE. TARA can be seen being more an objective than specific approach. According to cybersecurity guidebook (SAE J3061), TARA (Threat Analysis and Risk Assessment) is an analysis technique (SAE, 2016b) described as the following:

> An analysis technique that is applied in the concept phase to help identify potential threats to a feature and to assess the risk associated with the identified threats. Identifying the potential threats and assessing the risk associated with these threats, allows an organization to prioritize follow-on Cybersecurity activities associated with the threats so efforts and resources can be focused on the highest priority threats. (SAE, 2016b, 15.)

The cybersecurity guidebook was chosen to be the starting point for the security risk analysis method investigation. The guidebook introduced the TARA analysis technique and recommended TARA applicable security risk analysis methods. The guidebook recommended four different analysis methods which were stated to be TARA compatible. The recommended methods can be seen in the following table (table 8).

TABLE 8 Security risk analysis methods recommended by SAE J3061 (2016b, 70)

Security risk analysis method	**Description**
EVITA	E-Safety Vehicle Intrusion Protected Applications (Ruddle et al., 2009; SAE, 2016b)
TVRA	Threat, Vulnerability and Risk Assessment (ETSI, 2010; SAE, 2016b)
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation (Alberts, Behrens, Pethia & Wilson, 1999; SAE, 2016b)
HEAVENS	HEAling Vulnerabilities to ENhance Software Security and Safety (Lautenbach & Islam, 2016; SAE, 2016b)

However, a closer examination of the recommended methods revealed that not all of them were applicable in the automotive domain. More feasible security risk analysis methods were proposed by Macher et al. (2016a) in their research review and the those proposed methods were taken under analysis in this study. The selection of the methods was based on an automotive use case concerning safety and security. (Macher et al., 2016a.) The important criteria for the study were that the proposed methods should fulfil the requirements from the cybersecurity engineering standard. The proposed methods by Macher et al. (2016a) can be seen in the following table (table 9).

TABLE 9 Security risk analysis methods recommended by Macher et al. (2016a)

Security risk analysis method	**Description**
EVITA	E-Safety Vehicle Intrusion Protected Applications (Ruddle et al., 2009; SAE, 2016b)
HEAVENS	HEAling Vulnerabilities to ENhance Software Security and Safety (Lautenbach & Islam, 2016; SAE, 2016b)

(continues)

Table 9 (continues)

SAHARA	Security Aware Hazard Analysis and Risk Assessment (Macher et al., 2015)
BRA	Binary Risk Analysis (Sapiro, 2011)

As recommended by Macher et al. (2016a) in their research, the selection of security risk analysis methods to be analysed in the study were chosen to be EVITA, HEAVENS, SAHARA and BRA, and TARA Intel was kept as a comparison to TARA. STRIDE was excluded at this point as it was related to the software level and not to the system level where TARA approach is applicable. The second set of methods to be analysed can be seen in the following table (table 10).

TABLE 10 Second set of security risk analysis methods

Security risk analysis method	**Description**
EVITA	E-Safety Vehicle Intrusion Protected Applications (Ruddle et al., 2009; SAE, 2016b)
HEAVENS	HEAling Vulnerabilities to ENhance Software Security and Safety (Lautenbach & Islam, 2016; SAE, 2016b)
SAHARA	Security Aware Hazard Analysis and Risk Assessment (Macher et al., 2015)
BRA	Binary Risk Analysis (Sapiro, 2011)
TARA Intel	Threat Agent Risk Assessment (Rosenquist, 2009)

During the analysis of the chosen five methods, TARA+ method was discovered from the academic literature as well as TARA by MITRE corporation, MoRA, SARA and SINA. The new methods that were found were briefly examined if they were compatible with TARA approach in the automotive domain. It was discovered that TARA by MITRE corporation, MoRA and SINA did not meet the required needs to be taken into further analysis. TARA by MITRE corporation focused on Department of Defense in IT domain and it was customized for military purposes (Wynn et al., 2011). MoRA was in line with the cybersecurity standards but after investigating further, MoRA did not meet the requirements which were essential for the method analysis. MoRA was a graph-based modelling approach with high-level descriptions and short with details. (Angermeier, Beilke, Hansch & Eichler, 2019.) SINA had too specific topic regarding security networking of automotive systems and could not be applied with cybersecurity standards (Schmidt et al., 2014). The methods rejected can be seen in the following table (table 11).

TABLE 11 Security risk analysis methods rejected

Security risk analysis method	Description
TARA by MITRE corporation	Threat Assessment & Remediation Analysis (Wynn et al., 2011)
MoRA	Modular Risk Assessment (Angermeier, Beilke, Hansch & Eichler, 2019)
SINA	Security in Networked Automotive Systems (Schmidt et al., 2014)

TARA+ method was discovered to be an extension to existing TARA approach. TARA+ was using a method called SARA as its core, so SARA method was examined as well. SARA was compatible with the cybersecurity engineering standard, and it was taken into further analysis together with TARA+. The number of methods to be examined rose to seven in total. The third and final set of methods to be analysed can be seen in the following table (table 12).

TABLE 12 Third and final set of security risk analysis methods

Security risk analysis method	Description
EVITA	E-Safety Vehicle Intrusion Protected Applications (Ruddle et al., 2009; SAE, 2016b)
HEAVENS	HEAling Vulnerabilities to ENhance Software Security and Safety (Lautenbach & Islam, 2016; SAE, 2016b)
SAHARA	Security Aware Hazard Analysis and Risk Assessment (Macher et al., 2015)
BRA	Binary Risk Analysis (Sapiro, 2011)
TARA Intel	Threat Agent Risk Assessment (Rosenquist, 2009)
TARA+	Controllability-aware Threat Analysis and Risk Assessment (Bolovinou et al., 2019)
SARA	Security Automotive Risk Analysis (Monteuuis et al., 2018)

The seven chosen methods were analysed and compared using a matrix framework created with MS Excel. The comparison matrix is further elaborated in the study. The chosen methods can be seen in figure 13 in a chronological order by the year they were published (figure 13).

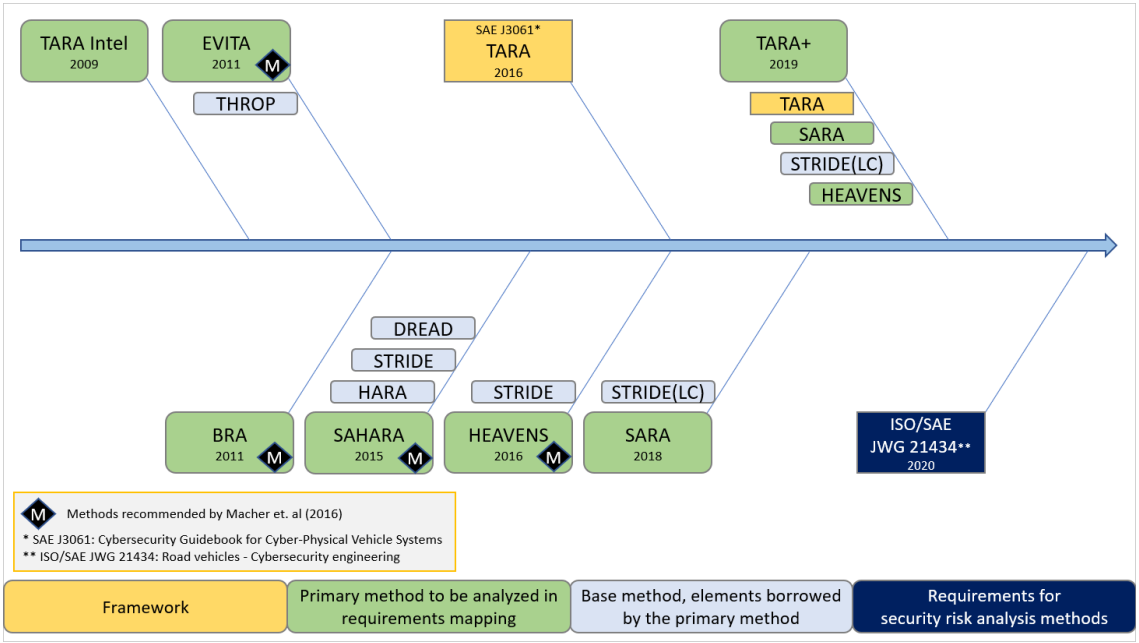

FIGURE 13 Security Risk Analysis Methods

The yellow box presents the TARA framework taken from the cybersecurity guidebook. The green boxes present the chosen methods to be analysed and the black diamond boxes with letter M indicate the methods recommended by Macher et al. (2016a). The light grey boxes present the base methods whose elements are borrowed by other methods. The dark blue box presents the new cybersecurity engineering standard which provides the requirements for the security risk analysis methods (ISO/SAE, 2020).

3.2.1 Evaluation of Security Risk Analysis Methods

The purpose of the method examination and analysis was, that once the appropriate method is determined, a security risk analysis in early design phases can be implemented and evaluated. Before deciding what the most suitable method is, all candidate methods should be evaluated. Then, the best practices of the selected risk analysis methods are gathered and compared based on the given requirements in the cybersecurity engineering standard. If a suitable risk analysis method which meets the criteria cannot be addressed, a new risk analysis method will be derived from the existing methods. The chosen or created risk analysis method will be the basis for the solution concept creation. The solution could be implemented as a model, a process or as a concept depending on which approach serves the target the most.

The evaluation of security risk analysis methods included a comparison of the pros and cons of the existing methods with an overview of each method and a short description. A mapping of requirements to specific methods by metrics and argumentation was carried out.

Terminology caused issues with interpretation. At first glance it seemed a method would not fulfil much of the requirements but once studying further, the different terminology could be considered to mean the same as the requirement intended. This however did not prevent possible misinterpretations. The terminology interpretation also worked the other way around. A promising method seemed plausible by its description, but in closer examination the method was not compatible with the given requirements.

None of the chosen methods managed to fulfil the requirements without borrowing elements from another method or methods. All feasible methods used at least one additional method. There were also issues among the different methods which are elaborated further in the study. SAHARA, HEAVENS, and TARA+ for example were borrowing elements from other methods but did not specify what the elements are exactly. A lot of assuming had to be done, as well as studying the borrowed methods to understand what the shared elements are. An issue rose whether TARA+ should be replaced with SARA as TARA+ was borrowing basically the whole concept from SARA. TARA+ was kept however as its own method since TARA+ provided an extension with automated driving features that could be evaluated with the planned use case in the study. Table 13 shows the selected methods, their reference articles and included additional methods (table 13).

TABLE 13 Overview of security risk analysis methods

Security risk analysis method (See definitions in table 12)	**Included Methods**	**References Used**
EVITA	THROP	Ruddle, A., Ward, D., Weyl, B., Idrees, S., Roudier, Y., Friedewald, M., ... & Wolf, M. (2009). Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios. *EVITA project*. SAE. (2016b). J3061: Cybersecurity guidebook for cyber-physical vehicle systems. *Society for automotive engineers*. Macher, G., Armengaud, E., Brenner, E., & Kreiner, C. (2016, September). A review of threat analysis and risk assessment methods in the automotive context. In *International Conference on Computer Safety, Reliability, and Security* (pp. 130-141). Springer, Cham. E-safety Vehicle Intrusion proTected Applications (EVITA) Project (2008). https://www.evita-project.org/

(continues)

Table 13 (continues)

HEAVENS	STRIDE	Lautenbach, A., & Islam, M. (2016). HEAVENS–HEAling Vulnerabilities to ENhance Software Security and Safety. *The HEAVENS Consortium (Borås SE)*. Islam, M. M., Lautenbach, A., Sandberg, C., & Olovsson, T. (2016, May). A risk assessment framework for automotive embedded systems. In *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security* (pp. 3-14). SAE. (2016b). J3061: Cybersecurity guidebook for cyber-physical vehicle systems. *Society for automotive engineers*. Macher, G., Armengaud, E., Brenner, E., & Kreiner, C. (2016a, September). A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context. In *International Conference on Computer Safety, Reliability, and Security* (pp. 130-141). Springer International Publishing.
SAHARA	HARA STRIDE DREAD	Macher, G., Sporer, H., Berlach, R., Armengaud, E., & Kreiner, C. (2015, March). SAHARA: a security-aware hazard and risk analysis method. In *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)* (pp. 621-624). IEEE. Macher, G., Armengaud, E., Brenner, E., & Kreiner, C. (2016a, September). A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context. In *International Conference on Computer Safety, Reliability, and Security* (pp. 130-141). Springer International Publishing. Macher, G., Armengaud, E., Brenner, E., & Kreiner, C. (2016b). Threat and risk assessment methodologies in the automotive domain. *Procedia computer science, 83*, 1288-1294.

(continues)

Table 13 (continues)

BRA	-	Sapiro, B. (2011) Binary Risk Analysis. *Creative Commons License, 1*. Macher, G., Armengaud, E., Brenner, E., & Kreiner, C. (2016a, September). A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context. In *International Conference on Computer Safety, Reliability, and Security* (pp. 130-141). Springer International Publishing.
TARA Intel	-	Casey, T. (2007). Threat agent library helps identify information security risks. *Intel White Paper, 2*. Rosenquist, M. (2009). Prioritizing information security risks with threat agent risk assessment. *Intel Corporation White Paper*. Karahasanovic, A., Kleberger, P., & Almgren, M. (2017, November). Adapting threat modeling methods for the automotive industry. In *Proceedings of the 15th ESCAR Conference* (pp. 1-10).
TARA+	TARA SARA STRIDE(LC) HEAVENS	Bolovinou, A., Atmaca, U. I., Sheik, A. T., Ur-Rehman, O., Wallraf, G., & Amditis, A. (2019, June). TARA+: Controllability-aware Threat Analysis and Risk Assessment for L3 Automated Driving Systems. In *2019 IEEE Intelligent Vehicles Symposium (IV)* (pp. 8-13). IEEE.
SARA	STRIDE(LC)	Monteuuis, J. P., Boudguiga, A., Zhang, J., Labiod, H., Servel, A., & Urien, P. (2018, May). Sara: Security automotive risk analysis method. In *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security* (pp. 3-14).

3.2.2 Elaboration of the Comparison Matrix

The requirements and recommendations were gathered from the cybersecurity engineering standard (ISO/SAE JWG 21434). There were in total 11 requirements and 5 recommendations. Under one requirement there were 4 sub-criteria which made the total amount of criteria 20. The requirement management was handled with MS Excel as requested by Virtual Vehicle to

cohere with their working tools and practises. All requirements and recommendations and their further term descriptions, related figures and tables were so large they could not be fit to the created comparison matrix. Thus, all the materials related to the criteria was copied in its original form to a separate Word document (later: requirements elaboration) to provide detailed information.

The comparison matrix contained all requirements and recommendations copied from the cybersecurity engineering standard as in their high-level descriptions without further elaboration. The detailed descriptions are in the related requirements elaboration. Requirements are presented in colour blue, and recommendations in colour orange in the comparison matrix to be differentiated from each other. The requirements and recommendations are positioned on the left of the matrix and on the right side are gathered the chosen 7 security risk analysis methods. Under each method there are two categories: coverage and justification. The coverage category presents the metrics how the method covers each criterion. The three metrics were set to be: Fully covered 67-100%, Partly covered 34-66%, and Not covered 0-33%. These values were given by senior researchers from Virtual Vehicle. The justification category presents the rationale why or why not and how the method covers the given requirement or recommendation. The justification is a shorter summary taken from the related requirements elaboration. An example of the comparison matrix can be seen in figure 14, where the coverage category is visible, but justification category is hidden (figure 14). The selection in the figure is partial and does not cover the whole matrix. The full version is presented in the Appendix 1. Sections 8.3, 8.4 and 8.5 are an example sample. The green colour means full coverage of the requirement in question, yellow presents partial coverage, and the orange colour means that the requirement is not covered by the method in question.

The requirements and recommendations are listed under 6 main topics presented in the cybersecurity engineering standard. The main topics are:

- 8.3 Asset Identification
- 8.4 Threat Scenario Identification
- 8.5 Impact Rating
- 8.6 Attack Path Analysis
- 8.7 Attack Feasibility Rating
- 8.8 Risk Determination

ISO/SAE JWG 21434 requirements	EVITA (+THROP)	HEAVENS (+STRIDE)	SAHARA (HARA+STRIDE +DREAD)	BRA	TARA Intel	SARA (+STRIDE(LC))	TARA+ (TARA+SARA +STRIDE(LC) +HEAVENS)
	COVERAGE	COVERAGE	COVERAGE	COVERAGE	COVERAGE	COVERAGE	COVERAGE
8.3 Asset Identification							
[RQ-08-01] Damage scenarios shall be identified.	Fully covered with THROP	Fully covered with STRIDE	Partly covered	Partly covered	Fully covered	Fully covered with STRIDE(LC)	Fully covered with SARA (Fully covered with STRIDE(LC))
[RQ-08-02] Assets with cybersecurity properties whose compromise leads to a damage scenario shall be enumerated.	Fully covered with THROP	Fully covered	Partly covered	Partly covered	Fully covered	Fully covered	Fully covered with SARA
8.4 Threat Scenario Identification							
[RQ-08-03] Threat scenarios shall be identified.	Fully covered	Fully covered	Partly covered	Not covered	Partly covered	Fully covered	Fully covered with SARA
8.5 Impact Rating							
[RQ-08-04] The damage scenarios shall be assessed against potential adverse consequences for stakeholders in the independent impact categories of safety, financial, operational, and privacy (S, F, O, P).	Fully covered with THROP	Fully covered	Partly covered	Not covered	Not covered	Fully covered	Fully covered with HEAVENS and SARA
[RQ-08-05] If further impact categories are considered beyond S, F, O and P, then those categories shall be documented.	Not covered	Fully covered	Not covered	Not covered	Not covered	Fully covered	Fully covered with TARA+, HEAVENS and SARA
[RQ-08-06] The impact rating of the damage scenario shall be determined to be one of the following:	Fully covered	Fully covered	Partly covered	Not covered	Not covered	Fully covered	Fully covered with HEAVENS and SARA

FIGURE 14 Excerpt from the full comparison matrix

As described in chapter 3.2, the chosen methods to be evaluated were selected along the evaluation process. The coverage and justification were conducted for each method and are shortly presented here.

EVITA (+THROP)

EVITA (E-Safety Vehicle Intrusion Protected Applications) as presented by the cybersecurity guidebook standard, is one of the labelled TARA methods (SAE, 2016b). EVITA was an EU funded project during 2008 and 2011. The objective for the project was to create an architecture for on-board networks of a vehicle and protect the cybersecurity related components. (SAE, 2016b.)

EVITA is borrowing elements from another method called THROP (Threat and Operability Analysis). THROP is introduced in the cybersecurity guidebook standard as an analysis technique which aims to identify potential threats of a feature and gives guidewords for functionalities of the feature. (SAE, 2016b.)

EVITA succeeded in the requirements mapping activity well together with THROP and received third position in the ranking of the most covering method. EVITA (+THROP) had full coverage of almost all requirements and recommendations:

- Fully covered: 16/20
    - 3 of the 16 are fully covered with THROP

- Not covered: 4/20

HEAVENS (+STRIDE)

HEAVENS (HEAling Vulnerabilities to ENhance Software Security and Safety) is another labelled TARA method by the cybersecurity guidebook standard (SAE, 2016b). HEAVENS was a Swedish project during 2013 and 2016. The project focused on vehicular E/E (electrical and/or electronic) systems. The project goals consisted of for example the construction of cybersecurity models via threat and vulnerability identification. Automotive standards like ISO 26262 were examined to investigate safety aspect and interplay with cybersecurity. (SAE, 2016b.)

HEAVENS is using elements from additional method called STRIDE (Spoofing Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege). STRIDE is created by Microsoft and it is a model-based threat modelling technique. STRIDE provides four steps how to model the system in question, and map, elicit and document the related threats. There are six categories of threats which are the terms behind each letter of the word STRIDE. (Scandariato et al., 2015.)

HEAVENS succeeded in the requirements mapping activity mediocre together with STRIDE and received fourth position in the ranking of the most covering method. HEAVENS (+STRIDE) had full or partial coverage of almost all requirements and recommendations:

- Fully covered: 13/20
  - 1 of the 13 are fully covered with STRIDE
- Partly covered: 4/20
  - 3 of the 4 are partly covered with STRIDE
- Not covered: 3/20

SAHARA (HARA+STRIDE+DREAD)

SAHARA (Security Aware Hazard Analysis and Risk Assessment) is a TARA method created by Macher et al. (2015). SAHARA is a combination of two methods, HARA and STRIDE. HARA (Hazard Analysis and Risk Assessment) is introduced in functional safety standard and it is a method which helps to find hazardous vehicular events. It also specifies safety goals and automotive security integrity levels (ASIL) to prevent the possible hazards and avoid unreasonable risk. (ISO, 2018.)

STRIDE was added into the SAHARA method as the security approach method (Macher et al., 2015) but later, Macher et al. tried to implement DREAD, a classification scheme, to cover the SAHARA's security aspect and impact rating. The results were poor, however. DREAD stands for Damage Potential,

Reproducibility, Exploitability, Affected Users and Discoverability. DREAD's purpose is to provide impact factors which eventually result a risk priority number for the threats. Unfortunately, the approach was not in line with the given requirements of the cybersecurity engineering standard. (Macher et al., 2016b.)

SAHARA was restricted to safety aspect only and no financial, operational or privacy aspects were given which were key elements among the requirements. Thus, SAHARA did not cover much of the requirements and recommendations or had very limited coverage. (Macher et al., 2016a.) SAHARA took fifth position in the ranking of the most covering method. Little over half of the requirements were partly covered due to the focus being only on safety aspect:

- Fully covered: 2/20
- Partly covered: 11/20
- Not covered: 7/20

BRA

BRA (Binary Risk Analysis) is presented by Macher et al. (2016a) as a TARA compatible method. The method works as its own without borrowing any elements from other methods. BRA was developed by Ben Sapiro in 2011. It is a lightweight risk assessment method determining threats and estimating the threat impacts with agreed steps. The steps consist of answering to ten yes/no questions, mapping the answers to matrices, and further on using given results to get a final risk metric. (Macher et al., 2016a)

BRA had almost non-existence coverage of the requirements and recommendations, and it did not meet TARA principles in the long run. BRA declared itself that it is not a full risk management method, nor does it provide quantitative analysis or manage threat discovery (Sapiro, 2011). This raises a concern why it was chosen by Macher et al. (2016a) in the first place. It needs to be addressed however, that the cybersecurity engineering standard was published four years after the review of TARA methods Macher et al. (2016a) made.

BRA positioned in the seventh and last place in the ranking the of most covering method with its poor coverage results:

- Partly covered: 2/20
- Not covered: 18/20

TARA Intel

TARA Intel (Threat Agent Risk Assessment) was developed by Matt Rosenquist in 2009 at Intel Corporation. Intel's version of TARA was chosen to be evaluated as it profiles people, agents, who can cause threats. Intel's version analyses what kind of skills the person must have to attack, and then decides the attacker profile. TARA Intel uses three libraries: Threat Agent Library (TAL), Common Exposure Library (CEL), and Methods and Objectives Library (MOL). (Rosenquist, 2009.)

Despite the same acronym TARA Intel uses, it does not fulfil the needs of the cybersecurity engineering standard and TARA framework defined in cybersecurity guidebook standard. Even though Karahasanovic et al. (2017) attempted to make an adaptation of TARA Intel for automotive industry via changes in TAL and MOL characteristics, the adaptation did not meet the given requirements.

TARA Intel took the sixth place in the ranking of the most covering method with its almost non-existent coverage:

- Fully covered: 2/20
- Partly covered: 1/20
- Not covered: 17/20

SARA (+STRIDE(LC))

SARA (Security Automotive Risk Analysis) was created by Monteuuis et al. (2018) in their research of connected and automated vehicles. The existing security risk analysis methods are mainly focusing on risk computation with the driver being in control but are lacking the driverless system factor. SARA aims to fill the gaps in the existing methods concerning driverless vehicles by presenting new metrics called Observation and Controllability. SARA also presents improvements and novelty in threat modelling, attack method and asset mapping, and adding an attacker to the attack tree. SARA implements the method STRIDE(LC), which is an extension to STRIDE. Added L stands for Linkability, and C for Confusion. (Monteuuis et al., 2018.) SARA method is elaborated further in chapter 3.3.

SARA can be considered to fully cover all the requirements and recommendations as the two not covered criteria were optional (1/3 of the options is covered). SARA positioned in the second place in the ranking of the most covering method:

- Fully covered: 18/20
  - 1 of the 18 are fully covered with STRIDE(LC)
- Not covered: 2/20

TARA+ (TARA+SARA+STRIDE(LC)+HEAVENS)

TARA+ (Controllability-aware Threat Analysis and Risk Assessment) was created by Bolovinou et al. (2019) as a part of an EU funded project L3Pilot. The method is based on TARA framework from the cybersecurity guidebook (SAE, 2016b). The TARA+ method could be described as a hybrid of different security risk analysis methods as it borrows elements from HEAVENS and STRIDE and uses the same concept as SARA. The novelty of TARA+ is within the controllability factor taken from SARA and split into two components: one component for the driver of the vehicle, and the other component for the system of the vehicle. (Bolovinou et al., 2019.)

Like SARA, TARA+ can be considered to fully cover all the requirements and recommendations. TARA+ positioned in the first place in the ranking of the most covering method:

- Fully covered: 18/20
  - 7 of the 18 are fully covered with HEAVENS and SARA
  - 7 of the 18 are fully covered with SARA
  - 1 of the 18 are fully covered with SARA (with STRIDE(LC))
  - 2 of the 18 are fully covered with SARA and TARA+
  - 1 of the 18 are fully covered with TARA+, HEAVENS and SARA
- Not covered: 2/20

3.2.3 The Decision of the Chosen Method

The evaluation of the methods brings to the ranking of the methods. The methods were prioritized to the most covering order:

1. TARA+ (TARA+SARA+ STRIDE(LC)+HEAVENS)
2. SARA (+STRIDE(LC))
3. EVITA (+THROP)
4. HEAVENS (+STRIDE)
5. SAHARA (HARA+STRIDE+DREAD)
6. TARA Intel (Threat Agent Risk Assessment)
7. BRA

The overview of the ranking of the methods is gathered into table 14 with the justifications how the method managed to fulfil the requirements and recommendations or if it failed to meet the targets (table 14).

TABLE 14 Justification for the ranking of the methods

Method	Coverage and Justifications
TARA+	• Fully covered with HEAVENS and SARA: 7/20 • Fully covered with SARA: 7/20 • Fully covered with SARA (Fully covered with STRIDE(LC)): 1/20 • Fully covered with SARA and TARA+: 2/20 • Fully covered with TARA+, HEAVENS and SARA: 1/20 • Not covered: 2/20 The TARA+ method could be described as a hybrid of different security risk analysis methods as it borrows elements from HEAVENS and STRIDE and uses the same concept as SARA. The novelty of TARA+ is within the controllability factor taken from SARA and split into two components: one component for the driver of the vehicle, and the other component for the system of the vehicle. (Bolovinou et al., 2019.) Like SARA, TARA+ can be considered to fully cover all the requirements and recommendations. TARA+ positioned in the first place in the ranking of the most covering method.
SARA	• Fully covered: 17/20 • Fully covered with STRIDE(LC): 1/20 • Not covered: 2/20 SARA aims to fill the gaps in the existing security risk analysis methods concerning driverless vehicles by presenting new metrics called Observation and Controllability. SARA also presents improvements and novelty in threat modelling, attack method and asset mapping, and adding an attacker to the attack tree. SARA implements the method STRIDE(LC), which is an extension to STRIDE. Added L stands for Linkability, and C for Confusion. (Monteuuis et al., 2018.) SARA can be considered to fully cover all the requirements and recommendations as the two not covered criteria were optional (1/3 of the options is covered). SARA positioned in the second place in the ranking of the most covering method.
EVITA	• Fully covered: 13/20 • Fully covered with THROP: 3/20 • Not covered: 4/20 EVITA is borrowing elements from another method called THROP (Threat and Operability Analysis). THROP is introduced in the cybersecurity guidebook standard as an analysis technique which aims to identify potential threats of a feature and gives guidewords for functionalities of the feature. (SAE, 2016b.) EVITA succeeded in the requirements mapping activity well together with THROP and received third position in the ranking of the most covering method. EVITA (+THROP) had full coverage of almost all requirements and recommendations.

(continues)

Table 14 (continues)

HEAVENS	• Fully covered: 12/20 • Fully covered with STRIDE: 1/20 • Partly covered: 1/20 • Partly covered with STRIDE: 3/20 • Not covered: 3/20 HEAVENS is using elements from additional method called STRIDE (Spoofing Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege). STRIDE is created by Microsoft and it is a model-based threat modelling technique. STRIDE provides four steps how to model the system in question, and map, elicit and document the related threats. There are six categories of threats which are the terms behind each letter of the word STRIDE. (Scandariato et al., 2015.) HEAVENS succeeded in the requirements mapping activity mediocre together with STRIDE and received fourth position in the ranking of the most covering method. HEAVENS (+STRIDE) had full or partial coverage of almost all requirements and recommendations.
SAHARA	• Fully covered: 2/20 • Partly covered: 11/20 • Not covered: 7/20 SAHARA was restricted to safety aspect only and no financial, operational or privacy aspects were given which were key elements among the requirements. Thus, SAHARA did not cover much of the requirements and recommendations or had very limited coverage. (Macher et al., 2016a.) SAHARA took fifth position in the ranking of the most covering method. Little over half of the requirements were partly covered due to the focus being only on safety aspect.
TARA Intel	• Fully covered: 2/20 • Partly covered: 1/20 • Not covered: 17/20 Despite the same acronym TARA Intel uses, it does not fulfil the needs of the cybersecurity engineering standard and TARA framework defined in cybersecurity guidebook standard. Even though Karahasanovic et al. attempted to make an adaptation of TARA Intel in 2017 for automotive industry via changes in TAL and MOL characteristics, the adaptation did not meet the given requirements. TARA Intel took the sixth place in the ranking of the most covering method with its almost non-existent coverage.

(continues)

Table 14 (continues)

BRA	• Partly covered: 2/20 • Not covered: 18/20 BRA had almost non-existence coverage of the requirements and recommendations, and it did not meet TARA principles in the long run. BRA declared itself that it is not a full risk management method, nor does it provide quantitative analysis or manage threat discovery (Sapiro, 2011). This raises a concern why it was chosen by Macher et al. (2016a) in the first place. It needs to be addressed however, that the cybersecurity engineering standard was published four years after the review of TARA methods Macher et al. (2016a) made. BRA positioned in the seventh and last place in the ranking the of most covering method with its poor coverage results.

TARA+ was chosen to be the best method to be implemented when validating the use case created for the study. The reasoning for choosing TARA+ instead of SARA, which also was a very viable method, can be summarized in three facts. Firstly, TARA+ uses SARA as a base and SARA covers all requirements and recommendations with STRIDE(LC) (the extension of STRIDE). Secondly, TARA+ uses HEAVENS to cover cybersecurity engineering standard section *8.5 Impact Rating* to correspond with functional safety standard ISO 26262. SARA does not refer directly to functional safety standard, but it uses the same concept. Thirdly, TARA+ brings an extension of automation levels to impact categories in cybersecurity engineering standard's section *8.5 Impact Rating* by dividing Controllability category, originated from functional safety standard (ISO, 2018) and used by SARA, into two components: one for the driver and one for the system. Thus TARA+ gives a total coverage of all requirements and adds extension with impact categories concerning driving automation levels.

3.3 Elaboration of the Chosen Method

TARA+ describes itself being based on the Threat Analysis and Risk Assessment (TARA) framework of cyber security analysis (SAE, 2016b). TARA+ is using SARA method's concept as its basis and hence applying STRIDE(LC) which is the additional method used and extended by SARA (Monteuuis et al., 2018). In addition, TARA+ applies HEAVENS method's impact rating as it is in line with the functional safety standard (Islam, Lautenbach, Sandberg & Olovsson, 2016). The extra which TARA+ offers, is within the SARA's controllability impact factor being split into two components. However, that is as far as TARA+ goes with its features. The framework of TARA+ is very specific and narrow compared to the framework of SARA which is covering security risk analysis from feature definition to risk countermeasures. It is essential to emphasize that the actual framework of security risk analysis used in this study is based on the framework of SARA method and enriched with

TARA+ method. The features of TARA+ fulfil the requirements of the cybersecurity engineering standard in small and partial way, or not at all. Nevertheless, TARA+ was the chosen method based on the reasoning in previous chapter.

3.3.1 Mapping the Frameworks

The mapping of requirements and recommendations of the cybersecurity engineering standard to the chosen security risk analysis method was explained in chapter 3.2.2. The mapping of the requirements and recommendations is illustrated in this section. Figure 15 presents the framework of the cybersecurity engineering standard requirements and recommendations (figure 15) whereas figure 16 is the framework of SARA method (figure 16).

8.3 Asset Identification
[RQ-08-01] Damage scenarios shall be identified.
[RQ-08-02] Assets with cybersecurity properties whose compromise leads to a damage scenario shall be enumerated.
8.4 Threat Scenario Identification
[RQ-08-03] Threat scenarios shall be identified.
8.5 Impact Rating
[RQ-08-04] The damage scenarios shall be assessed against potential adverse consequences for stakeholders in the independent impact categories of safety, financial, operational, and privacy (S, F, O, P).
[RQ-08-05] If further impact categories are considered beyond S, F, O and P, then those categories shall be documented.
[RQ-08-06] The impact rating of the damage scenario shall be determined to be one of the following: Safety Impact Rating Financial Impact Rating Operational Impact Rating Privacy Impact Rating
[RQ-08-07] Safety related impacts shall be derived from ISO 26262-3:2018, 6.4.3 Classification of hazardous events.
8.6 Attack Path Analysis
[RQ-08-08] The threat scenarios shall be analyzed to describe possible attack paths.
[RQ-08-09] The attack path analysis approach applied shall be documented.
[RC-08-01] The attack path description should include a reference to the threat scenarios that can be realized by the attack path.
8.7 Attack Feasibility Rating
[RQ-08-10] For each attack path the attack feasibility rating shall be determined as one of the following: High Medium Low Very low
[RC-08-02] The defined rating method should be based on one of the following assessment approaches: a) attack potential-based approach; b) CVSS based approach; or c) attack vector-based approach.
[RC-08-03] If an attack potential-based approach is used, it should be determined based on core factors including elapsed time, specialist expertise, knowledge of the item or component, window of opportunity, and equipment.
[RC-08-04] If a CVSS based approach is used, it should be determined based on the exploit metrics group of the base metrics, including attack vector, attack complexity, privileges required, and user interaction.
[RC-08-05] If an attack vector-based approach is used, it should evaluate the predominant attack vector (cf. CVSS) of the attack path.
8.8 Risk Determination
[RQ-08-11] The risk value of a threat scenario shall be determined from the impact of the associated damage scenario and the attack feasibility of the associated attack paths.

FIGURE 15 The framework of cybersecurity engineering standard requirements and recommendations (ISO/SAE, 2020)

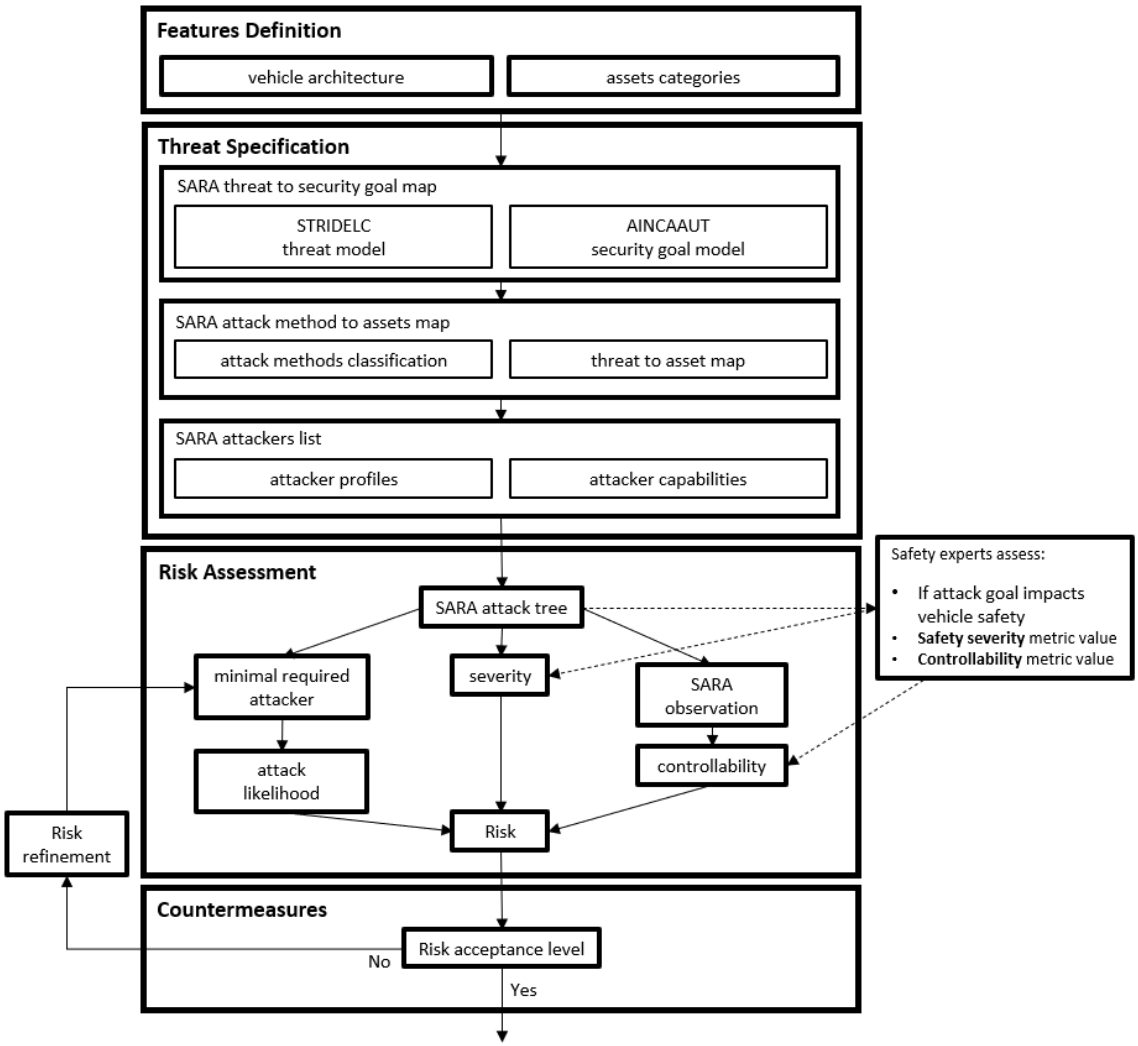

FIGURE 16 SARA method's framework (based on Monteuuis et al., 2018, 5)

The illustration of mapping the requirements and recommendations to the chosen security risk analysis method is built so that SARA method's framework acts as the basis for the chosen analysis method. Then the association between the two frameworks is marked to SARA framework with the requirement and recommendation IDs like *[RQ-08-01]* and *[RC-08-01]*. Finally, the contributions from TARA+ and HEAVENS methods are added to the SARA framework beside related requirement or recommendation with star symbols. The framework mapping is colour coded and illustrated in the following figure (figure 17).

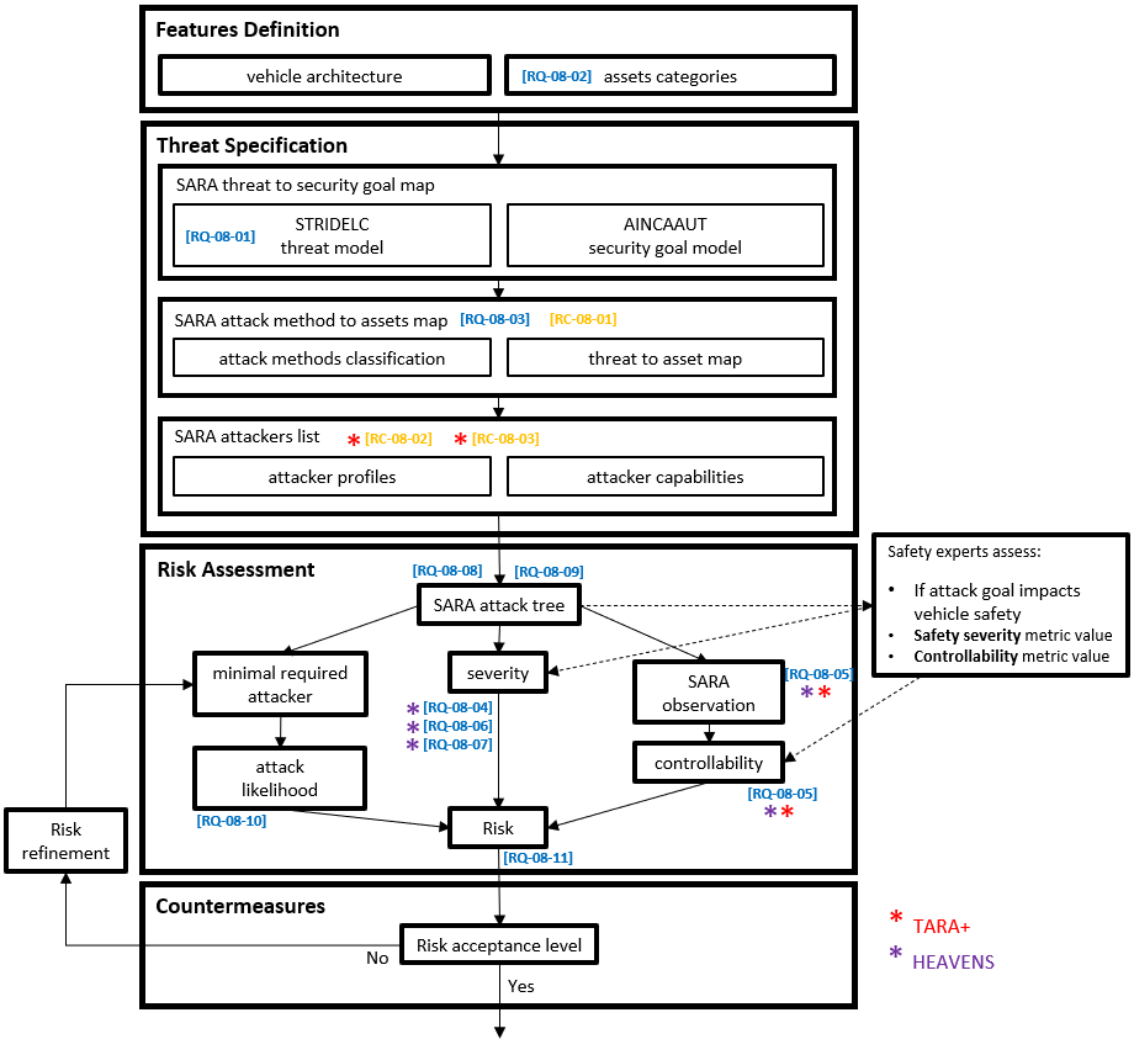

FIGURE 17 Framework mapping (based on Monteuuis et al., 2018; ISO/SAE, 2020; Bolovinou et al., 2019; Islam et al., 2016)

The issue with the given framework lies in the terminology and unnecessary components. Terminology between the cybersecurity engineering standard and SARA, TARA+ and HEAVENS differ from each other in certain ways which gives the framework challenges to be understood. Also, there are some features in SARA framework which are not required with the given criteria by the cybersecurity engineering standard. To address these issues, a new approach is constructed.

3.3.2 The New Analysis Framework – TARA+AD

To have the most practical and feasible security risk analysis method for the study, a new approach was derived from the chosen methods. The new approach consists of the necessary parts of the selected methods to comply with the requirements and recommendations of the cybersecurity engineering standard. The analysis framework was named TARA+AD, which is an

abbreviation of Threat Analysis and Risk Assessment for Automated Driving. TARA+ is a reference to actual TARA+ method by Bolovinou et al. (2019) which is used in the study, and AD (Automated Driving) refers to the automated driving features which are key elements in the study (SAE, 2016a). The approach was considered to act as a framework rather than as a method. A method gives guidance and/or steps how to perform a certain task. The TARA+AD consists of the most feasible parts of two TARA methods (SARA and TARA+) and provides a larger concept and guidance how to perform a security risk analysis. (Vaishnavi et al., 2004/2019.)

The creation process of the new analysis framework had three major turning points and several enhancements during the iterations. The three meaningful instances were: 1) creation of the new analysis framework based on SARA method, 2) re-creation of the analysis framework based on the requirements of the cybersecurity engineering standard, and 3) the analysis template logic change from individual task execution to one analysis table combining all tasks. The three instances are described next in detail.

Creation of the new analysis framework based on SARA method

The initial target was to use SARA method's framework and its detailed steps as the backbone structure for the new analysis framework. The decision to use SARA's framework came from the fact that TARA+ method was using SARA method as its basis. It appeared evident to start building the analysis framework from SARA method's principles and translate the features of SARA method to match the terminology of the cybersecurity engineering standard. For the new analysis framework, terms STRIDELC, AINCAUUT and SARA were removed from the diagram as the terms were specifically SARA oriented, but the new analysis framework should be more neutral with general terminology. Specific IDs were decided to represent activities and different tasks in the analysis framework. The functions of the different blocks in the analysis framework diagram were named as follows: A = activity, T = task, ST = sub-task. All tasks got sequence numbers in relation to the main activity. The selected three activities and related tasks were:

- A1 Features Definition
    - T1.1 vehicle architecture
    - T1.2 assets categories
- A2 Threat Specification
    - T2.1 threat to security goal map
        - ST2.1.1 threat model
        - ST2.1.2 security goal model
    - T2.2 attack method to assets map
        - ST2.2.1 threat to asset map
        - ST2.2.2 attack methods classification
    - T2.3 attackers list

        - ST2.3.1 attacker capabilities
        - ST2.3.2 attacker profiles
- A3 Risk Assessment
    - T3.1 attack tree
    - T3.2 severity
    - T3.3 observation
    - T3.4 controllability
    - T3.5 minimal required attacker
    - T3.6 attack likelihood
    - T3.7 Risk

The last block, A4 Countermeasures, was related to the excluded section *8.9 Risk treatment decision* of the cybersecurity engineering standard discussed in chapter 2.5.4, so it was not included to the new analysis framework. However, as SARA method incorporated vehicle architecture for the assets' definition, it was decided that the section *9.3 Item definition* of the cybersecurity engineering standard was taken into the analysis framework. The new approach of TARA+AD analysis framework can be seen in figure 18 (figure 18). The related requirements, recommendations and methods were mapped to the blocks with colour coding.

After defining the new analysis framework, a Word document was created for general instructions and an MS Excel spreadsheet was established as the analysis template with detailed instructions of specific steps how to make the security risk analysis. The general instructions consisted of high-level descriptions of each activity, task, and sub-task with given examples and illustrations. The descriptions, examples and illustrations were taken from the cybersecurity engineering standard and SARA method. The analysis template consisted of 17 sheets, each sheet representing a task or a sub-task. There were also two additional sheets, a cover sheet for project and version control, and a sheet for TARA+AD analysis framework as a diagram and a list of all activities and related tasks and sub-tasks. The descriptions, examples and illustrations of each task sheet were taken from the cybersecurity engineering standard and from SARA method.

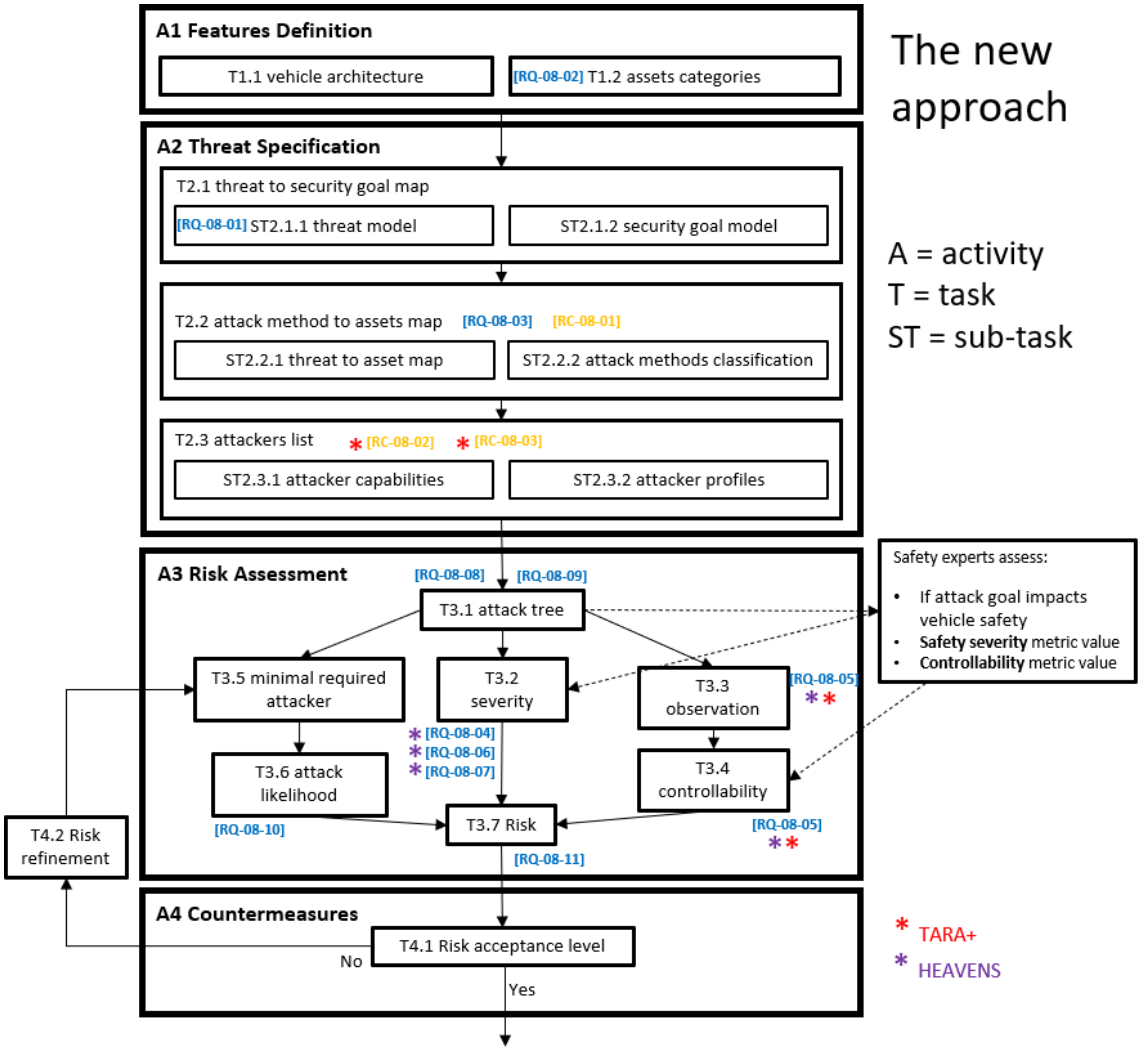

FIGURE 18 The new approach of TARA+AD analysis framework (based on Monteuuis et al., 2018; ISO/SAE, 2020; Bolovinou et al., 2019; Islam et al., 2016)

The aim of the analysis template was to complete each task in its dedicated sheet and move on to next task sheet once the previous task was completed. Every task sheet was supposed to include a table where the task in question would have been executed with the given detailed instructions. After few iterations of the analysis template development, it was noticed, that the mapping of the requirements to SARA method's framework did not work in practise as wanted. There were conflictions with terminology and in the logic of the steps where the user would have to go forward in the process of completing the tasks and then return. It was evident, that mapping the requirements to SARA method's framework did not work rationally. A decision was made to create an analysis framework which follows the logic and order of the cybersecurity engineering standard instead of trying to fit SARA method's logic into the requirements or vice versa. The necessary parts from SARA, TARA+ and HEAVENS methods would be added regardless. Also, the analysis template needed to be more user-friendly, and the steps should flow in a logical

order. It would not make sense to jump forward and come back in the security risk analysis process. The re-creation of the analysis framework was initiated.

Re-creation of the analysis framework based on the cybersecurity engineering standard

The second major iteration of creating the analysis framework was derived from the new cybersecurity engineering standard, and was not considered as a mapping activity anymore, but as a standard compatible approach. The analysis framework diagram was re-built based on the requirements and recommendations instead of the framework by SARA method. The activities, tasks and sub-tasks were created and named after the requirements and recommendations of the cybersecurity engineering standard. The requirements and recommendations were presented in figure 15 in chapter 3.3.1 (see figure 15). The six new activities and related tasks were:

- A1 Asset Identification
  - T1.1 Damage scenarios
  - T1.2 Assets
- A2 Threat Scenario Identification
  - T2.1 Threat scenarios
- A3 Impact Rating
  - T3.1 Damage scenario assessment
  - T3.2 Impact category documentation
  - T3.3 Impact rating categorization
  - T3.4 Safety impact
- A4 Attack Path Analysis
  - T4.1 Threat scenario analysis
  - T4.2 Attack path documentation
    - ST4.1 Attack path reference
- A5 Attack Feasibility Rating
  - T5.1 Attack feasibility rating
    - ST5.1 Rating method approach
    - ST5.2 Attack potential -approach
    - ST5.3 CVSS -approach
    - ST5.4 Attack vector -approach
- A6 Risk Determination
  - T6.1 Risk value

The re-created analysis framework is illustrated in figure 19 (figure 19). The blue rectangles represent the requirements, and the orange rectangles represent the recommendations of the cybersecurity engineering standard.

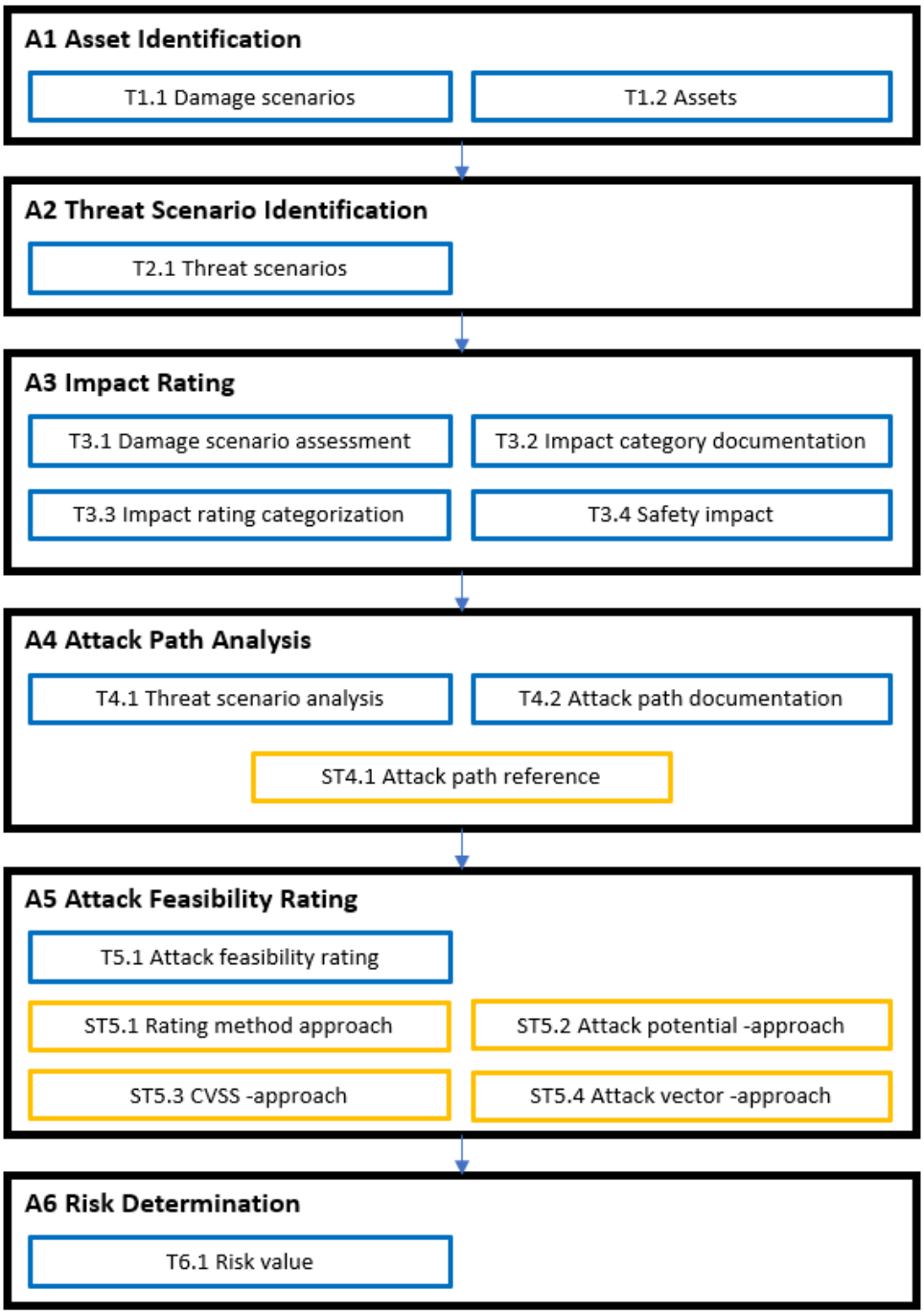

FIGURE 19 The re-created analysis framework (based on ISO/SAE, 2020)

An overview of the different activity sections in the cybersecurity engineering standard was re-examined as the designing of the use case was started in parallel while developing the analysis template. A discussion was held if the section selection together with new requirements should be extended. SARA method's feature of defining vehicle architecture would be useful while validating the analysis template with a use case involving a robot vehicle. The equivalent feature for vehicle architecture in the cybersecurity engineering standard was *Item definition* in section 9.3. SARA method was also referring to

cybersecurity goals on several occasions in its framework, thus it was considered that the cybersecurity goal aspect should be covered as the outcome of the analysis template. The cybersecurity goal aspect involvement seemed also evident as the whole security risk analysis process was derived from the requirement *[RQ-09-05] Perform risk analysis* in section *9.4 Cybersecurity goals* of the cybersecurity engineering standard as discussed in chapter 2.5.4. The fresh selection of the sections from the cybersecurity engineering standard are marked in dotted red rectangles in the following figure (figure 20).

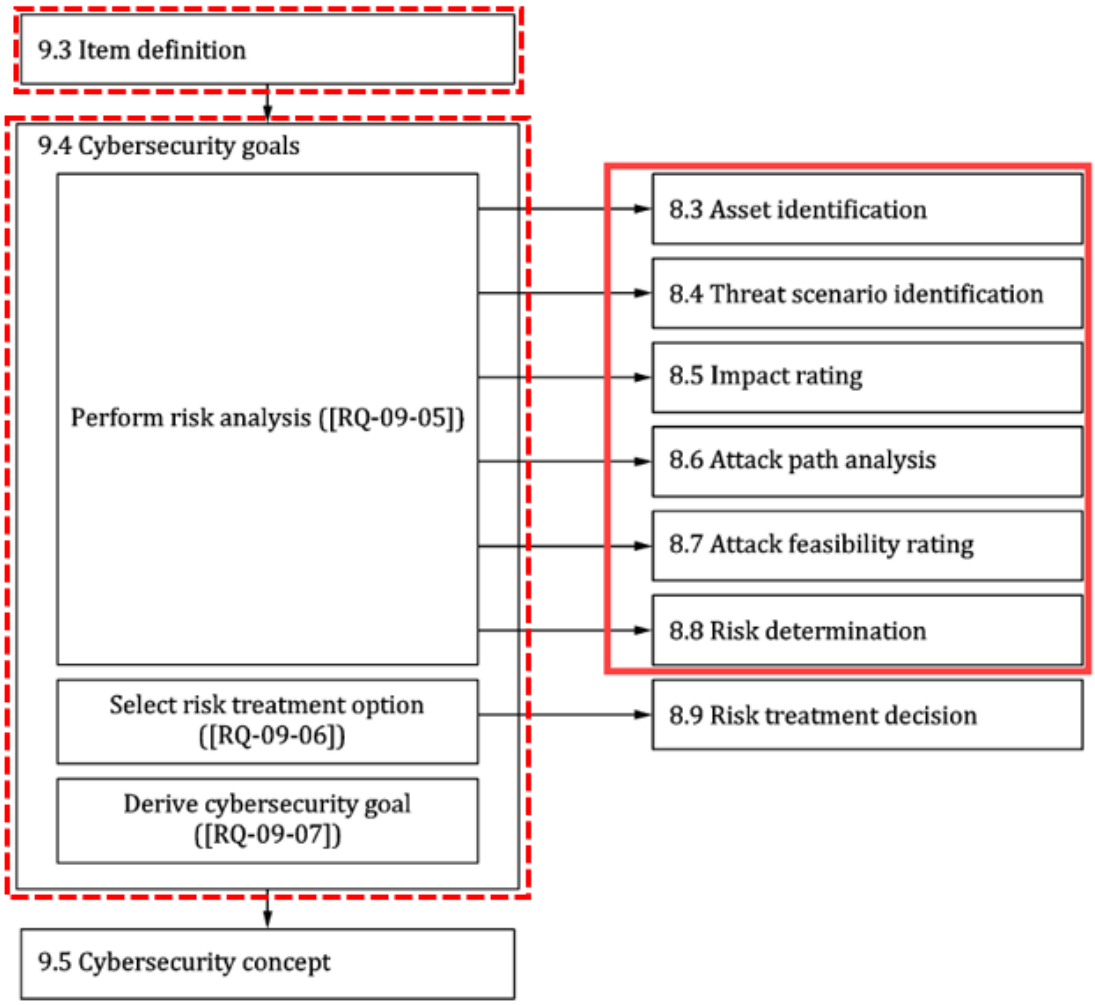

FIGURE 20 Extended sections chosen for security risk analysis (ISO/SAE, 2020, 80)

As the decision was made to include new requirements into the analysis framework, the diagram was updated accordingly. Item definition was incorporated to asset identification activity (A1 Asset Identification) and Cybersecurity goals was incorporated to risk determination activity (A6 Risk Determination). Item definition would help defining the assets, and cybersecurity goals would be the analysis outcome after risk determination. The enhanced analysis framework can be seen in the following figure (figure 21).

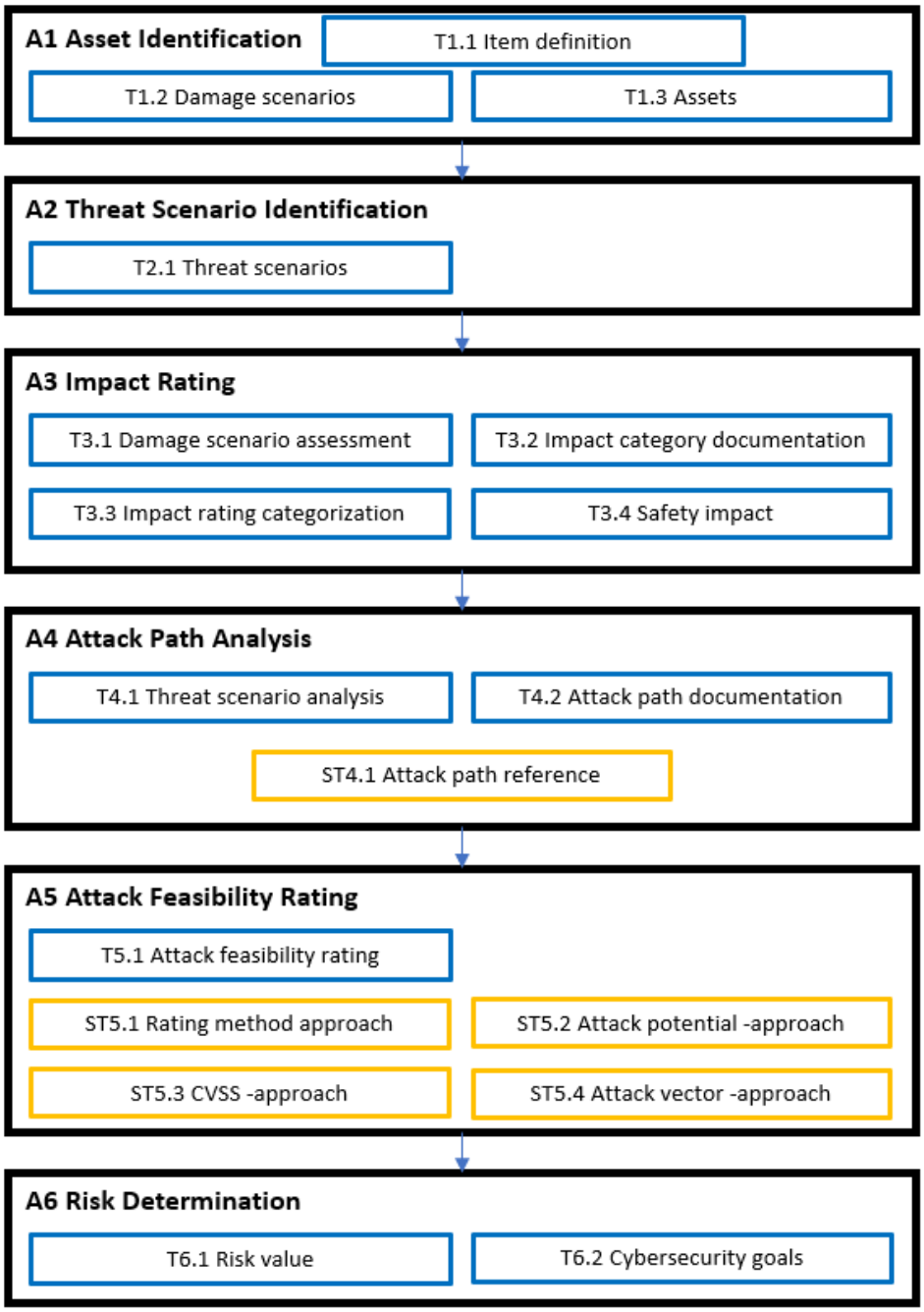

FIGURE 21 Enhanced analysis framework based on the cybersecurity engineering standard (ISO/SAE, 2020)

After some iterations of the analysis template with the added tasks T1.1 Item definition, and T6.2 Cybersecurity goals, it was noticed that the incorporation of cybersecurity goals did not quite fit the analysis template. Also, the process of the security risk analysis could not involve cybersecurity goals as the outcome as the cybersecurity goals were part of a later concept phase. The *9.4 Cybersecurity goals* section's requirements would also enlarge the security risk analysis process in such way that it would go beyond the scope of the study. An

outline had to be done and T6.2 Cybersecurity goals task was removed from the risk determination activity. Section *8.9 Risk Treatment Decision* was examined and thought fulfilling the need for an outcome of the security risk analysis, so it was chosen to be included to the analysis framework. The final selections of sections from the cybersecurity engineering standard are marked in the next three figures (figure 22; figure 23; figure 24). The original and primary set of chosen sections are marked with red rectangles, and the added sections are marked with red dotted rectangles in each figure to present the general view. Figure 24 shows the interactions of the different sections, and the risk analysis is conducted between *9.3 Item Definition* and *9.4 Cybersecurity goals*.

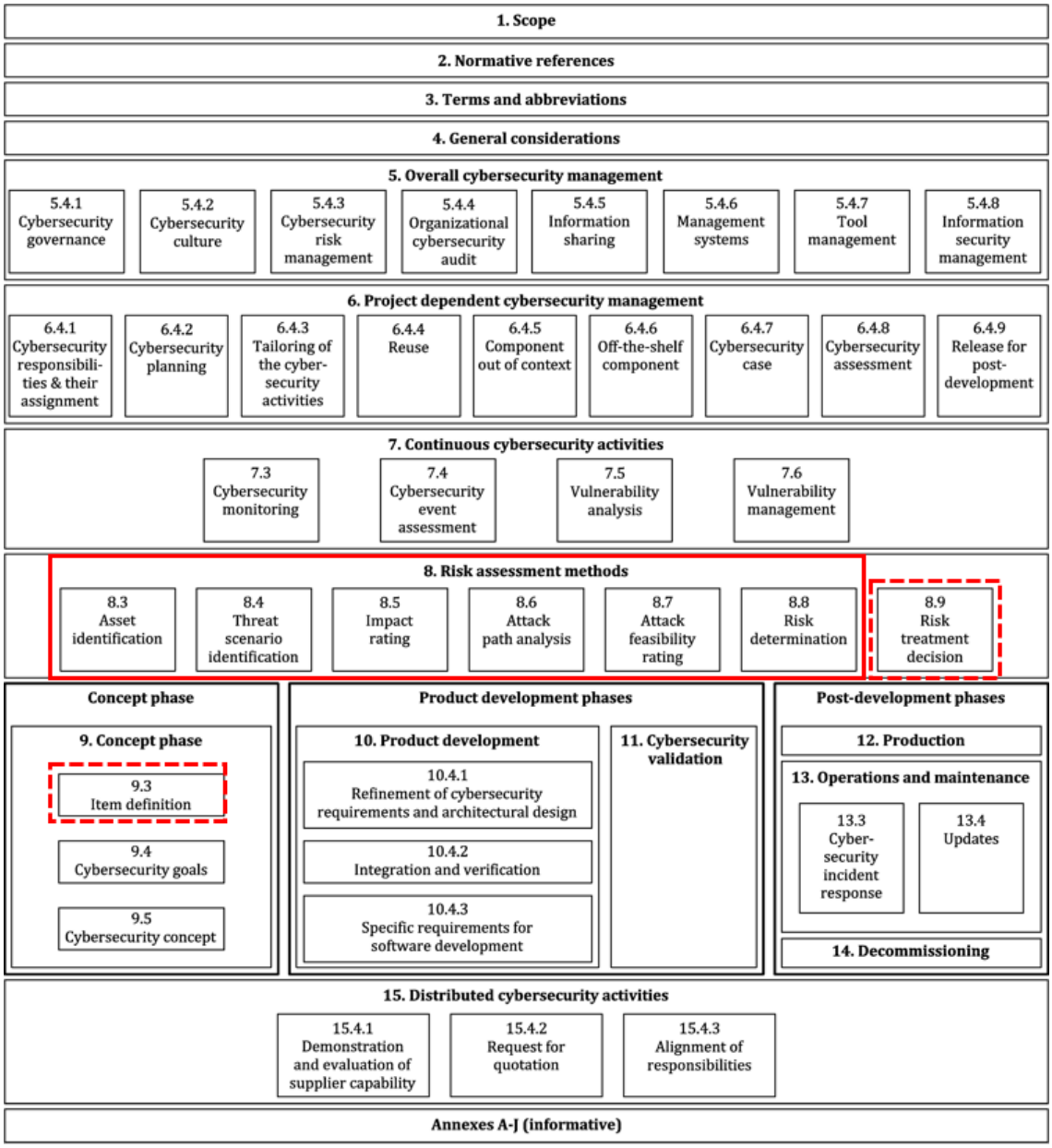

FIGURE 22 Overview of sections in the cybersecurity engineering standard (ISO/SAE, 2020, 8)

	Activities		Work Products
Organization Culture			
Cybersecurity Management	5. Overall Cybersecurity Management	[WP-05-01]	Cybersecurity policy, rules and processes
		[WP-05-02]	Evidence of competence management, awareness management and continuous improvement
		[WP-05-03]	Organizational cybersecurity audit report
		[WP-05-04]	Evidence of the organization's management systems
		[WP-05-05]	Evidence of tool management
	6. Project Dependent Cybersecurity Management	[WP-06-01]	Cybersecurity plan
		[WP-06-02]	Cybersecurity case
		[WP-06-03]	Cybersecurity assessment report
		[WP-06-04]	Release for post-development report
Continuous Cybersecurity Activities			
Continuous Cybersecurity Activities	7.3 Cybersecurity Monitoring	[WP-07-01]	List of sources for cybersecurity monitoring
		[WP-07-02]	Results from the triage of cybersecurityinformation
	7.4 Cybersecurity Event Assessment	[WP-07-03]	Cybersecurity event assessment
	7.5 Vulnerability Analysis	[WP-07-04]	Vulnerability analysis
	7.6 Vulnerability Management	[WP-07-05]	Rationale for the managed vulnerability
Concept and Product Development Phases			
Risk Assessment Methods	8.3 Asset Identification	[WP-08-01]	Damage scenarios
		[WP-08-02]	Identified assets and cybersecurity properties
	8.4 Threat Scenario Identification	[WP-08-03]	Threat scenarios
	8.5 Impact Rating	[WP-08-04]	Impact rating, including the associated impact categories of the damage scenarios
	8.6 Attack Path Analysis	[WP-08-05]	Identified attack paths
	8.7 Attack Feasibility Rating	[WP-08-06]	Attack feasibility rating
	8.8 Risk Determination	[WP-08-07]	Risk value
	8.9 Risk Treatment Decision	[WP-08-08]	Risk treatment decision per threat scenario
Concept Phase	9.3 Item Definition	[WP-09-01]	Item definition
	9.4 Cybersecurity Goals	[WP-09-02]	Threat analysis and risk assessment
		[WP-09-03]	Risk treatment decisions
		[WP-09-04]	Cybersecurity goals
		[WP-09-05]	Cybersecurity claims
		[WP-09-06]	Verification report
	9.5 Cybersecurity Concept	[WP-09-07]	Cybersecurity concept
		[WP-09-08]	Verification report of cybersecurity concept
Product Development Phases	10.4.1 Refinement of Cybersecurity Requirements and Architectural Design	[WP-10-01]	Refined cybersecurity specification
		[WP-10-02]	Cybersecurity requirements for post-development
		[WP-10-03]	Verification report for the refined cybersecurity specification
	10.4.2 Integration and Verification	[WP-10-04]	Vulnerability analysis report
		[WP-10-05]	Integration and verification specification
		[WP-10-06]	Integration and verification reports
	10.4.3 Specific Requirements for Software Development	[WP-10-07]	Documentation of the modelling, design, or programming languages and coding guidelines
		[WP-10-08]	Software unit design and software unit implementation
	11. Cybersecurity Validation of the Item at Vehicle Level	[WP-11-01]	Validation specification
		[WP-11-02]	Validation report
Post-Development phases			
	12. Production	[WP-12-01]	Production control plan
	13.3 Cybersecurity Incident Response	[WP-13-01]	Cybersecurity incident response plan
		[WP-13-02]	Cybersecurity incident response information
	13.4 Updates	[WP-13-03]	Procedures to communicate end of cybersecurity support
	14. Decommissioning	None	
Supporting Processes			
	15. Distributed Cybersecurity Activities	[WP-15-01]	Cybersecurity interface agreement

FIGURE 23 Activities and work products of the cybersecurity engineering standard (ISO/SAE, 2020, 66, 67)

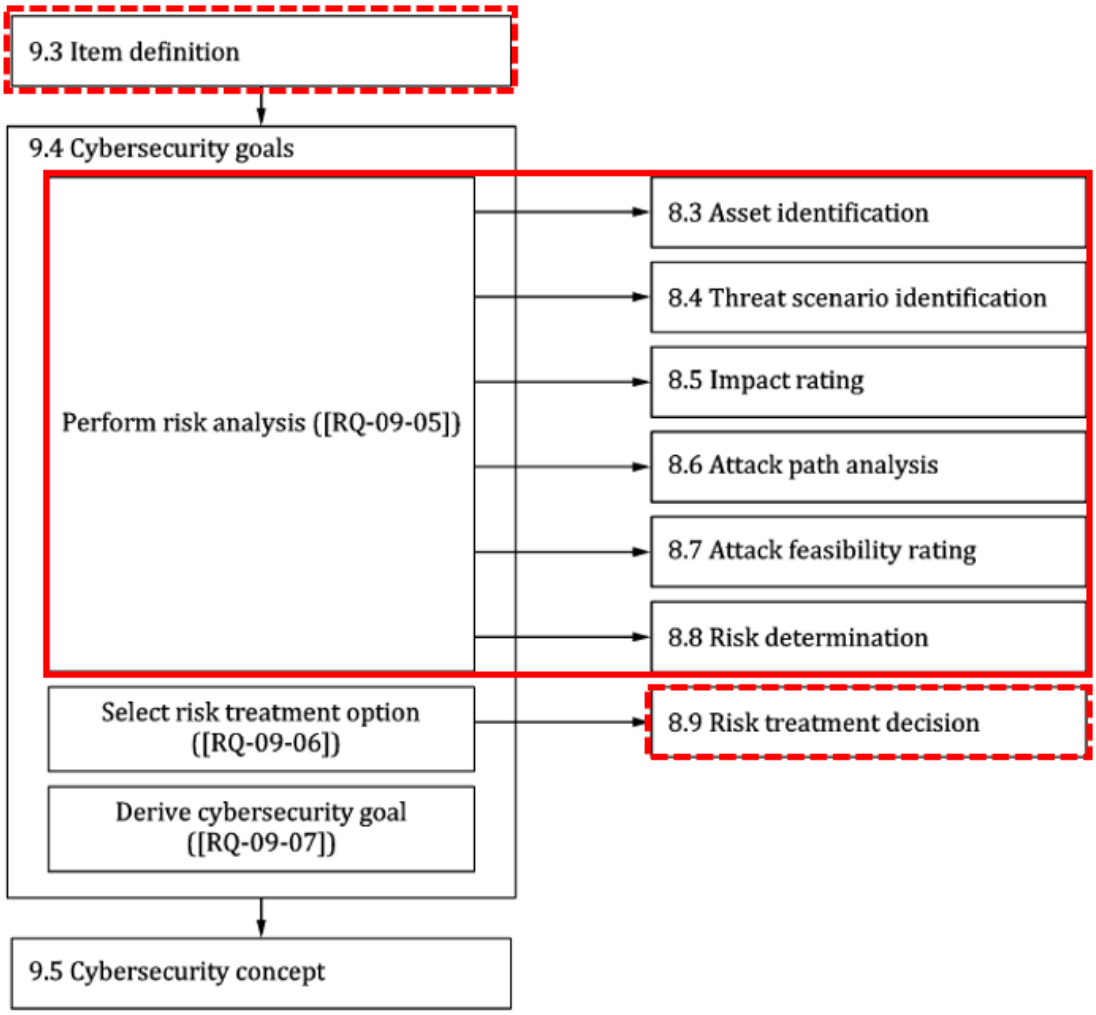

FIGURE 24 Final selection of the chosen sections for security risk analysis (ISO/SAE, 2020, 80)

A new activity was created for the risk treatment: A7 Risk Treatment Decision. Item definition was still considered to bring value to the analysis template, but its place would not be with the asset identification activity. Item definition was marked to the analysis framework as a file icon with the given activity number 0 (zero) as a provider of the input to initiate the analysis process. These added sections (9.3 and 8.9) with related requirements were not relevant for the analysis of the TARA methods discussed in chapter 3.2.1. However, the additions were considered being valuable for the new analysis framework and the use case validation. Because of these reasons, the requirements from *9.3 Item Definition* and *8.9 Risk Treatment Decision* were not added to the documents of evaluation of the security risk analysis methods but they were included to the analysis framework, template development and to general instructions. The finetuned and final version of the analysis framework is presented in figure 25 (figure 25). The order of the tasks in activity A1 (Asset Identification) were switched to reflect the logic of the cybersecurity engineering standard.

Modifications were also done in activities A4 (Attack Path Analysis) and A5 (Attack Feasibility Rating). In A4 the name of task T4.1 *Threat scenario analysis* was changed to *Attack path description* to give the task a more descriptive name of its actual intention. Also, sub-task ST4.1 *Attack path reference* was changed to be an equivalent task as the first two tasks. In A5 the rating method approach sub-task was changed to a task. The rating approach was decided to concern only attack potential -approach since SARA method's characteristics were adapted in the analysis template development. SARA method was focused on the attacker perspective which can be seen in the SARA method's framework in figure 16 in chapter 3.3.1 (see figure 16). The names of the sub-tasks in A5 were labelled with letters a, b and c as described in the cybersecurity engineering standard.

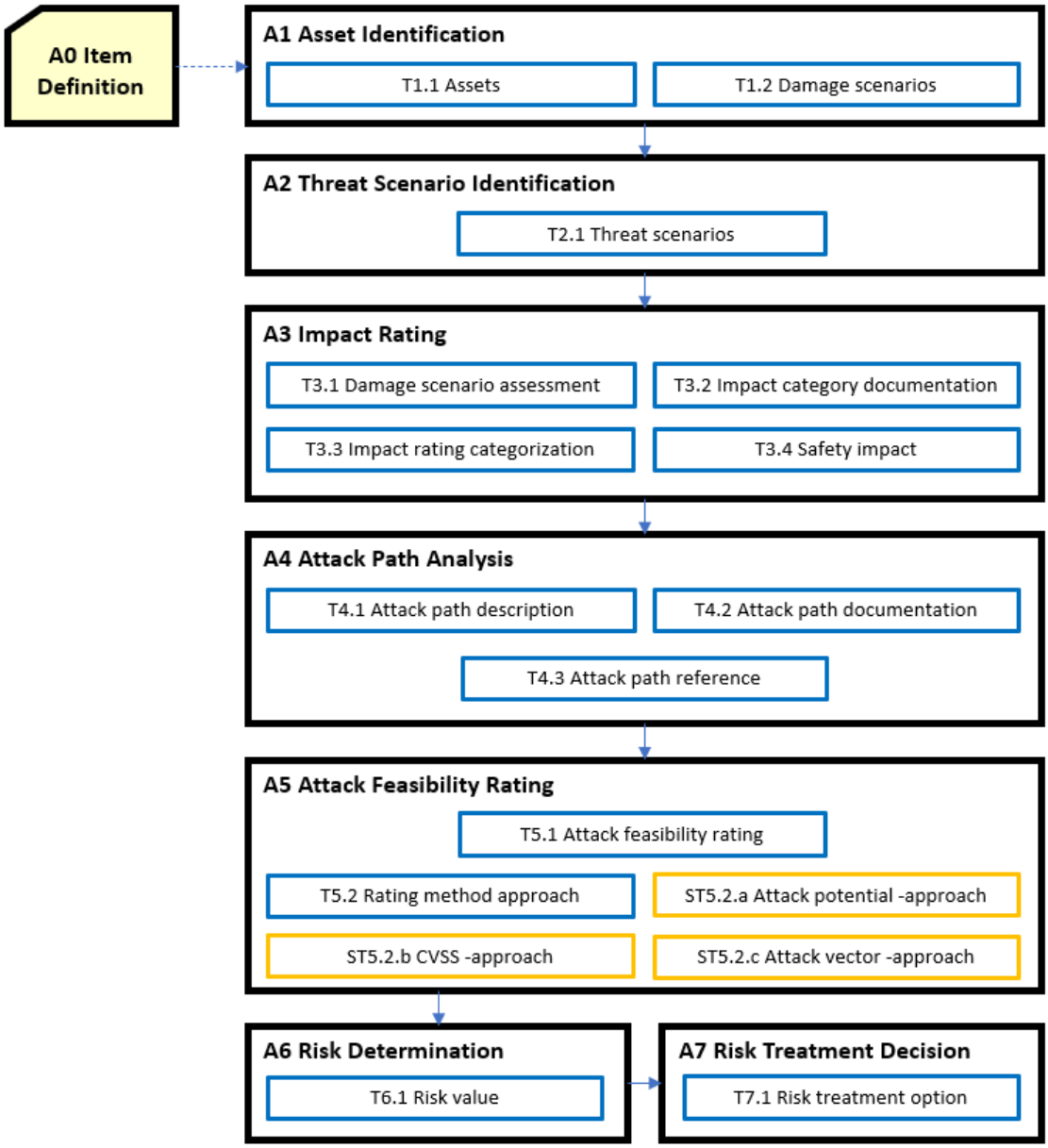

FIGURE 25 Final version of the analysis framework (based on ISO/SAE, 2020)

After finalizing the analysis framework, new versions of the general instructions and the analysis template were created. The descriptions, examples and illustrations in the general instructions were mostly taken from the cybersecurity engineering standard, but some reference to SARA and TARA+ method was used, like STRIDE(LC) (SARA) and an impact factor (TARA+). The general instructions remained consisting of the high-level descriptions, and SARA method's specific tasks were removed accordingly. The final set of the activities and tasks was as follows:

- A0 Item Definition
- A1 Asset Identification
    - T1.1 Assets
    - T1.2 Damage scenarios
- A2 Threat Scenario Identification
    - T2.1 Threat scenarios
- A3 Impact Rating
    - T3.1 Damage scenario assessment
    - T3.2 Impact category documentation
    - T3.3 Impact rating categorization
    - T3.4 Safety impact
- A4 Attack Path Analysis
    - T4.1 Attack path description
    - T4.2 Attack path documentation
    - T4.3 Attack path reference
- A5 Attack Feasibility Rating
    - T5.1 Attack feasibility rating
    - T5.2 Rating method approach
        - ST5.2.a Attack potential -approach
        - ST5.2.b CVSS -approach
        - ST5.2.c Attack vector -approach
- A6 Risk Determination
    - T6.1 Risk value
- A7 Risk Treatment Decision
    - T7.1 Risk treatment option

The analysis template was changed so that every activity had its own sheet instead of dividing every task into a separate sheet. The analysis template consisted of 13 sheets. There were eight activity sheets (from A0 Item Definition to A7 Risk Treatment Decision) and five supplementary sheets: Cover Sheet, A_Assumptions, B_TARA+AD framework, C_Further Information, and Data. The additional sheets are elaborated in the forthcoming chapter concerning the analysis template logic change.

The activity sheets included further material in addition to the table where the tasks were executed. The further material consisted of general descriptions

of the tasks, the requirements and recommendations, and examples and illustrations taken from the cybersecurity engineering standard. Some formulas, figures and tables were adapted from the TARA+ and SARA methods. The further material appeared to pose a challenge to the analysis process as in some sheets there were a lot of information that took the space before the actual analysis part started. The workaround for the challenge was to hide the guidance and informative parts or insert the guidance as a floating picture. Neither of the options were applied however, as the analysis process was about to be changed.

The progress of developing the activity sheets was paused during iteration of the activity A4 Attack Path. It became evident that the analysis process could not work practically with the separated sheets and tables approach. When developing the activities and related task execution tables, the next activity required information and input from the previous activity before it could start its tasks execution. In the activity A4 case, some information was required even from the next activity. In every case, the outcome of each activity had to be copied to the next activity so the analysis process could continue as defined by the cybersecurity engineering standard. Soon it was noticed that a one analysis table approach would be the only rational and logical solution as the analysis template did not have automated functionality which would copy the required information from sheet to sheet. The logic of the analysis template got changed.

The analysis template logic change

The analysis template was constructed in a new way. Instead of having a sheet for every activity for task execution, one big table was built in one sheet which included all the tasks and subtasks of each activity. The activity sheets were kept however for detailed information, instructions, illustrations, examples, and references. A total of 15 sheets were created:

1. Cover Sheet
2. TARA+AD Progress
3. A_Assumptions
4. B_TARA+AD framework
5. A0 Item Definition
6. RISK ANALYSIS
7. A1 Assets
8. A2 Threat Scenarios
9. A3 Impact
10. A4 Attack Path
11. A5 Attack Feasibility
12. A6 Risk Determination
13. A7 Risk Treatment
14. C_Further Information
15. Data

In addition to activity related sheets and the risk analysis sheet, there were six supplementary sheets for project control, progress monitoring, assumptions, navigation, further information, and data for functionality management of the Excel spreadsheet itself. The sheets of the analysis template are elaborated in the following table (table 15).

TABLE 15 Sheets of the analysis template

Sheet name	**Content of the sheet**
Cover Sheet	Basic information of the project in question. Document scope and summary. Version control.
TARA+AD Progress	Graphical progress bar of the security risk analysis activities (manual). Version control.
A_Assumptions	Table of assumptions with related assumption ID, comments, and project's confirmation. Version control.
B_TARA+AD framework	TARA+AD analysis framework diagram. List of activities with related tasks and sub-tasks. Legend of activities, tasks, and sub-tasks. Instructions to the reader how to use the analysis template with navigation table to sheets in question of each instruction. Table of abbreviations used in the analysis template. Version control.
A0 Item Definition	Information of the activity and tasks. Listing of related requirements as per the cybersecurity engineering standard (ISO/SAE, 2020). Example figure of vehicle architecture by SARA method (Monteuuis et al., 2018). Checklist of features used in item definition adapted from the cybersecurity engineering standard. Table for item definition adapted from the cybersecurity engineering standard including labels Component, Function, Input Interface, Output Interface, Asset ID, and Asset. Version control.
RISK ANALYSIS	Table for the security risk analysis consisting of seven blocks labelled by activities from A1 Assets to A7 Risk Treatment, as A0 Item Definition is performed in its own sheet. Every block in the table contains the activity related tasks with possible formulas, drop-down menus, detailed instructions and elaborations as notes of the meaning of terms and values. Above the table there are activity related value range tables and/or formulas explained in detail. Version control.
A1 Assets	Information of the activity and tasks. Listing of related requirements as per the cybersecurity engineering standard (ISO/SAE, 2020). Snapshot of the related activity section in the table on the RISK ANALYSIS sheet. Version control.
A2 Threat Scenarios	Information of the activity and tasks. Listing of related requirements as per the cybersecurity engineering standard (ISO/SAE, 2020). Snapshot of the related activity section in the table on the RISK ANALYSIS sheet. Version control.

(continues)

Table 15 (continues)

A3 Impact	Information of the activity and tasks. Listing of related requirements and example tables as per the cybersecurity engineering standard (ISO/SAE, 2020). Formula of the calculation of the impact value. Snapshot of the related activity section (first iteration) in the table on the RISK ANALYSIS sheet. Table of second iteration of the impact for future usage. Version control.
A4 Attack Path	Information of the activity and tasks. Listing of related requirements and recommendations, and an example figure as per the cybersecurity engineering standard (ISO/SAE, 2020). Snapshot of the related activity section in the table on the RISK ANALYSIS sheet. Version control.
A5 Attack Feasibility	Information of the activity and tasks. Listing of related requirements and recommendations, and example tables as per the cybersecurity engineering standard (ISO/SAE, 2020). Snapshot of the related activity section in the table on the RISK ANALYSIS sheet. Version control.
A6 Risk Determination	Information of the activity and tasks. Listing of related requirements and an example table as per the cybersecurity engineering standard (ISO/SAE, 2020). Snapshot of the related activity section in the table on the RISK ANALYSIS sheet. Version control.
A7 Risk Treatment	Information of the activity and tasks. Listing of related requirements as per the cybersecurity engineering standard (ISO/SAE, 2020). Snapshot of the related activity section in the table on the RISK ANALYSIS sheet. Version control.
C_Further Information	Empty sheet available for the user to add further information when needed, like pictures and other useful material. Version control.
Data	Data sheet including lists of different options used by the functionalities embedded in the table on the RISK ANALYSIS sheet. Explanations for values used in A3 Impact and A5 Attack Feasibility sections in the RISK ANALYSIS table.

Once the analysis template was finished, it was to be validated with a use case created for a robot vehicle. The use case creation and execution are described in the following chapters.

3.4 Use Case for Applied Research

As presented in the introductory chapter of the study, the research topic was originated from the Austrian research center, Virtual Vehicle, operating in the automotive domain. Virtual Vehicle provides research services for its partners, but actual products are not manufactured. The focus is on System and Software Design and in automation of testing and validation. Virtual Vehicle has a robot vehicle available to apply the demonstrations. When a partner offers an item to

be validated, the item is put to the robot vehicle to be tested and improved. The item can be an algorithm or a perception unit with AI (Artificial Intelligence). This type of validations of items happens in early development phases. (Virtual Vehicle, 2021c.) Virtual Vehicle has 300 employees, two offices, around 100 partners from different companies, and partners from over 40 scientific institutes. Daimler, Porsche, Bosch, IBM, Siemens, and Berlin Institute of Technology are among the large network of Virtual Vehicle. (Virtual Vehicle, 2021a; Virtual Vehicle, 2021b.)

The research process, and especially the iterations during the development of the analysis framework and template were conducted in collaboration with two employees of Virtual Vehicle. The employees were a Lead Researcher from Cybersecurity and Functional Safety department, and a Functional Safety Specialist from Model-based System Engineering department. By the time the use case development got started, a third employee from Virtual Vehicle joined the research activity. A Researcher specialized in Dependable Systems took part to the use case development process as an expert of robot vehicles.

3.4.1 Use Case Creation

The new analysis framework, TARA+AD, was to be evaluated by using an automotive industrial use case for automated driving. The use case was created for a robot vehicle called SPIDER (Smart PhysIcal Demonstration and Evaluation Robot). The SPIDER was created for testing autonomous driving, and it uses both manual and automated driving functions which both can be tested in the use case. (Virtual Vehicle, 2020a.) There were preconditions set for the use case creation and validation. The use case should include a functional description, present interconnections, and describe an architecture to identify the potential security risks based on the TARA+AD analysis framework. The use case should concern remote communication and what kind of cyberthreats that scenario might have. In the scenario there should be a remote control over the network with a laptop to the robot vehicle SPIDER with automated driving features (like path planning) and safety measures (like collision avoidance).

The use case creation was started with the given preconditions in mind and by utilizing the analysis template. The development of the analysis template continued while creating the use case, as certain practical matters arose during the parallel development. To get started with the use case creation, the item definition and the overall architecture and functions of the SPIDER were examined. The item definition provided by Virtual Vehicle consisted of technical and functional descriptions of the SPIDER, its external interfaces, interactions of the SPIDER with other items or elements like a power supply, and operational and environmental constraints as well as legal requirements and relevant standards. The details of the SPIDER item definition are classified as company confidential, thus they are not provided in the study. Another document provided by Virtual Vehicle contained the high-level and low-level architectures of the SPIDER describing the HW, SW controllers and functions.

Due to company confidential reasons stated earlier, not all the SPIDER architectural details are available in the study, just the use case essential ones. (Virtual Vehicle, 2020b.)

The use case was illustrated first in a general level to present the chosen item boundary and some preliminary architecture as per activity **`A0 Item Definition`** in the analysis template. The SPIDER functions specific to the use case were documented only to the analysis template. It was stated that the use case creation for any project should be conducted at the same time when executing the item definition activity in the analysis template. The item definition activity gives useful information what to include to the use case. The use case should also be added to the **`A0`** activity sheet in the analysis template for documentation.

The general level of the use case can be seen in figure 26 (figure 26). The item boundary area is marked with red dotted line. The item boundary represents the examined environment that is separated from the SPIDER. The SPIDER itself is the black vehicle-like icon on top in the figure. The black arrows present hard-wired connections like physical connections via cable. The blue arrows mean wireless communication, or OTA (Over the Air). The green arrows are for human interaction with equipment.

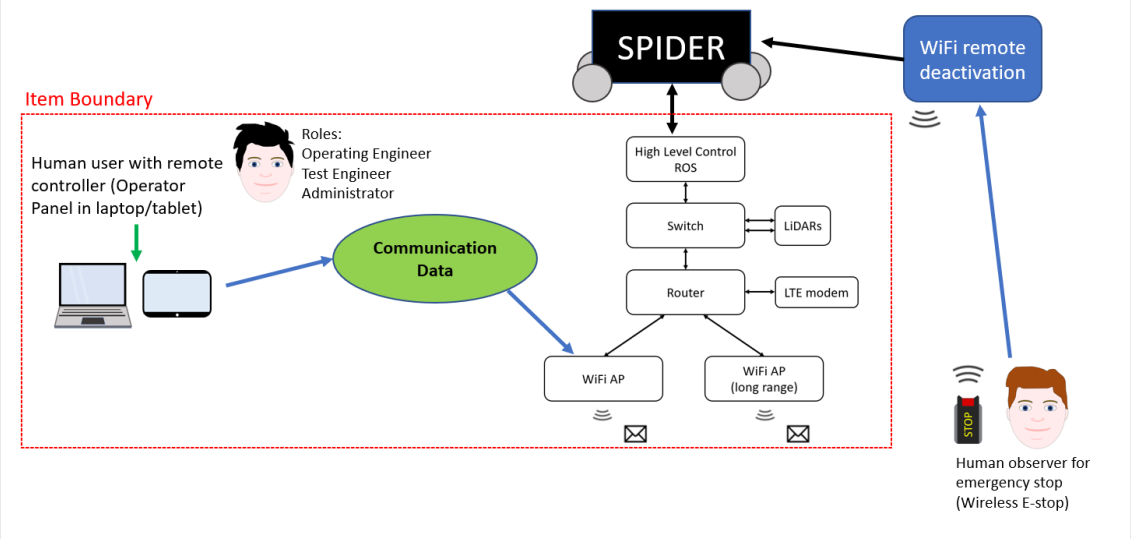

FIGURE 26 SPIDER use case in general level (based on Virtual Vehicle, 2020b)

The human user with remote controller is on the left side. The remote controller means a laptop or a tablet in which there is an Operator Panel installed. The Operator Panel is the user interface for connecting, controlling, and monitoring the SPIDER. Different roles are given to the human user, as there are many roles which can be used for attacking. In the attack scenarios in the study, the focus is on the Operating Engineer role.

The green oval shape represents wireless communication data from the remote controller to the WiFi AP (access point). The WiFi AP is part of the SPIDER's High Level Controller (HLC), aka an industrial PC running ROS

(Robot Operating System). The SPIDER's HLC is connected with a switch which is connected to LiDARs (Light Detection and Ranging). The switch is connected to a router, which has connection to an LTE modem. The router is connected with two kinds of WiFis: short and long range. The WiFi AP used in the use case is the short range one. (Virtual Vehicle, 2020b.)

With every usage and field test of the SPIDER, there is a mandatory human observer with a wireless emergency stop instrument (E-stop) which is directly connected to SPIDER's batteries. The E-stop can disable the batteries and enables halting the brakes. The human observer is located on the right side in the figure 21. The blue rectangle presents the WiFi remote deactivation.

The need with the use case was to apply cybersecurity in a vehicle level with two different threat scenarios: communication in application level with Operator Panel, and communication in transport/network level with WiFi AP. Two cyberattack scenarios (CAS) were distinguished: CAS1 and CAS2.

CAS1 Description: *The hacker could have stolen the laptop/tablet and acquired the employee ID (username and password)*. In this scenario the human attacker has committed a company theft and stolen both the equipment and login credentials from an Operating Engineer. The CAS1 is presented in the following figure (figure 27).

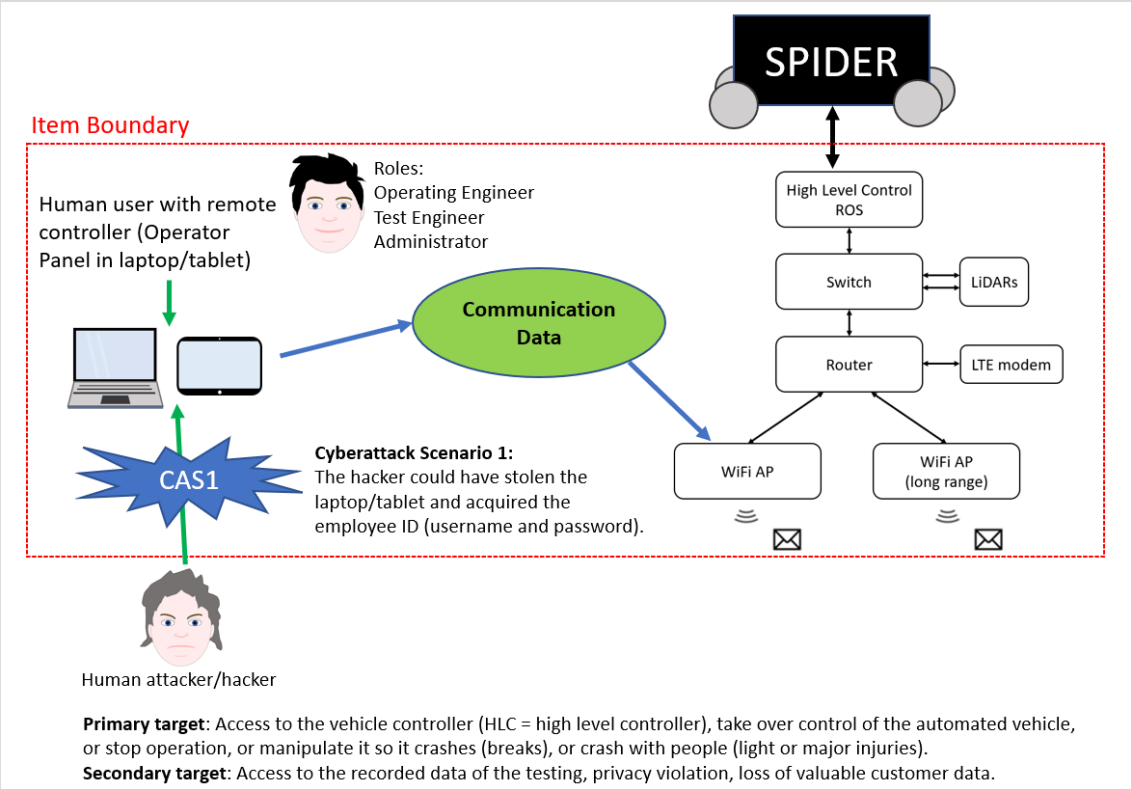

FIGURE 27 Cyberattack scenario 1 of the SPIDER use case (based on Virtual Vehicle, 2020b)

The grounds of the use case with the CAS1 are the same as in figure 26 (see figure 26). The CAS1 is presented in the left down corner with the human

attacker/hacker. The green arrow goes from the attacker to the stolen equipment which then connects to WiFi AP via Communication Data. Under the human attacker there are explanations of the primary and secondary targets of both attacks (CAS1 and CAS2). The primary target is to gain access to the vehicle controller (in this use case SPIDER HLC), take over control of the automated vehicle, or stop operation, or manipulate it so the vehicle crashes (breaks), or crashes with people causing light or major injuries. The secondary target is to gain access to the recorded data of the test case, causing privacy violation, and a loss of valuable customer data.

CAS2 Description: *The hacker uses remote equipment (laptop/tablet).* In the second scenario the human attacker is using his/her own equipment to gain access to the SPIDER HLC. The attacker has been able to make a breach into the company's systems and has primary and secondary targets to cause damage of any kind. The green arrow goes first to the equipment and then the blue arrow to the Communication Data which then connects to the WiFi AP. The CAS2 is presented in the following figure (figure 28).

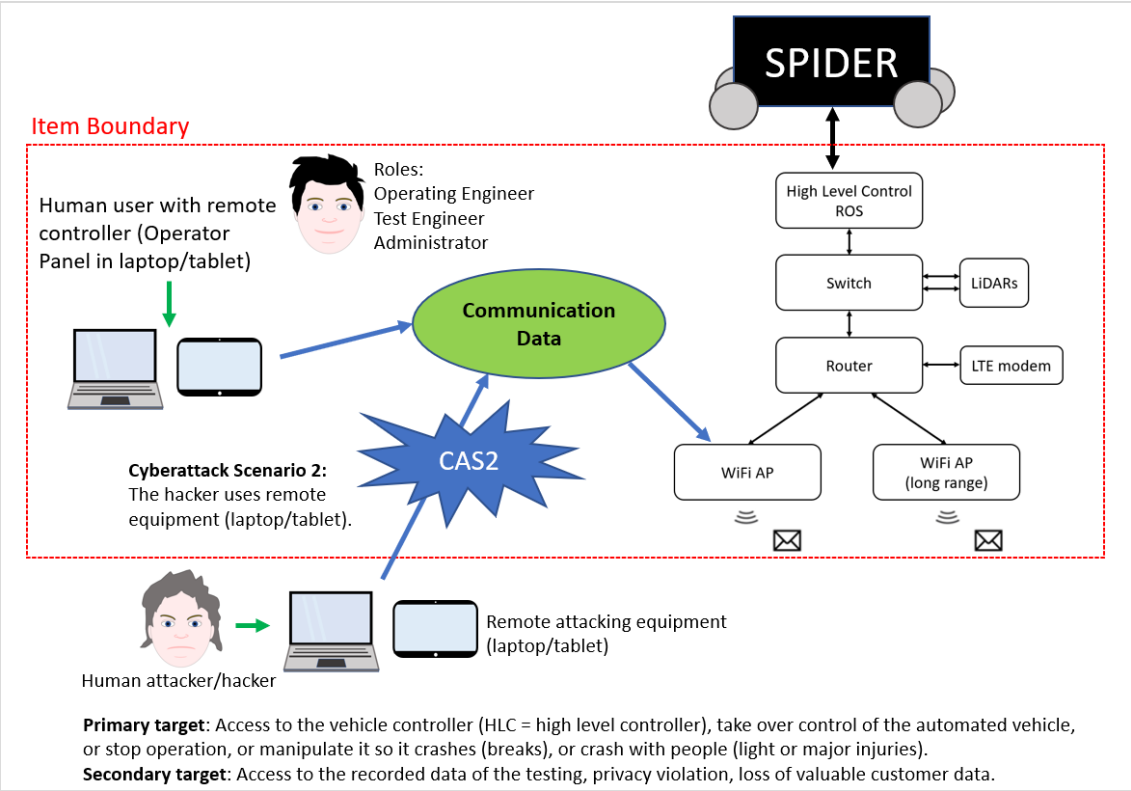

FIGURE 28 Cyberattack scenario 2 of the SPIDER use case (based on Virtual Vehicle, 2020b)

3.4.2 Use Case Execution and Analysis Template Enhancement

Once the designing of the use case and its cyberattack scenarios was completed, the execution of the use case could be initiated in the analysis template. As stated earlier, the development of the analysis template happened in parallel with the use case iteration, and the analysis template was modified based on

practical observations from the use case execution. The made updates to the analysis template are listed in table 16 (table 16). For each sheet of the analysis template there are two cells in the table of which the lower cell describes the made changes. The risk analysis sheet is discussed separately, as it was modified significantly.

TABLE 16 Updates of analysis template during and after use case execution

Sheet name	**Content of the sheet**
Cover Sheet	Basic information of the project in question. Document scope and summary. Version control.
	Update: New sheets added to version control table.
TARA+AD Progress	Graphical progress bar of the security risk analysis activities (manual). Version control.
	Update: Instructions added how to utilize the progress bar table.
A_Assumptions	Table of assumptions with related assumption ID, comments, and project's confirmation. Version control.
	No updates
B_TARA+AD framework	TARA+AD analysis framework diagram. List of activities with related tasks and sub-tasks. Legend of activities, tasks, and sub-tasks. Instructions to the reader how to use the analysis template with navigation table to sheets in question of each instruction. Table of abbreviations used in the analysis template. Version control.
	Updates: More instructions added to the reader (parts 8-10). Table of abbreviations updated.
A0 Item Definition	Information of the activity and tasks. Listing of related requirements as per the cybersecurity engineering standard (ISO/SAE, 2020). Example figure of vehicle architecture by SARA method (Monteuuis et al., 2018). Checklist of features used in item definition adapted from the cybersecurity engineering standard. Table for item definition adapted from the cybersecurity engineering standard including labels Component, Function, Input Interface, Output Interface, Asset ID, and Asset. Version control.
	Update: Guidance given to include a use case or use cases of the item. References added.

(continues)

Table 16 (continues)

RISK ANALYSIS	Table for the security risk analysis consisting of seven blocks labelled by activities from A1 Assets to A7 Risk Treatment, as A0 Item Definition is performed in its own sheet. Every block in the table contains the activity related tasks with possible formulas, drop-down menus, detailed instructions, and elaborations as notes of the meaning of terms and values. Above the table there are activity related value range tables and/or formulas explained in detail. Version control.
	Multiple updates. Discussed separately.
A1 Assets	Information of the activity and tasks. Listing of related requirements as per the cybersecurity engineering standard (ISO/SAE, 2020). Snapshot of the related activity section in the table on the RISK ANALYSIS sheet. Version control.
	Updates: New snapshot of the related activity section in the table on the RISK ANALYSIS sheet due to made changes. References added.
A2 Threat Scenarios	Information of the activity and tasks. Listing of related requirements as per the cybersecurity engineering standard (ISO/SAE, 2020). Snapshot of the related activity section in the table on the RISK ANALYSIS sheet. Version control.
	Updates: New snapshot of the related activity section in the table on the RISK ANALYSIS sheet due to made changes. References added.
A3 Impact	Information of the activity and tasks. Listing of related requirements and example tables as per the cybersecurity engineering standard (ISO/SAE, 2020). Formula of the calculation of the impact value. Snapshot of the related activity section (first iteration) in the table on the RISK ANALYSIS sheet. Table of second iteration of the impact for future usage. Version control.
	Updates: New snapshot of the related activity section in the table on the RISK ANALYSIS sheet due to made changes. References added.
A4 Attack Path	Information of the activity and tasks. Listing of related requirements and recommendations, and an example figure as per the cybersecurity engineering standard (ISO/SAE, 2020). Snapshot of the related activity section in the table on the RISK ANALYSIS sheet. Version control.
	Updates: New snapshot of the related activity section in the table on the RISK ANALYSIS sheet due to made changes. References added.

(continues)

Table 16 (continues)

A5 Attack Feasibility	Information of the activity and tasks. Listing of related requirements and recommendations, and example tables as per the cybersecurity engineering standard (ISO/SAE, 2020). Snapshot of the related activity section in the table on the RISK ANALYSIS sheet. Version control.
	Updates: New snapshot of the related activity section in the table on the RISK ANALYSIS sheet due to made changes. Added modified table of Attacker Profiles by SARA method (focusing on Expertise and Knowledge, SARA method specific values left out). References added.
A6 Risk Determination	Information of the activity and tasks. Listing of related requirements and an example table as per the cybersecurity engineering standard (ISO/SAE, 2020). Snapshot of the related activity section in the table on the RISK ANALYSIS sheet. Version control.
	Updates: New snapshot of the related activity section in the table on the RISK ANALYSIS sheet due to made changes. References added.
A7 Risk Treatment	Information of the activity and tasks. Listing of related requirements as per the cybersecurity engineering standard (ISO/SAE, 2020). Snapshot of the related activity section in the table on the RISK ANALYSIS sheet. Version control.
	Updates: New snapshot of the related activity section in the table on the RISK ANALYSIS sheet due to made changes. References added.
C_Further Information	Empty sheet available for the user to add further information when needed, like pictures and other useful material. Version control.
	No updates
Data	Data sheet including lists of different options used by the functionalities embedded in the table on the RISK ANALYSIS sheet. Explanations for values used in A3 Impact and A5 Attack Feasibility sections in the RISK ANALYSIS table.
	Update: Asset categories and attackers lists added.

As there were multiple changes made to the risk analysis sheet for every activity block, the changes are discussed as the outcome of the use case execution. Each activity is described here, also item definition, even though it is in a separate sheet as item definition starts the security risk analysis process. As per the two cyberattack scenarios (CAS1 and CAS2) created for the SPIDER use case, the details of these scenarios are elaborated in Appendix 2.

A0 Item Definition

In item definition, the use case is described, and related figures are attached. Assets are introduced and given ID numbers. The components, functions, input

interfaces (signal) and output interfaces are defined as per the cybersecurity engineering standard.

A1 Assets
The asset IDs are placed to the risk analysis table, and they are given an asset category from a drop-down menu. The options are equipment, data flow or external entity. The meaning of the options is described in a note. Any elaborative comments can be given to a comments field. In the damage scenarios section, the STRIDE(LC) categories as per SARA method are listed and the relevant ones need to be bolded. The not needed ones need to be in cursive. The STRIDE(LC) categories are described in a note. A description or rational is required for the selected category.

A2 Threat Scenarios
The damage scenarios defined in the **`A1`** are given an attack class based on which STRIDE(LC) category was chosen. The classes are adapted from SARA method and the original STRIDE by Microsoft. For every damage scenario, threat scenarios are given. The threat scenarios get an individual ID and there can be more than one threat scenario for each damage scenario. The description for each threat scenario is required.

A3 Impact
The damage scenarios and related threat scenarios are assessed with different impact categories with specified values. The categories are Safety, Financial, Operational, and Privacy as per the cybersecurity engineering standard. The values are from 0 to 3 where the 0 has low impact and 3 has high impact on the damage/threat scenario in the category in question. The values of the categories are summed together for an Impact Value (IV) based on their weight factors. Safety is three times, and Operational is two times more important than Financial and Privacy. The formula for the Impact Value (IV) calculation is adapted from the TARA+ method. An Impact Factor (IF) is calculated after Impact Value (IV) is formed. The Impact Factor values are from 0 to 4 where the 0 has low impact and 4 has high impact. The Impact Factor (IF) is also adapted from the TARA+ method and the original purpose was to include two additional impact categories to the impact examination: Observation Factor (OF) and Controllability Factor (CF). These factors are defined by TARA+ method and they are meant to address the issue with automated driving by dividing the controllability factor from SARA method into the system and the human driver. It was noticed though, that this kind of advanced impact calculation was not relevant in this phase of security risk analysis but should be conducted in section *9.5 Cybersecurity concept* of the cybersecurity engineering standard which is not part of this study. For these reasons, two iterations were established where the first iteration happens during the security risk analysis executed with the created analysis template, and the second iteration was documented in the sheet **`A3 Impact`** for future implementation.

A4 Attack Path
The attack path is required for each threat scenario. The attack paths are given an ID to which the attack class name from block **A2** needs to be attached. The attack path is described step by step to show the whole scenario of the possible attack.

A5 Attack Feasibility
The attack paths are rated in the attack feasibility with ease of exploitation by different factors. The factors are elapsed time, attackers' expertise, knowledge of the asset, window of opportunity and equipment used for the attack. The factors have values from 0 to 3 or 4 and 0 means the easiest opportunity for the attack and 3 or 4 is the hardest option for the attack. Justification is required for the selected value of each factor. Like in **A3 Impact**, the attack feasibility has formulas and calculations adapted from the TARA+ method. Attack Potential (APo) sums the values given for each factor and Attack Probability (AP) calculates the probability of the attack. The Attack Probability has values from 0 to 4 where 0 means the lowest probability and 4 the highest probability for an attack.

A6 Risk Determination
The risk determination is based on the Impact Factor (IF) from **A3 Impact** and the Attack Probability (AP) from **A5 Attack Feasibility** which are put to a risk value ranking table from which an index looks for the correct values and presents it in the activity block. The target value of the cybersecurity risk for the project of the use case needs to be set as the risk values need to be colour coded manually in the table. The risk values are QM (Quality Management), Low, Medium, High and Critical. If the target value for the project is Low, then all values above Low need to be colour coded red. Low and QM would then be green. The colour coding is meant to directly show the criticality of the risk given to each threat scenario.

A7 Risk Treatment
Risk treatment is directed from the outcome of **A3 Impact**, **A4 Attack Paths** and **A6 Risk Determination**. The options for the risk treatment are avoiding the risk, reducing the risk, sharing the risk, and retaining the risk. There can be more than one option selected for the risk treatment. Each selected option or combination of options are given an ID. Every option needs to be also justified.

With this given security risk analysis template, the discovering and listing of potential attacks can be produced and documented in one place. The analysis template has very little automation within its functions and there are some manual activities to be done, but the usage has been designed and experimented to work as effortlessly as possible.

Field testing of the SPIDER use case

Due to the COVID-19 pandemic during years 2020 and 2021 when the study's practical implementation took place, the SPIDER robot was used in international test locations despite the pandemic, but the testing did not include cybersecurity features. Since the pandemic prevented the real-life validation of the TARA+AD analysis framework, it was decided that any use case evaluation would be conducted in practise later in the future.

When the proper time would come, the evaluation would be executed with safety in mind (ISO, 2018). That means in practise that the SPIDER is without human passengers in any case, thus it would not pose a threat to human passengers inside a vehicle. However, the humans around the SPIDER could be in danger because the robot vehicle weights about 400 kg and any unintended movement may danger any human bystander and spectators. The SPIDER is able to perform high dynamic and omnidirectional movement with independent 4 wheels-drive and 4 wheels-steering. (Virtual Vehicle, 2020a.) In the real-life evaluation of the TARA+AD analysis framework, the remote operator of the SPIDER would be considered as the human driver as the person is giving commands to the robot vehicle as per automation level technical report (SAE, 2016a). During the real-life evaluation, there would be a further human observer who is responsible to deactivate the SPIDER in case of any emergency. In an ideal situation, the researcher of the study could take part to the real-life evaluation of the TARA+AD analysis framework.

The use case designed for the study was more a theory-based approach due to the lack of field testing with the SPIDER. The use case for the field test would most probably be designed in a more practical way.

3.5 Chapter Summary

This chapter explained how the study was designed and executed. The study contained three parts: 1) finding a security risk analysis method which meets the requirements of the cybersecurity engineering standard (*Comparison of the different TARA approaches*), 2) modelling of the cybersecurity engineering standard compliant analysis framework (TARA+AD) together with a security risk analysis template (*Elaboration of the new approach*), and 3) use case creation and execution with the derived security risk analysis template (*Application of the specific approach for the UC*). Each part contained phases that were iterated several times. The chosen research method was Design Science (DS) as the study targeted to produce an artifact to solve the research problem. Different approaches how to define and plan design science research by scholars were introduced. The chosen approach for the study was Design Science Research Method (DSRM) created by Peffers et al. (2007). The DSRM process model is used to describe and evaluate the study's progress and outcome in the next chapter, findings.

4 FINDINGS

This chapter discusses the findings of the comparison of the different TARA approaches, and the elaboration and application of the TARA+AD analysis framework and the analysis template for specific use case. The findings and the progress of the study is examined through Design Science Research Method (DSRM) process model by Peffers et al. (2007).

4.1 Result Examination with DSRM Process Model

The DSRM process model (Peffers et al., 2007) was introduced in figure 12 (see figure 12) in chapter 3.1. The six activities of the model are shown in figure 29 (figure 29). The activities are problem identification and motivation, defining the objectives for a solution, design and development, demonstration, evaluation, and communication.

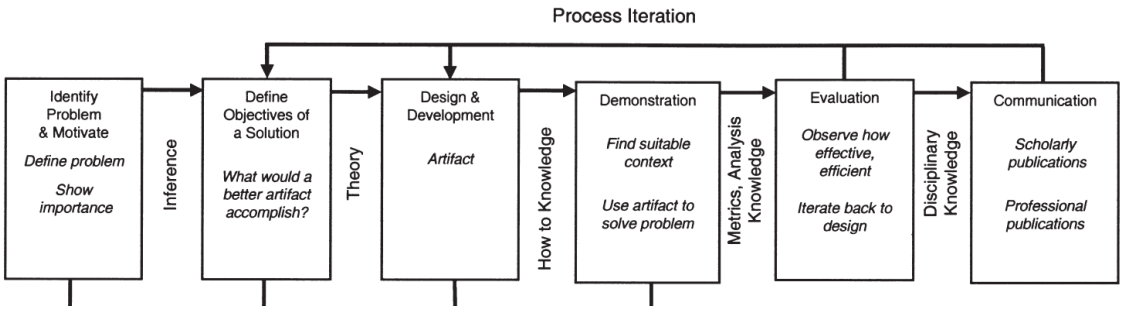

FIGURE 29 The activities of the DSRM process model (Peffers et al., 2007, 54)

The DSRM process does not define how, or in which phase the empirical data is gathered. Nor does it specify if the data is qualitative or quantitative. For the design science research, knowledge is required in every phase and activity. (Vaishnavi et al., 2004/2019; Hevner et al., 2004; Peffers et al., 2007). The client, Virtual Vehicle, had identified the problem (Activity 1) and the cybersecurity

engineering standard provided the initial knowledge for specifying the solution, an artifact (Activity 2). The artifact was developed (Activity 3) and demonstrated (Activity 4), after which the empirical data was utilised by evaluation (Activity 5). According to Peffers et al. (2007), the fifth activity of the DSRM process is the most common phase of empirical data evaluation in design science research. The communication (Activity 6) is handled via company confidential report and presentation to client, Virtual Vehicle, and as a master's thesis to the public. The DSRM process iteration (see figure 29) happened in the study in activities 3, 4, 5 and 6. The most iteration was between activities 3 and 4 while developing the artifact and use case in parallel. Activity 5 evaluation also concerned activities 3 and 4 as the client side took part into the development and demonstration by evaluating and giving feedback on the go. As the company confidential materials were handed over in the activity 6 communication, the research process returned to supplement the background theories and update problem identification among others. Each activity is presented here and its applicability in the study is evaluated:

> *Activity 1: Problem identification and motivation*. Define the specific research problem and justify the value of a solution. Because the problem definition will be used to develop an artifact that can effectively provide a solution, it may be useful to atomize the problem conceptually so that the solution can capture its complexity. Justifying the value of a solution accomplishes two things: it motivates the researcher and the audience of the research to pursue the solution and to accept the results and it helps to understand the reasoning associated with the researcher's understanding of the problem. Resources required for this activity include knowledge of the state of the problem and the importance of its solution. (Peffers et al., 2007, 52, 55.)

The problem identification was specified by Virtual Vehicle with their assignment to have a method and a tool how to analyse cybersecurity in road vehicles (passenger cars, trucks, buses, trailers, and motorcycles, excluding mopeds). The key reason for the assignment was an approaching cybersecurity engineering standard "ISO/SAE JWG 21434 Road vehicles - Cybersecurity engineering" (ISO/SAE, 2020). The standard would provide the requirements for a security risk analysis in the automotive domain but would not instruct how the analysis should be done or with what TARA method. The target was to investigate and compare the different existing TARA (Threat Analysis and Risk Assessment) (SAE, 2016b) approaches which meet the requirements of the new cybersecurity engineering standard. Once the proper method would be found, a tool for the actual analysis would be constructed as there weren't such tools available. The motivation for the study stemmed from the fact that road vehicles are already containing widely code and software that needs to be protected from cyberattacks. The trend is growing as vehicles gain more and more automated driving functions and communication interfaces, and the industry is targeting to manufacture self-driving independent road vehicles. The goal of any means of transport is to function in a secure and safe way.

> *Activity 2: Define the objectives for a solution*. Infer the objectives of a solution from the problem definition and knowledge of what is possible and feasible. The objectives can be quantitative, such as terms in which a desirable solution would be better than current ones, or qualitative, such as a description of how a new artifact is expected to support solutions to problems not hitherto addressed. The objectives should be inferred rationally from the problem specification. Resources required for this include knowledge of the state of problems and current solutions, if any, and their efficacy. (Peffers et al., 2007, 55.)

The objectives for the solution were to find a TARA based and cybersecurity engineering standard compliant security risk analysis method for road vehicles, and to create an equivalent tool to perform the analysis in a comprehensive manner. The study's practical section contained three parts: 1) finding a security risk analysis method which meets the requirements of the cybersecurity engineering standard (DSRM Activity 2 = *Comparison of the different TARA approaches*), 2) modelling of the cybersecurity engineering standard compliant analysis framework (TARA+AD) together with a security risk analysis template (DSRM Activity 3 = *Elaboration of the new approach*), and 3) use case creation and execution with the derived security risk analysis template (DSRM Activity 4 = *Application of the specific approach for the UC*).

The new cybersecurity engineering standard which defines the minimum criteria for cybersecurity of road vehicles is demanded by the UNECE (United Nations Economic Commission for Europe) (UNECE, 2021a). The standard was in a key role with its requirements and recommendations when the TARA based security risk analysis methods were examined through other standards and academic literature. The cybersecurity engineering standard referred to some frameworks to apply with threat modelling. The frameworks were EVITA (Ruddle et al., 2009; SAE, 2016b), TVRA (ETSI, 2010; SAE, 2016b), PASTA (UcedaVelez & Morana, 2015), and STRIDE (Microsoft Corporation, 2005). Out of this range, EVITA and STRIDE were already selected to the examination in the study. TVRA (Threat, Vulnerability and Risk Assessment) was abandoned from the selection as being insufficient, and PASTA (Process for Attack Simulation and Threat Analysis) was not considered being a candidate while searching the TARA based methods from the literature.

After few iterations, the final selection of security risk analysis methods consisted of seven candidates: TARA+, SARA, EVITA, HEAVENS, SAHARA, TARA Intel, and BRA. The evaluation and rating of the methods was performed by comparing each method how it covers the requirements and recommendations of the cybersecurity engineering standard. The comparison was executed with a matrix framework created with MS Excel. The chosen method was TARA+ which covered fully 18 out of 20 requirements and recommendations. SARA method covered also 18 out of 20 and TARA+ was built based on SARA, so in practise, the two methods were in a way the chosen ones. In addition, TARA+ borrowed elements from HEAVENS and STRIDE, and split the controllability factor taken from SARA into two components: one component for the driver of the vehicle, and the other component for the system of the vehicle. These enhancements took TARA+ in first place in the ranking.

> *Activity 3: Design and development*. Create the artifact. Such artifacts are potentially constructs, models, methods, or instantiations (each defined broadly) or "new properties of technical, social, and/or informational resources". Conceptually, a design research artifact can be any designed object in which a research contribution is embedded in the design. This activity includes determining the artifact's desired functionality and its architecture and then creating the actual artifact. Resources required for moving from objectives to design and development include knowledge of theory that can be brought to bear in a solution. (Peffers et al., 2007, 55.)

The mapping of the requirements and recommendations of the cybersecurity engineering standard with TARA+ revealed issues which could not be managed in a sensible manner. The different terminology of the standard and SARA, TARA+ and HEAVENS methods caused misunderstandings, and unnecessary components from SARA created challenges which could not be solved; thus, a new approach was initiated. The new approach is the artifact of the study.

A new analysis framework was developed: TARA+AD. The AD stands for Automated Driving which refers to the automated driving features which are key elements in the study (SAE, 2016a). Instead of making the skeleton of TARA+AD consisting of the elements from TARA+, SARA and HEAVENS, and matching the requirements of the cybersecurity engineering standard to it, the TARA+AD follows the exact form and sequence of the standard's requirements and recommendations. The necessary parts of selected methods are matched to the cybersecurity engineering standard and not vice versa. Instead of being a task-oriented method, TARA+AD acts as a framework providing a larger concept and guidance how to perform a security risk analysis.

The creation process of the new analysis framework TARA+AD had three major turning points and several enhancements during the iterations. The first instance was the creation of the new analysis framework based on SARA method. The reason was that TARA+ is basically same as SARA as TARA+ uses the same layout of the features. Based on the new framework illustration, a Word document was created for general instructions and an MS Excel spreadsheet was established as the analysis template with detailed instructions of specific steps how to make the security risk analysis. The aim of the analysis template was to complete each task in its dedicated sheet and move on to next task sheet once the previous task was completed. Every task sheet was supposed to include a table where the task in question would have been executed with the given detailed instructions. The progress of the analysis template was illogical and there were terminology issues. This led to the second turning point, in which a decision was made to create an analysis framework which follows the logic and order of the cybersecurity engineering standard instead of trying to fit SARA method's logic into the requirements. The third turning point was the analysis template logic change. Instead of having a sheet for every activity for task execution, one big table was built in one sheet which included all the tasks and subtasks of each activity.

After all iterations and modifications, the artifact, TARA+AD analysis framework, consisted of a framework diagram, general instructions (MS Word

document), and analysis template (MS Excel spreadsheet). The next step was to create a use case and test the analysis template.

> *Activity 4: Demonstration*. Demonstrate the use of the artifact to solve one or more instances of the problem. This could involve its use in experimentation, simulation, case study, proof, or other appropriate activity. Resources required for the demonstration include effective knowledge of how to use the artifact to solve the problem. (Peffers et al., 2007, 55.)

The demonstration was executed with a use case. The use case was created for a robot vehicle called SPIDER (Smart PhysIcal Demonstration and Evaluation Robot). The SPIDER was created for testing autonomous driving, and it uses both manual and automated driving functions which both can be tested in the use case. There were preconditions set for the use case creation and validation. The use case should include a functional description, present interconnections, and describe an architecture to identify the potential security risks based on the TARA+AD analysis framework. The use case should concern remote communication and what kind of cyberthreats that scenario might have. In the scenario there should be a remote control over the network with a laptop to the robot vehicle SPIDER with automated driving features (like path planning) and safety measures (like collision avoidance). The use case creation was started with the given preconditions in mind and by utilizing the analysis template. The development of the analysis template continued while creating the use case, as certain practical matters arose during the parallel development. The need with the use case was to apply cybersecurity in a vehicle level with two different threat scenarios: communication in application level, and communication in transport/network level. Two cyberattack scenarios (CAS) were distinguished: CAS1 and CAS2. CAS1 Description: *The hacker could have stolen the laptop/tablet and acquired the employee ID (username and password)*. In this scenario the human attacker has committed a company theft and stolen both the equipment and login credentials from an Operating Engineer. CAS2 Description: *The hacker uses remote equipment (laptop/tablet)*. In the second scenario the human attacker is using his/her own equipment to gain access to the SPIDER. The attacker has been able to make a breach into the company's systems and has primary and secondary targets to cause damage of any kind. The use case execution happened on paper as COVID-19 pandemic prevented the real-life validation with the SPIDER robot vehicle.

> *Activity 5: Evaluation*. Observe and measure how well the artifact supports a solution to the problem. This activity involves comparing the objectives of a solution to actual observed results from use of the artifact in the demonstration. It requires knowledge of relevant metrics and analysis techniques. Depending on the nature of the problem venue and the artifact, evaluation could take many forms. It could include items such as a comparison of the artifact's functionality with the solution objectives from activity 2, objective quantitative performance measures such as budgets or items produced, the results of satisfaction surveys, client feedback, or simulations. It could include quantifiable measures of system performance, such as response time or availability. Conceptually, such evaluation could include any appropriate empirical

> evidence or logical proof. At the end of this activity the researchers can decide whether to iterate back to activity 3 to try to improve the effectiveness of the artifact or to continue on to communication and leave further improvement to subsequent projects. The nature of the research venue may dictate whether such iteration is feasible or not. (Peffers et al., 2007, 56.)

The evaluation of the artifact happened via client feedback. The whole research process, and especially the iterations during the development of the analysis framework and template were conducted in collaboration with two employees of Virtual Vehicle. The employees were a Lead Researcher from Cybersecurity and Functional Safety department, and a Functional Safety Specialist from Model-based System Engineering department. By the time the use case development got started, a third employee from Virtual Vehicle joined the research activity. A Researcher specialized in Dependable Systems took part to the use case development process as an expert of robot vehicles.

The evaluation of the artifact is divided into three parts as per the research design: 1) Comparison of the different TARA approaches, 2) Elaboration of the new approach, and 3) Application of the specific approach for the UC.

1) Comparison of the different TARA approaches

During the investigation of related literature for the study, different TARA approaches were identified and analysed. All of them provided pros and cons for their use in specific fields of applications. For the application in the study at hand, the need was to have a suitable approach for Automated Driving (AD) applications in the sector of road vehicles. For such application, the new, upcoming standard "ISO/SAE 21434 - Road Vehicle: Cybersecurity Engineering" had to be taken as a basis for the work. For better comparison of the different TARA approaches with the different aspects of requirements and recommendations in the cybersecurity engineering standard, it was decided to elaborate a table that contains at the one side the requirements of the standard and a coverage analysis of the different TARA approaches. Based on that table a systematic decision process was possible, by using a coverage metric and providing specific rational for each metric.

2) Elaboration of the new approach

As a successful result of the comparison of the different TARA approaches, the two most promising security risk analysis approaches (TARA+ and SARA) were identified, and both were chosen to be used as a basis for the following elaboration of a specific TARA approach. To present such result, the joint decision was taken to use an MS Excel-based approach to elaborate a stepwise security risk analysis approach called TARA+AD. The analysis steps were defined based on the cybersecurity engineering standard and the specific activities of each step has been elaborated based on TARA+ and SARA. As a very satisfying result a security risk analysis (Spreadsheet) template was

created to be usable for the SPIDER use case of automated driving in the study. The analysis template contains all relevant guidance, descriptions, assessment metrics and required rationales to perform each of the steps in a very systematic and straight forward way.

3) Application of the specific approach for the UC

The evaluation of the application of the TARA+AD analysis framework approach for the SPIDER use case of automated driving was considered very satisfactory. The use case contained two specific cybersecurity threat scenarios which were directly related to the communication between the Operator (human user) and the SPIDER. As a result, a list of possible malicious attack scenarios was provided representing the main vulnerabilities that SPIDER has at the vehicle level in the context of cybersecurity. Finally, a risk assessment of such vulnerabilities generated a valuable output to enhance cybersecurity for SPIDER and an adequate example to understand the application of the presented TARA+AD analysis framework and its security risk analysis template.

> *Activity 6. Communication*. Communicate the problem and its importance, the artifact, its utility and novelty, the rigor of its design, and its effectiveness to researchers and other relevant audiences such as practicing professionals, when appropriate. In scholarly research publications, researchers might use the structure of this process to structure the paper, just as the nominal structure of an empirical research process (problem definition, literature review, hypothesis development, data collection, analysis, results, discussion, and conclusion) is a common structure for empirical research papers. Communication requires knowledge of the disciplinary culture. (Peffers et al., 2007, 56.)

The communication manifests as three outputs: 1) Report handover to Virtual Vehicle, 2) Presentation of the solution to selected internal audience in Virtual Vehicle, and 3) Master's Thesis.

The report handover to Virtual Vehicle happened after the implementation phase was completed. The partial thesis handover was done as the allocated project was ending. The report was a 269-page document written in a thesis template. The report contained a selection of most relevant chapters, and the missing chapters were indicated with a disclaimer that the chapter is not part of the report version but will be published later in the master's thesis. The company confidential material was added as appendixes and majority of the material is removed from the public thesis based on NDA (non-disclosure agreement). TARA+AD analysis framework and analysis template related documents as well as SPIDER use case execution file were handed over together with the report.

A presentation of the solution, the artifact, was given remotely to selected internal audience in Virtual Vehicle, Austria. The MS PowerPoint slideshow covered the following topics: Motivation, Requirements for Security Risk Analysis, Investigation of TARA Methods, Selected TARA Methods, New

Framework: TARA+AD, Use Case Application, Use Case Results, and Conclusions. Based on the received feedback from the audience, the slideshow was updated accordingly and handed over for Virtual Vehicle's internal distribution.

The research study is published as a master's thesis electronically by University of Jyväskylä, Faculty of Information Technology. The thesis presents majority of the TARA+AD analysis framework process, and shares examples or excerpts of the analysis template, but excludes the documents and details under Virtual Vehicle's NDA. The analysis template is developed only for Virtual Vehicle's usage and cannot be shared publicly.

4.2 The Artifact

The concept of artifact in the design science was introduced by Herbert Simon (1996) in his book of the sciences of the artificial. Simon (1996) considered design science to be research about how things could be. The purpose of design science research is to create something new with innovative artifacts to solve real-world problems (vom Brocke et al., 2020). Different scholars have defined what an artifact can be. The definitions are listed in the following table (table 17).

TABLE 17 Design science artifact definitions by scholars

Scholars	**Definition of Artifact**
Hevner, March, Park & Ram (2004)	Constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), and instantiations (implemented and prototype systems).
Vaishnavi, Kuechler & Petter (2004/2019)	The artifacts created in the design science research process include, but are not limited to, algorithms, human/computer interfaces, and system design methodologies or languages.
Peffers, Tuunanen, Rothenberger & Chatterjee (2007)	Artifacts may include constructs, models, methods, and instantiations. They may also include social innovations or new properties of technical, social, or informational resources. In short, this definition includes any designed object with an embedded solution to an understood research problem.

(continues)

Table 17 (continues)

Gregor & Hevner (2013)	In IS, DSR involves the construction of a wide range of socio-technical artifacts such as decision support systems, modelling tools, governance strategies, methods for IS evaluation, and IS change interventions.
Vom Brocke & Maedche (2019)	Design entities are design artifacts like constructs, models, methods and instantiations, design processes, and artifact evolution processes.

The artifact of the design science research study is the TARA+AD analysis framework. TARA+AD consists of the necessary parts of the selected methods SARA (Monteuuis et al., 2018) and TARA+ (Bolovinou et al., 2019) to comply with the requirements and recommendations of the cybersecurity engineering standard (ISO/SAE, 2020). The framework's full name is Threat Analysis and Risk Assessment for Automated Driving. TARA+ is a reference to the actual TARA+ method by Bolovinou et al. (2019), and AD (Automated Driving) refers to the automated driving features like lane keeping (SAE, 2016a). The approach was considered to act as a framework rather than as a method. A method gives guidance and/or steps how to perform a certain task (Vaishnavi et al., 2004/2019). The TARA+AD consists of the most feasible parts of two TARA methods (SARA and TARA+) and provides a larger concept and guidance how to perform a security risk analysis.

The TARA+AD analysis framework acts as a high-level guidance for the public. The diagram of the framework was introduced in figure 25 (see figure 25) in chapter 3.3.2 and the functions of the different blocks in the analysis framework diagram are named as: A = activity, T = task, and ST = sub-task. Due to the nature of client-oriented research, the created products of the TARA+AD analysis framework are company confidential. The products are a MS Word document called general instructions, and a MS Excel spreadsheet called analysis template. The general instructions consists of high-level descriptions of each security risk analysis activity, task, and sub-task with given examples and illustrations. The descriptions, examples and illustrations in the general instructions are mostly taken from the cybersecurity engineering standard, but some reference to SARA and TARA+ methods are used. The analysis template consists of fifteen sheets. Eight of them are dedicated to the activities providing detailed information, instructions, illustrations, examples, and references taken from the cybersecurity engineering standard. Some formulas, figures and tables are adapted from the TARA+ and SARA methods. The actual risk analysis happens in a sheet with one big table including all the tasks and subtasks of each activity. In addition to activity related sheets and the risk analysis sheet, there are six supplementary sheets for project control, progress monitoring, assumptions, navigation, further information, and data for functionality management of the spreadsheet itself. With this given security risk analysis template, the discovering and listing of potential attacks can be produced and documented in one place. The analysis template has very little

automation within its functions and there are some manual activities to be done, but the usage has been designed and experimented to work as effortlessly as possible. The decision to use MS Office tools was done as the given schedule of the allocated project was closing and programming a separate software would have been too time consuming, and possibly challenging to be administered.

The artifact was evaluated within the DSRM process model (Peffers et al., 2007), but it is interesting to reflect the artifact also to other design science research approaches. Hevner et al. (2004) defined five different design evaluation methods. The evaluation methods are displayed in the following table (table 18).

TABLE 18 Design Evaluation Methods (Hevner et al., 2004, 86)

Design Evaluation Methods	
1. Observational	Case Study: Study artifact in depth in business environment
	Field Study: Monitor use of artifact in multiple projects
2. Analytical	Static Analysis: Examine structure of artifact for static qualities (e.g., complexity)
	Architecture Analysis: Study fit of artifact into technical IS architecture
	Optimization: Demonstrate inherent optimal properties of artifact or provide optimality bounds on artifact behavior
	Dynamic Analysis: Study artifact in use for dynamic qualities (e.g., performance)
3. Experimental	Controlled Experiment: Study artifact in controlled environment for qualities (e.g., usability)
	Simulation - Execute artifact with artificial data
4. Testing	Functional (Black Box) Testing: Execute artifact interfaces to discover failures and identify defects
	Structural (White Box) Testing: Perform coverage testing of some metric (e.g., execution paths) in the artifact implementation
5. Descriptive	Informed Argument: Use information from the knowledge base (e.g., relevant research) to build a convincing argument for the artifact's utility
	Scenarios: Construct detailed scenarios around the artifact to demonstrate its utility

The TARA+AD analysis framework evaluation can be considered being experimental. The usability of the analysis template was developed and tested together with the client representatives and the simulation was executed in paper (= artificial data) with a use case of threat scenarios. The descriptive evaluation was a possible candidate as there was not a clear TARA based security risk analysis method and a tool to perform the risk analysis as per cybersecurity engineering standard. But the descriptive evaluation concerns only innovative artifacts which are challenging to be evaluated otherwise with the existing means. (Hevner et al., 2004.) The TARA+AD analysis framework uses existing methods, standards, and software applications. The novelty lies in

the enhanced framework based on the requirements of the cybersecurity engineering standard and the analysis template for the practical security risk analysis.

Another appealing approach to evaluate TARA+AD analysis framework is the DSR knowledge contribution framework by Gregor and Hevner (2013). The framework is illustrated in figure 30 (figure 30) and it presents a solution maturity and application domain maturity in its axes. The application domain axe shows if the maturity of problem context is high or low. The solution axe shows if the maturity of existing artifact as a potential solution is high or low.

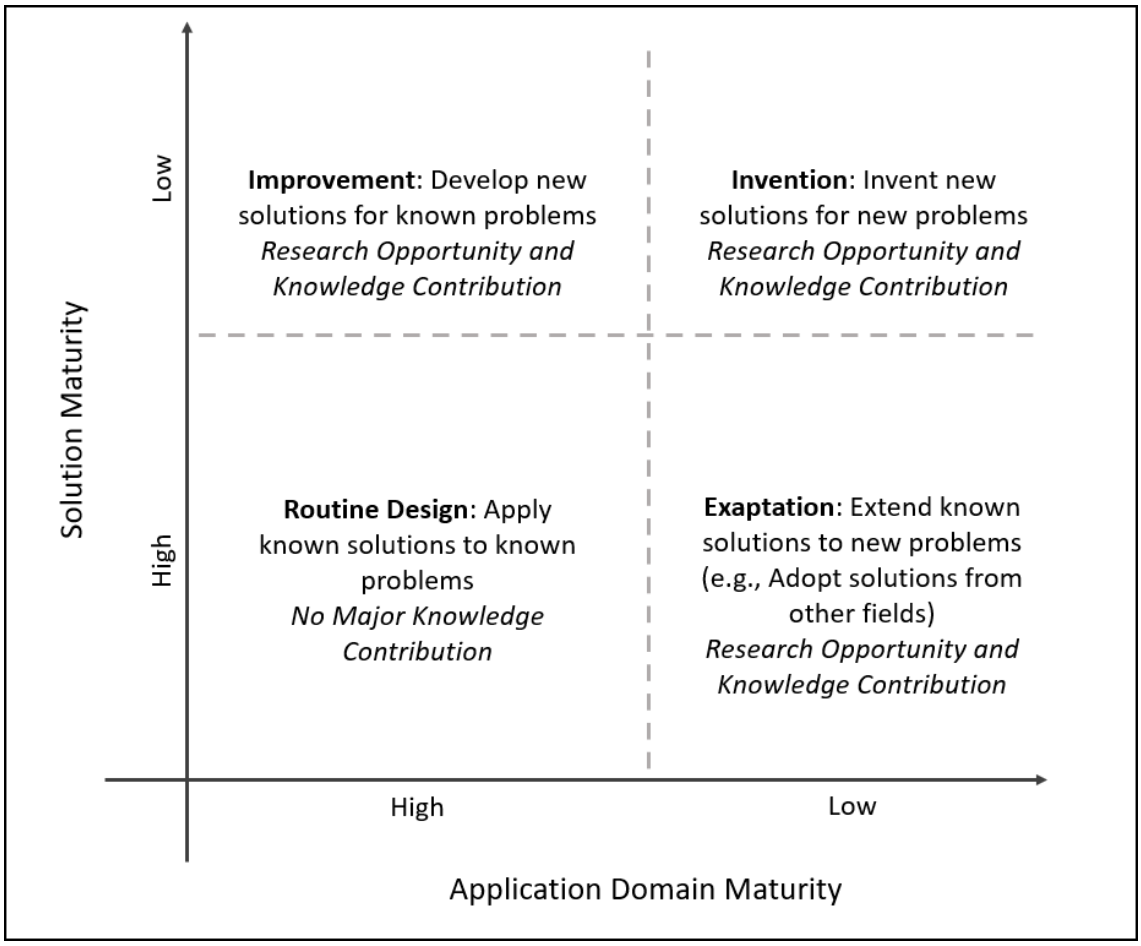

FIGURE 30 DSR Knowledge Contribution Framework (Gregor & Hevner, 2013, 345)

The different quadrants describe the type and outcome scenarios of design science research and if there is research opportunity and knowledge contribution in the first place. Each quadrant is presented below.

Invention: New Solutions for New Problems

This quadrant is almost next to impossible to be achieved today. Nothing is truly new, but is based on existing tools, products, hardware, methods, frameworks, ideas, knowledge etc. The problems should be so new that no one

realises they even exist. And the solution should be something that hasn't existed before. The invention, the artifact, should take form from pure void, and not after some design theory. Examples how this quadrant can be achieved are way back in the history as inventing a bicycle or a calculating machine. The new artifact should be a radical breakthrough requiring creativity, insight, imagination, knowledge, and cognitive skills.

Improvement: New Solutions for Known Problems

This quadrant is the most typical result in the design science research. The purpose is to create better solutions with efficient and effective artifacts. The artifacts can be technologies, products, services, processes, or ideas. It is essential to point out that the existing solutions do not resolve the problem or there isn't a solution on hand. A reasoning is needed why the new solution is different from others, and how the artifact improves e.g., productivity or efficiency, or any quality measure.

Exaptation: Known Solutions Extended to New Problems

This quadrant is based on interdisciplinary research and is common in information systems research. Artifacts can be applied from a different field of science to resolve a problem in another field. This can happen in situations in which the own discipline does not offer feasible artifacts, or artifacts do not exist. This kind of scenario allows artifacts to be exapted to a different discipline to solve new kind of problem context. Example of exaptation is for instance applying data warehousing in the health care domain in health information systems.

Routine Design: Known Solutions for Known Problems

This quadrant represents routine work where the problem area is well known and understood, and existing artifacts will solve the problem. It is in fact questionable if this falls at all contributing to the research. In some cases, the discoveries of routine work might lead to actual research, but in these cases the quadrant will also change.

The TARA+AD analysis framework lands into the improvement quadrant. The research problem was that the new cybersecurity engineering standard was approaching, and it contained requirements and recommendations what to include to a TARA based security risk analysis for road vehicles. None of the existing TARA based security risk analysis methods did exclusively fulfil the requirements of the standard, nor was there a tool to perform the analysis. The new TARA+AD analysis framework solves the lack of having a specific TARA based security risk analysis method tailored for the cybersecurity engineering standard. The framework is illustrated with a diagram of the analysis flow and related activities, tasks, and sub-tasks. The framework provides general

instructions and an analysis template for the actual security risk analysis. The general instructions and analysis template are company confidential, but the information used to these products is public and can be gathered for a tool creation by any instance. The TARA+AD analysis framework was evaluated iteratively during development phase and with a use case. The results were pleasant to the client and the framework solved the research problem.

5 DISCUSSION

This chapter discusses the research problems and answers to the research questions and gathers the implications to research and to practice. The focus on research implications is on the literature from the standards, technical report and guidebook of automotive industry, and the security risk analysis methods. The practical side is discussed from the perspective of the created TARA+AD analysis framework and related analysis template, and the evaluation of both with the SPIDER use case.

5.1 Reflection on Research Problems

The new standard ISO/SAE 21434 concerning cybersecurity engineering of road vehicles was released in early 2020 and as such, there was no previous studies concerning a security analysis of the brand-new standard when the study was conducted. The new standard has been developed since 2016 by experts from ISO (International Organization for Standardization) and SAE (Society of Automotive Engineers) organizations involving different companies and manufacturers. (Schmittner et al., 2018.)

ISO/SAE 21434 aims to provide a starting point and an official reference for vehicular cybersecurity. The standard defines a common terminology so that different operators in the automotive domain can better understand each other. The standard gives the minimum criteria for cybersecurity in a vehicle and defines security assurance levels for metrics and analysis purposes. With the new cybersecurity engineering standard, the vehicle manufacturers can make sure their products are sufficiently secured when driving on the roads. (Akram, 2019.)

The cybersecurity engineering standard does not provide an exact schema how to perform a security risk analysis from start to end as one entity. The guidance gets shattered when instructions and suggestions are spread into different sections and annexes. The standard indicates that TARA, Threat

Analysis and Risk Assessment (SAE, 2016b) framework is the basis of the security risk analysis, but very few TARA based methods are mentioned. This leads to the research problem: how to make a TARA based and cybersecurity engineering standard compliant security risk analysis for road vehicles. The solution requires a security risk analysis method with detailed instructions, and an equivalent tool to perform the analysis in a comprehensive manner.

The research questions proposed in chapter 1.4:

Research Question #1:
Which existing risk analysis methods cover the requirements regarding security risk analysis in the standard ISO/SAE JWG 21434?

Research Question #2:
How could a standard compatible security risk analysis method look like in the early design phase?

The targets of the research questions were to discover the potential TARA compatible security risk analysis method for examining cybersecurity in road vehicles, and to provide the most feasible method fulfilling the requirements of the cybersecurity engineering standard (ISO/SAE, 2020). Research question 2 aimed to provide a solution concept based on the results from the research question 1. As an outcome, a hybrid of two TARA compatible risk analysis methods were selected for the security risk analysis framework and template creation. A description of the selected approach by concrete steps was defined and a use case for the execution part was created and tested.

The findings are encouraging, as there were such TARA compatible security risk analysis methods which met the requirements of the cybersecurity engineering standard. Even though there was not a fully compatible analysis method to match the cybersecurity engineering standard requirements, there were methods that could be utilized in the creation of the new approach. The approach was built as an analysis framework due to its nature of consisting of assessment metrics and required rationales in addition to basic guidance and descriptions. It was considered being more than just a method that gives steps how to perform a certain task (Vaishnavi et al., 2004/2019).

The results of executing the SPIDER use case of automated driving brought meaningful findings in two ways. The analysis template was evaluated and developed based on the practical observations during the use case execution. This approach improved the analysis template when there were inconsistencies and illogical functions discovered. The other meaningful finding was the results of the security risk analysis based on the SPIDER use case. The analysis revealed the main vulnerabilities that the SPIDER could have as an automated vehicle in its cybersecurity interface. The analysis provided a list of possible damage and threat scenarios and their impact on assets, and attack paths and their feasibility for a probability of an attack. The threats could then

be assessed in the risk determination and risk treatment sections to improve the cybersecurity interface of the SPIDER.

5.2 Implications to Research

The implications to research can be viewed from two perspectives. The first perspective is producing a feasible security risk analysis method, or in this case, a new analysis framework to address the need for threat and risk analysis required by the cybersecurity engineering standard. The new standard is giving requirements and recommendations what to include to a security risk analysis but does not provide the tools or methods how to make the analysis in practise (ISO/SAE, 2020). The predecessor cybersecurity guidebook provides information of the TARA compatible security risk analysis methods but as the guidebook was created in 2016, it is lacking behind with its method proposals (SAE, 2016b). With this study, new TARA compatible security risk analysis methods have been discovered. From the basis of the found methods, a new analysis framework has been created to address the exact needs of the cybersecurity engineering standard.

The second perspective of viewing the implications to research is bringing a new security risk analysis framework to the scientific community. SARA (Monteuuis et al., 2018) and TARA+ (Bolovinou et al., 2019) methods were created before the cybersecurity engineering standard (ISO/SAE, 2020) was published, so they did not follow the exact pattern of given requirements and recommendations needed for the analysis. Both methods did have the skeleton of cybersecurity in place, as they were using the cybersecurity guidebook (SAE, 2016b), the automation level technical report (SAE, 2016a) and the functional safety standard (ISO, 2018) as reference like this study. TARA+ was also referring to a draft version of the cybersecurity engineering standard, but as the standard was not ready during that time, the exact details were missing. The created analysis framework TARA+AD is a tribute to SARA and TARA+ methods by sharing the best practises from both methods and to bring a new approach to the field which addresses the needs of the cybersecurity engineering standard. The advanced features of TARA+ method can take the risk analysis even further with its automated driving level approach, which is an interesting topic for the future research.

5.3 Implications to Practice

The implications to practice are twofold. The result of the study was a new TARA compatible analysis framework, TARA+AD, and related analysis template. The TARA+AD analysis framework and the template corresponded to the need to have methods and tools for making a risk analysis based on the

requirements and recommendations by the cybersecurity engineering standard (ISO/SAE, 2020). The TARA+AD analysis framework was created based on the cybersecurity engineering standard, and the SARA (Monteuuis et al., 2018) and TARA+ (Bolovinou et al., 2019) methods. The analysis template was created from the basis of the TARA+AD analysis framework and enhanced during the SPIDER use case execution to match better the practise. The practise in this sense means the practicalities used by Virtual Vehicle who ordered the research. The analysis template itself is solely used by Virtual Vehicle for its purposes, but the TARA+AD analysis framework is public as the framework is based on the cybersecurity engineering standard, and SARA and TARA+ methods. The TARA+AD analysis framework can be utilized by scientific communities and other organizations for making a tool for the security risk analysis of cybersecurity in road vehicles.

6 CONCLUSIONS

This chapter summarizes and concludes the study. The contribution of the results are presented, limitations are discussed, and further research topics are proposed.

6.1 Summary of the Study

The purpose of the study was to discover a potential TARA (Threat Analysis and Risk Assessment) based security risk analysis method for examining cybersecurity in road vehicles, and to provide the most feasible method fulfilling the requirements of the new cybersecurity engineering standard. The design of the empirical section of the study consisted of three parts: 1) Comparison of the different TARA approaches, 2) Elaboration of the new approach, and 3) Application of the specific approach for the UC.

The introduction explained the backgrounds and motivations for the topic. As road vehicles are not anymore plain mechanical devices but contain numerous amounts of computers and myriad lines of code, they need to be protected from cyberattacks. The research objectives and the scope targeted to explore the security impact on road vehicle safety. The goal was to find a TARA compatible security risk analysis method which meets the assignment's expectations and fulfils the requirements of the cybersecurity engineering standard. The research problem was identified being the lack of a feasible method and a tool how to make the security risk analysis. The forthcoming cybersecurity engineering standard gives the requirements and recommendations of TARA compatible security risk analysis but does not tell how it should be carried through. The rest of the introductory chapter presented shortly the research methodology and results and explained the structure of the research study.

The theoretical background concentrated on important automotive concepts and standards. The concepts concerned the automotive industry today,

dependability from the information technology area and how it affects road vehicles, cybersecurity, like IoT (Internet of Things), and vehicular communication, like V2X (Vehicle-to-Everything). Vehicles are getting more and more intelligent and having greater amounts of automated features and systems in them. Automated driving is a transportation mode of a vehicle with less manual interaction from the driver. Automated driving requires intelligent vehicles which contain system algorithms that understand the environment around and can act accordingly. These dependable systems aim to avoid service failures and gain trust. It all comes to making vehicles safe and secure. Cybersecurity concerns all aspects of life. The Internet of Things (IoT), Cyber-Physical Systems (CPS) and Cyber-Physical Vehicle Systems (CPVS) are part of vehicles' structure and functionality. Vehicles are smart devices with their multiple sensors and embedded technology and services enabling communication with other smart devices and infrastructure around. This kind of communication is called Vehicle-to-Everything Communication. It is an evolving new technology that will eventually connect vehicles, infrastructure, pedestrians, networks, clouds, devices, and grids together for intelligent, energy sufficient and safe transportation. This kind of technology is open to cyberattacks. People's safety is threatened not only physically, but also privacy and data security are jeopardized. Any kind of threats are essential to be identified so countermeasures can be developed in advance.

The standards in automotive industry were presented on the latter half of the theoretical background chapter. The discussion concerned two standards, one technical report, and one guidebook related to the research. The standards by ISO (Organization for Standardization) were *ISO 26262 Functional Safety* (ISO, 2018) and *ISO/SAE JWG 21434 Road vehicles - Cybersecurity engineering* (ISO/SAE, 2020). The technical report by SAE (Society of Automotive Engineers) was *SAE J3016 Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems* (SAE, 2016a) and the guidebook by SAE was *SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems* (SAE, 2016b). The standards and equivalent reports are vital in the automotive industry and can be considered as laws as any road vehicle has to meet the set requirements to be secure and safe for the passenger(s) and surrounding vehicles, people, and environment (ISO, 2018). As vehicles contain and gain software systems in an increasing rate, it is important to make the vehicles compatible with the requirements of cybersecurity (SAE, 2016b; ISO/SAE, 2020). The vehicles become more and more independent with the automated driving functionalities (SAE, 2016a), so it is vital to invest to the security risk analysis to improve the road vehicles' cybersecurity (ISO/SAE, 2020).

The research methods of the study discussed Design Science Research (DSR) and described the empirical part of the study. The research method used was Design Science (DS) (Simon, 1996) as the target was to make an IT artifact that solves the problem with a real-life solution, in this case, a security risk analysis method. Design science is research about how things could be. The purpose of DSR is to create something new with innovative artifacts to solve real-world problems (vom Brocke et al., 2020). Scholars have developed

different approaches how to define and evaluate design science research. The chosen approach for the study is Design Science Research Method (DSRM) process model created by Peffers et al. (2007).

The empirical part catalogued the different security risk analysis methods discovered during investigation of TARA (Threat Analysis and Risk Assessment) (SAE, 2016b) compatible methods. The criteria were that the method must match with the given requirements and recommendations by the cybersecurity engineering standard. During the investigation, the selection of the final candidates changed and expanded due to perceived findings. Some methods were not applicable in the automotive domain, but new matching methods were discovered. The research by Macher et al. (2016a) was utilized to finetune the final selection of the risk analysis methods to be evaluated and rated against the requirements and recommendations by the cybersecurity engineering standard. After examining the seven chosen methods, two of the methods showed outstanding features. The chosen method was TARA+ (Controllability-aware Threat Analysis and Risk Assessment) by Bolovinou et al. (2019) but as TARA+ was created from the basis of SARA (Security Automotive Risk Analysis) by Monteuuis et al. (2018), it was evident that both methods could be stated as primary selections. After selecting the appropriate methods, an analysis framework named TARA+AD (Threat Analysis and Risk Assessment for Automated Driving) was created. A mapping activity was conducted to match the requirements and recommendations of the cybersecurity engineering standard. After some iterations, it was noticed that the defined activities and tasks adapted from TARA+ and SARA methods did not meet well with the cybersecurity engineering standard's analysis framework in practise. While creating the TARA+AD analysis framework, related analysis template with MS Excel for the actual security risk analysis was developed in parallel. The logic of the analysis template did not work with the logic adapted from the SARA method. A decision was made to start all over the creation of the TARA+AD from the basis of the cybersecurity engineering standard's requirements and recommendations. The logic of the analysis template was also changed from individual task performing to a one analysis table approach consisting of all tasks created for the analysis process. The created solution (analysis template) needed to be evaluated, thus a use case for a robot vehicle called SPIDER (Smart PhysIcal Demonstration and Evaluation Robot) was created. The use case contained two cyberattack scenarios where an external hacker could cause harm and damage to the SPIDER or humans or infrastructure around the SPIDER. During the execution of the SPIDER use case, the analysis framework and related analysis template was developed and improved based on the practical findings during the evaluation of the use case.

The closing chapters presented the findings of the study and results were discussed. The DSRM process model was used to evaluate the research and its outcome. The DSRM process contains six activities, and each activity was presented and its applicability in the study was evaluated. The activities are problem identification and motivation, defining the objectives for a solution,

design and development, demonstration, evaluation, and communication. The created TARA+AD analysis framework is the artifact of the design science research study. The TARA+AD analysis framework acts as a high-level guidance for the public. The related general instructions and analysis template are company confidential due to the nature of client-oriented research. The evaluation of the artifact was discussed from three aspects: 1) the comparison of the different TARA approaches, 2) the elaboration of the new approach, and 3) the application of the specific approach for the UC (the analysis template) for the SPIDER use case. Each aspect was considered successful and satisfactory. The comparison of the different TARA approaches provided good grounds for the next phase which was creating the new TARA+AD analysis framework approach. Then the TARA+AD analysis framework and related analysis template was evaluated and developed during SPIDER use case execution. The results of the security risk analysis for the SPIDER use case provided meaningful input of the vulnerabilities with the SPIDER's cybersecurity interface and how the vulnerabilities could be addressed correctly.

6.2 Summary of the Contribution

The contribution of the study is the TARA+AD analysis framework which addresses the need for threat and risk analysis required by the cybersecurity engineering standard (ISO/SAE, 2020). The standard gives the needed requirements and recommendations and suggests using TARA compatible security risks analysis methods for threat assessment. The standard does not provide practical information how the threat assessment should be done. The need for a specified method and tool was evident, and as the TARA based methods were examined, new methods were discovered. The most important discovered methods were SARA (Monteuuis et al., 2018) and TARA+ (Bolovinou et al., 2019) which fulfilled the requirements and recommendations of the cybersecurity engineering standard. The challenge to use these methods came to terminology issues, unnecessary elements and illogical performing of the analysis steps. Thus, it was clearer and more logical to create a new framework based on the cybersecurity engineering standard and fit the elements from SARA and TARA+ to the framework. The TARA+AD analysis framework brings a new kind of security risk analysis framework to the scientific community and automotive domain and honours the effort of SARA and TARA+ methods.

The examination of the different concepts related to the study brings more insight what kind of technologies there exists in the automotive domain. In the future, when autonomous self-driving vehicles are reality, there might be competition between software providers and carmakers concerning who dominates the automotive industry (Rahim et al., 2021). The new kind of communication technology Vehicle-to-Everything (V2X) with its many categories gives an important outlook what is approaching and what kind of

possibilities humankind could have when the technology is harnessed in the right way. Less accidents, injuries, and deaths in the traffic, and more flexible, easy, and time-saving commuting can be real in the future. (Sedar et al., 2023.)

6.3 Limitations

The study had different limitations related to security risk analysis methods, tools used for the solution creation, use case of the implementation of the solution, and restrictions related to research documentation.

The chosen TARA methods, SARA (Monteuuis et al., 2018) and TARA+ (Bolovinou et al., 2019) were not 100% utilized in the new TARA+AD analysis framework. SARA's driverless system factor was not included to the new framework. SARA aims to fill the gaps in the existing methods concerning driverless vehicles by presenting new metrics called Observation and Controllability. Observation is a metric which goal is to have the autonomous vehicle's automated driving system (ADS) able to detect possible threats and hazards which cause system failures. The Observation factor is needed since fully autonomous vehicle needs to make internal and external observations as the human is not involved or human perception cannot be trusted. The Controllability factor then quantifies the influence of the ADS or human driver on security risk. TARA+ method enhances the Controllability factor even further by splitting it into two components: one component for the driver of the vehicle, and the other component for the system of the vehicle. TARA+AD analysis framework does not separate whether the vehicle is driven by a human, or if its fully autonomous. This factor is defined manually in the use case prepared for the security risk analysis done with the TARA+AD analysis template (MS Excel spreadsheet).

The tools used to model and implement TARA+AD analysis framework were MS Office applications instead of coding a separate tool for the practicalities. As an example, MS Excel spreadsheet was established for the security risk analysis. The modelling was aimed to be carried out with SysML (Systems Modeling Language) (SysML.org, 2023) or MSTMT (Microsoft Threat Modeling Tool) (Microsoft, 2022). The SysML and MSTMT were found too time consuming and laborious in relation to the demand from Virtual Vehicle and to the given schedule of the allocated project.

The use case scenarios were designed only for a robot vehicle and a passenger car with human inside was not taken into consideration. The use case execution and evaluation needed to be as realistic and feasible as possible. The use case was though fitting the needed purpose at the time, but it could have been useful to also design another kind of scenario with human driver inside a vehicle. Another situation-based issue was that the use case was executed on paper, but this was due to the COVID-19 pandemic which had outbursts during the implementation phase. The use case designed for the study was more a theory-based approach due to the lack of field testing with the robot vehicle.

The use case for the field test would most probably be designed in a more practical way.

The documents created for TARA+AD analysis framework are company confidential, which is due to the nature of the client-based research. Different documents were created with MS Office tools during each phase of the study. The most essential documents created were general instructions (MS Word document) describing the TARA+AD analysis framework in high-level, and analysis template (MS Excel spreadsheet) with which the actual analysis can be executed in practise. The TARA+AD analysis framework diagram is open for the public and some excerpts from the analysis template are shared in the study.

6.4 Further Research Topics

Some potential research topics rouse during the outlining of the research scope and examining literature for the theoretical background. The human aspect on security threats is an interesting topic as in the center of everything is a human with human nature and features. What kind of security threats the humans inside the vehicle are causing and how to mitigate the impact of humans on security threats? That is a question worth studying. In automated driving with intelligent vehicles, the systems are assisting the driver. Even if the vehicle contains assisting features, one can drive like a crazy and trust the vehicle to do the security and safety related decisions and actions. Where is the limit of intervention? Can a driver overrule the assisting feature? As an example, a person had a reverse radar feature in his vehicle. When he drove a vehicle that hadn't the radar, he pushed another vehicle for quite a distance before realizing what was happening. He explained that the vehicle did not alarm him about the collision with the other vehicle. Are humans becoming helpless and insensitive to basic functions of a vehicle because of automated assisting features? When giving a vehicle some autonomy, how does it affect the driver? Humans will have a kind of familiarization and habituation effect and they trust the technology and cannot react or react wrong without the assistance.

Another possible future research topic is the ethics of automated driving. Which one makes the decision of ethical choices while operating a vehicle: the human driver or the vehicle itself? In case of certain crash, should the vehicle try to cause minimum damage to the driver who is alone in the vehicle, or the other vehicle which has a family of five in it, or a crowd of schoolchildren passing pedestrian crossing? Another interesting point is how can a vehicle be taught to operate ethically. What does it require using artificial intelligence (AI) to make a vehicle learn? And who gets to decide what is right or wrong when creating the ethical scenarios to be taught.

The vehicular industry and research area are providing multiple issues and uncertainties to be studied further. The future with intelligent independently operating vehicles is being built little by little but most certainly with determination.

REFERENCES

Akram, H. I., [ISO 21434 The Standard for Automotive Cyber Security (2019)]. (28.2.2019). *ISO 21434 The Standard for Automotive Cyber Security (2019)* [video]. Retrieved 6.7.2020 from https://www.youtube.com/watch?v=ybs969W53nk

Al-Fuqaha, A., Kwigizile, V., & Oh, J. (2018). *Vehicle-to-device (V2D) communications: readiness of the technology and potential applications for people with disability* (No. TRCLC 2016-06). Western Michigan University.

Alalewi, A., Dayoub, I., & Cherkaoui, S. (2021). On 5G-V2X use cases and enabling technologies: A comprehensive survey. *IEEE Access, 9*, 107710-107737.

Alberts, C. J., Behrens, S. G., Pethia, R. D., & Wilson, W. R. (1999). *Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, Version 1.0*. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Alnasser, A., Sun, H., & Jiang, J. (2019). Cyber security challenges and solutions for V2X communications: A survey. *Computer Networks, 151*, 52-67.

Anderson, J. M., Nidhi, K., Stanley, K. D., Sorensen, P., Samaras, C., & Oluwatola, O. A. (2014). Autonomous vehicle technology: A guide for policymakers. Rand Corporation.

Angermeier, D., Beilke, K., Hansch, G., & Eichler, J. (2019). Modeling security risk assessments.

Avizienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing, 1*(1), 11-33.

Baheti, R., & Gill, H. (2011). Cyber-physical systems. *The impact of control technology, 12*(1), 161-166.

Bayless, S., Guan, A., Paruch, J., Carter, J., Schaffnit, T., Shaw, A., & America, I. T. S. (2016). *The impact of a vehicle-to-vehicle communications rulemaking on growth in the dsrc automotive aftermarket a market adoption model and forecast for dedicated short range communications (dsrc) for light and heavy vehicle categories* (No. FHWA-JPO-17-487). United States. Department of Transportation. Intelligent Transportation Systems Joint Program Office.

Bishop, R. (2000). A survey of intelligent vehicle applications worldwide. In Intelligent Vehicles Symposium, 2000. IV 2000. *Proceedings of the IEEE* (pp. 25-30). IEEE.

Bolovinou, A., Atmaca, U. I., Sheik, A. T., Ur-Rehman, O., Wallraf, G., & Amditis, A. (2019, June). TARA+: Controllability-aware Threat Analysis and Risk Assessment for L3 Automated Driving Systems. In *2019 IEEE Intelligent Vehicles Symposium (IV)* (pp. 8-13). IEEE.

Bradley, J. M., & Atkins, E. M. (2015). Optimization and control of cyber-physical vehicle systems. *Sensors, 15*(9), 23020-23049.

Burton, S., Likkei, J., Vembar, P., & Wolf, M. (2012). Automotive functional safety= safety+ security. In *Proceedings of the First International Conference on Security of Internet of Things* (pp. 150-159).

Casey, T. (2007). Threat agent library helps identify information security risks. *Intel White Paper, 2*.

Cavelty, M. D. (2015). Cyber-security. In *The routledge handbook of new security studies* (pp. 154-162). Routledge.

Charette, R. N. (2009). This car runs on code. *IEEE spectrum, 46*(3), 3.

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., ... & Kohno, T. (2011, August). Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *USENIX Security Symposium* (Vol. 4, pp. 447-462).

Chemweno, P., Pintelon, L., Muchiri, P. N., & Van Horenbeek, A. (2018). Risk assessment methodologies in maintenance decision making: A review of dependability modelling approaches. *Reliability Engineering & System Safety, 173*, 64-77.

Costigan, S. S., & Hennessy, M. (2016). *Cybersecurity: A Generic Reference Curriculum*. 6 October 2016.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10).

Czerny, B. J. (2013). System security and system safety engineering: Differences and similarities and a system security engineering process based on the ISO 26262 process framework. *SAE International Journal of Passenger Cars-Electronic and Electrical Systems, 6*(2013-01-1419), 349-359.

Ding, D., Han, Q. L., Ge, X., & Wang, J. (2020). Secure state estimation and control of cyber-physical systems: A survey. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51*(1), 176-190.

Doms, T., Rauch, B., Schrammel, B., Schwald, C., Spahovic, E., & Schwarzl, C. (2018). Highly Automated Driving-The new challenges for Functional Safety and Cyber Security. *TÜV Austria Holding AG and VIRTUAL VEHICLE, Vienna, Austria, Tech. Rep*.

Dong, W. (2011, September). An overview of in-vehicle route guidance system. In *Australasian Transport Research Forum* (Vol. 2011).

Duan, W., Gu, J., Wen, M., Zhang, G., Ji, Y., & Mumtaz, S. (2020). Emerging technologies for 5G-IoV networks: applications, trends and opportunities. *IEEE Network, 34*(5), 283-289.

E-safety Vehicle Intrusion proTected Applications (EVITA) Project (2008). Retrieved 26.10.2020 from https://www.evita-project.org/

Ebert, C. (2017). Risk-Oriented Security Engineering. *Automotive-Safety & Security 2017-Sicherheit und Zuverlässigkeit für automobile Informationstechnik.*

Elagin, V., Spirkina, A., Buinevich, M., & Vladyko, A. (2020). Technological aspects of blockchain application for vehicle-to-network. *Information, 11*(10), 465.

ETSI (2010). *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis* (Report TS 102 165-1 V4.2.x). European Telecommunications Standards Institute.

Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on internet of things (IoT). *International journal of computer applications, 113*(1), 1-7.

Furqan, H. M., Solaija, M. S. J., Hamamreh, J. M., & Arslan, H. (2019). Intelligent physical layer security approach for V2X communication. *arXiv preprint arXiv:1905.05075*.

Ghosal, A., & Conti, M. (2020). Security issues and challenges in V2X: A survey. *Computer Networks, 169*, 107093.

Glas, B., Gebauer, C., Hänger, J., Heyl, A., Klarmann, J., Kriso, S., ... & Wörz, P. (2015). Automotive safety and security integration challenges. *Automotive-Safety & Security 2014*.

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS quarterly*, 337-355.

Guo, C., Sentouh, C., Popieul, J. C., Haué, J. B., Langlois, S., Loeillet, J. J., ... & That, T. N. (2019). Cooperation between driver and automated driving

system: Implementation and evaluation. *Transportation research part F: traffic psychology and behaviour, 61*, 314-325.

Gurumurthy, K. M., Kockelman, K. M., & Loeb, B. J. (2019). Sharing vehicles and sharing rides in real-time: Opportunities for self-driving fleets. In *Advances in Transport Policy and Planning* (Vol. 4, pp. 59-85). Academic Press.

Han, K., Weimerskirch, A., & Shin, K. G. (2014). Automotive cybersecurity for in-vehicle communication. In IQT QUARTERLY (Vol. 6, No. 1, pp. 22-25).

Harding, J., Powell, G., R., Yoon, R., Fikentscher, J., Doyle, C., Sade, D., Lukuc, M., Simons, J., & Wang, J. (2014, August). *Vehicle-to-vehicle communications: Readiness of V2V technology for application*. (Report No. DOT HS 812 014). Washington, DC: National Highway Traffic Safety Administration.

Hars, A. (2016). Top misconceptions of autonomous cars and self-driving vehicles. *Thinking outside the box: Inventivio Innovation Briefs*, Issue 2016-09 (Version 1.3). Nuernberg.

Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer networks, 148*, 283-294.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. MisQuarterly. *MISQ Discovery, 28*(1).

Islam, M. M., Lautenbach, A., Sandberg, C., & Olovsson, T. (2016, May). A risk assessment framework for automotive embedded systems. In *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security* (pp. 3-14).

ISO, I. (2021). International Organization for Standardization: ISO STANDARDS ARE INTERNATIONALLY AGREED BY EXPERTS. Retrieved 29.5.2021 from https://www.iso.org/standards.html

ISO, I. (2018). 26262: Road vehicles-Functional safety. *International Standard ISO/FDIS*, 26262.

ISO/SAE, (2020). 21434: Road vehicles-Cybersecurity engineering. *International Standard ISO/Society for automotive engineers SAE*.

Ivanov, I., Maple, C., Watson, T., & Lee, S. (2018). Cyber security standards and issues in V2X communications for Internet of Vehicles. *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, Proceedings of the IEEE, London, pp. 1-6.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973-993.

Ji, B., Zhang, X., Mumtaz, S., Han, C., Li, C., Wen, H., & Wang, D. (2020). Survey on the internet of vehicles: Network architectures and applications. *IEEE Communications Standards Magazine, 4*(1), 34-41.

Jonsson, E. (2006, April). Towards an integrated conceptual model of security and dependability. In *First International Conference on Availability, Reliability and Security (ARES'06)* (pp. 8-pp). IEEE.

kamal Kaur, R., Pandey, B., & Singh, L. K. (2018). Dependability analysis of safety critical systems: Issues and challenges. *Annals of Nuclear Energy, 120*, 127-154.

Karahasanovic, A., Kleberger, P., & Almgren, M. (2017, November). Adapting threat modeling methods for the automotive industry. In *Proceedings of the 15th ESCAR Conference* (pp. 1-10).

Keskin, U. (2009). In-vehicle communication networks: a literature survey. Computer Science Reports; Vol. 0910). Eindhoven: Technische Universiteit Eindhoven.

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., ... & Savage, S. (2010). Experimental security analysis of a modern automobile. In *2010 IEEE Symposium on Security and Privacy* (pp. 447-462). IEEE.

Krasniqi, X., & Hajrizi, E. (2016). Use of IoT technology to drive the automotive industry from connected to full autonomous vehicles. *IFAC-PapersOnLine, 49*(29), 269-274.

Kyriakidis, M., Happee, R., & de Winter, J. C. (2015). Public opinion on automated driving: Results of an international questionnaire among 5000 respondents. *Transportation research part F: traffic psychology and behaviour,* 32, 127-140.

Lautenbach, A., & Islam, M. (2016). HEAVENS–HEAling Vulnerabilities to ENhance Software Security and Safety. *The HEAVENS Consortium (Borås SE)*.

Lehto, M., & Neittaanmäki, P. (Eds.). (2015). *Cyber security: Analytics, technology and automation* (Vol. 78, p. 258). London: Springer.

Litman, T. (2017). *Autonomous vehicle implementation predictions* (p. 28). Victoria, Canada: Victoria Transport Policy Institute.

Liu, C., Chau, K. T., Wu, D., & Gao, S. (2013). Opportunities and challenges of vehicle-to-home, vehicle-to-vehicle, and vehicle-to-grid technologies. *Proceedings of the IEEE, 101*(11), 2409-2427.

Lu, M., Wevers, K., & Van Der Heijden, R. (2005). Technical feasibility of advanced driver assistance systems (ADAS) for road traffic safety. *Transportation Planning and Technology, 28*(3), 167-187.

Lu, R., Zhang, L., Ni, J., & Fang, Y. (2019). 5G vehicle-to-everything services: Gearing up for security and privacy. *Proceedings of the IEEE, 108*(2), 373-389.

Lv, C., Xing, Y., Zhang, J., & Cao, D. (2020). Cyber-Physical Vehicle Systems: Methodology and Applications. *Synthesis Lectures on Advances in Automotive Technologies, 4*(1), 1-85.

Macher, G., Armengaud, E., Brenner, E., & Kreiner, C. (2016a, September). A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context. In *International Conference on Computer Safety, Reliability, and Security* (pp. 130-141). Springer International Publishing.

Macher, G., Armengaud, E., Brenner, E., & Kreiner, C. (2016b). Threat and risk assessment methodologies in the automotive domain. *Procedia computer science, 83*, 1288-1294.

Macher, G., Armengaud, E., Kreiner, C., Brenner, E., Schmittner, C., Ma, Z., ... & Krammer, M. (2021). Integration of security in the development lifecycle of dependable automotive CPS. In *Research anthology on artificial intelligence applications in security* (pp. 101-142). IGI Global.

Macher, G., Sporer, H., Berlach, R., Armengaud, E., & Kreiner, C. (2015, March). SAHARA: a security-aware hazard and risk analysis method. In *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)* (pp. 621-624). IEEE.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision support systems, 15*(4), 251-266.

Marojevic, V. (2018). C-V2X security requirements and procedures: Survey and research directions. *arXiv preprint arXiv:1807.09338*.

Martin, H., & Winkler, B. (2018). Introduction to Functional Safety according to ISO 26262. In *Functional Safety Introduction Workshop*. Virtual Vehicle.

Matsumoto, S., Mikami, T., Yumoto, N., & Tabe, T. (1979). Comprehensive automobile traffic control system. *J. of IECE, 62*(8), 870-887.

Microsoft Corporation (2022, 25. August). Microsoft Threat Modeling Tool. Retrieved 23.4.2023 from https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool

Microsoft Corporation. (2005). The STRIDE Threat Model.

Monteuuis, J. P., Boudguiga, A., Zhang, J., Labiod, H., Servel, A., & Urien, P. (2018, May). Sara: Security automotive risk analysis method. In *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security* (pp. 3-14).

Nahri, M., Boulmakoul, A., Karim, L., & Lbath, A. (2018). IoV distributed architecture for real-time traffic data analytics. *Procedia computer science, 130*, 480-487.

Nora, S., & Minc, A. (1980). L'Informatisation de la société. Rapport à M. le Président de la République. La Documentation Française, Paris, 1978. English version: The Computerization of Society. A report to the President of France.

Onishi, H., Wu, K., Yoshida, K., & Kato, T. (2017). Approaches for vehicle cyber-security in the US. *International Journal of Automotive Engineering, 8*(1), 1-6.

Pa, Y. M. P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T., & Rossow, C. (2015). {IoTPOT}: Analysing the Rise of {IoT} Compromises. In *9th USENIX Workshop on Offensive Technologies (WOOT 15)*.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems, 24*(3), 45-77.

Pratticò, F. G., Lamberti, F., Cannavò, A., Morra, L., & Montuschi, P. (2021). Comparing state-of-the-art and emerging augmented reality interfaces for autonomous vehicle-to-pedestrian communication. *IEEE Transactions on Vehicular Technology, 70*(2), 1157-1168.

Rahim, M. A., Rahman, M. A., Rahman, M. M., Asyhari, A. T., Bhuiyan, M. Z. A., & Ramasamy, D. (2021). Evolution of IoT-enabled connectivity and applications in automotive industry: A review. *Vehicular Communications, 27*, 100285.

Rangarajan, S., Verma, M., Kannan, A., Sharma, A., & Schoen, I. (2012, August). V2c: a secure vehicle to cloud framework for virtualized and on-demand service provisioning. In *Proceedings of the International Conference on Advances in Computing, Communications and Informatics* (pp. 148-154).

RGBSI (2020). *Driving Change: The Future of Mobility* (Whitepaper). Rapid Global Business Solutions, Engineering Solutions.

Rosenquist, M. (2009). Prioritizing information security risks with threat agent risk assessment. *Intel Corporation White Paper*.

Ruddle, A., Ward, D., Weyl, B., Idrees, S., Roudier, Y., Friedewald, M., ... & Wolf, M. (2009). Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios. *EVITA project*.

Sadiku, M. N., Tembely, M., & Musa, S. M. (2018). Internet of vehicles: An introduction. *International Journal of Advanced Research in Computer Science and Software Engineering, 8*(1), 11.

SAE. (2016a). J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. *Society for automotive engineers*.

SAE. (2016b). J3061: Cybersecurity guidebook for cyber-physical vehicle systems. *Society for automotive engineers*.

SAE. (2016c). J3061-1: Automotive Cybersecurity Integrity Level (ACsIL). *Society for automotive engineers*.

Sapiro, B. (2011) Binary Risk Analysis. *Creative Commons License, 1*.

Scandariato, R., Wuyts, K., & Joosen, W. (2015). A descriptive study of Microsoft's threat modeling technique. *Requirements Engineering, 20*(2), 163-180.

Schmidt, K., Tröger, P., Kroll, H. M., Bünger, T., Krueger, F., & Neuhaus, C. (2014). Adapted development process for security in networked automotive systems. *SAE International Journal of Passenger Cars-Electronic and Electrical Systems, 7*(2014-01-0334), 516-526.

Schmittner, C., Griessnig, G., & Ma, Z. (2018, September). Status of the Development of ISO/SAE 21434. In *European Conference on Software Process Improvement* (pp. 504-513). Springer, Cham.

Schoitsch, E., Schmittner, C., Ma, Z., & Gruber, T. (2016). The need for safety and cyber-security co-engineering and standardization for highly automated automotive vehicles. In *Advanced Microsystems for Automotive Applications 2015* (pp. 251-261). Springer, Cham.

Sedar, R., Kalalas, C., Vázquez-Gallego, F., Alonso, L., & Alonso-Zarate, J. (2023). A Comprehensive Survey of V2X Cybersecurity Mechanisms and Future Research Paths. *IEEE Open Journal of the Communications Society*.

Sewalkar, P., & Seitz, J. (2019). Vehicle-to-pedestrian communication for vulnerable road users: Survey, design considerations, and challenges. *Sensors, 19*(2), 358.

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security, 124*, 102974.

Sharma, V., You, I., & Guizani, N. (2020). Security of 5G-V2X: Technologies, standardization, and research directions. *IEEE Network, 34*(5), 306-314.

Shen, X., Fantacci, R., & Chen, S. (2020). Internet of vehicles [scanning the issue]. *Proceedings of the IEEE, 108*(2), 242-245.

Simon, H. A. (1996). The sciences of the artificial. MIT Press. *Cambridge, MA*.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. Oxford University Press.

Smith, C. (2016). *The Car Hacker's Handbook: A Guide for the Penetration Tester*. No Starch Press.

Smith, D. J., & Simpson, K. G. (2010). *Safety critical systems handbook: a straight forward guide to functional safety, IEC 61508 (2010 Edition) and related standards, including process IEC 61511 and machinery IEC 62061 and ISO 13849*. Elsevier.

Sommerville, I. (2016). Software Engineering 10th Edition (International Computer Science). *Essex, UK: Pearson Education*, 1-808.

SysML.org (2023). SysML Open Source Project: What is SysML? Who created SysML? Retrieved 23.4.2023 from https://sysml.org/

Tan, K. M., Ramachandaramurthy, V. K., & Yong, J. Y. (2016). Integration of electric vehicles in smart grid: A review on vehicle to grid technologies and optimization techniques. *Renewable and Sustainable Energy Reviews, 53*, 720-732.

Teague, C. (2021, 3. May). Autoweek: Everything You Need to Know about V2X Technology. Vehicle-to-everything tech is coming—here's what it will entail. Retrieved 8.3.2023 from https://www.autoweek.com/news/technology/a36190311/v2x-technology/

UcedaVelez, T., & Morana, M. M. (2015). *Risk Centric Threat Modeling: process for attack simulation and threat analysis*. John Wiley & Sons.

Uden, L., & He, W. (2017). How the Internet of Things can help knowledge management: a case study from the automotive domain. *Journal of Knowledge Management*.

UNECE (2021a). UN Regulation No. 155 - Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. *UNECE Regulation*, (155).

UNECE (2021b). WP.29 - Introduction. Retrieved 12.6.2021 from https://unece.org/wp29-introduction

UNECE (2021c). Mission. Retrieved 12.6.2021 from https://unece.org/mission

Vaishnavi, V., Kuechler, W., & Petter, S. (2004/2019). Design science research in information systems. *January, 20*, 2004.

Villarreal-Vasquez, M., Bhargava, B., & Angin, P. (2017, June). Adaptable safety and security in V2X systems. In *2017 IEEE International Congress on Internet of Things (ICIOT)* (pp. 17-24). IEEE.

Virtual Vehicle (2020a, 21. January). Meet the SPIDER – a mobile platform for fast, flexible reproducible ADAS or sensor tests. Retrieved 11.2.2020 from https://www.v2c2.at/spider-mobileplatform-en/

Virtual Vehicle (2020b). *Item Definition - "SPIDER"*. (Project: SPIDER, Version: V1.0). Virtual Vehicle, 1.7.2020.

Virtual Vehicle (2021a). WORLDWIDE PARTNER NETWORK. Retrieved 24.5.2021 from https://www.v2c2.at/cooperation/partnernetwork/

Virtual Vehicle (2021b). ABOUT US. Retrieved 24.5.2021 from https://www.v2c2.at/about/

Virtual Vehicle (2021c). SPIDER. Retrieved 30.5.2021 from https://www.v2c2.at/spider/

vom Brocke, J., Hevner, A., & Maedche, A. (2020). Introduction to design science research. *Design science research. Cases*, 1-13.

Vom Brocke, J., & Maedche, A. (2019). The DSR grid: six core dimensions for effectively planning and communicating design science research projects. *Electronic Markets, 29*, 379-385.

Wang, J., Shao, Y., Ge, Y., & Yu, R. (2019). A survey of vehicle to everything (V2X) testing. *Sensors, 19*(2), 334.

Weimerskirch, A., & Gaynier, R. (2015). An Overview of Automotive Cybersecurity: Challenges and Solution Approaches. In *TrustED@ CCS* (p. 53).

Wen, H., Chen, Q. A., & Lin, Z. (2020). {Plug-N-Pwned}: Comprehensive Vulnerability Analysis of {OBD-II} Dongles as A New {Over-the-Air} Attack Surface in Automotive {IoT}. In *29th USENIX Security Symposium (USENIX Security 20)* (pp. 949-965).

Wolf, M., Weimerskirch, A., & Paar, C. (2006). Secure in-vehicle communication. In *Embedded Security in Cars* (pp. 95-109). Springer, Berlin, Heidelberg.

Wolf, M., Weimerskirch, A., & Wollinger, T. (2007). State of the art: Embedding security in vehicles. EURASIP Journal on Embedded Systems, 2007(1), 074706.

Wortmann, F., & Flüchter, K. (2015). Internet of things. *Business & Information Systems Engineering, 57*(3), 221-224.

Wynn, J., Whitmore, J., Upton, G., Spriggs, L., McKinnon, D., McInnes, R., ... & Clausen, L. (2011). *Threat assessment & remediation analysis (tara): Methodology description version 1.0* (No. MTR110176). MITRE CORP BEDFORD MA.

Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and microsystems, 77*, 103201.

Zhao, Y. (2002). Telematics: safe and fun driving. *IEEE Intelligent systems, 17*(1), 10-14.

Zhou, H., Xu, W., Chen, J., & Wang, W. (2020). Evolutionary V2X technologies toward the Internet of vehicles: Challenges and opportunities. *Proceedings of the IEEE, 108*(2), 308-323.

APPENDIX 1 SECURITY RISK ANALYSIS COMPARISON MATRIX

Coverage metrics:
Fully covered 67-100%
Partly covered 34-66%
Not covered 0-33%

ISO/SAE JWG 21434 requirements	EVITA (+THROP)	HEAVENS (+STRIDE)	SAHARA (HARA+STRIDE +DREAD)	BRA	TARA Intel	SARA (+STRIDE(LC))	TARA+ (TARA+SARA +STRIDE(LC) +HEAVENS)
	COVERAGE	COVERAGE	COVERAGE	COVERAGE	COVERAGE	COVERAGE	COVERAGE
8.3 Asset Identification							
[RQ-08-01] Damage scenarios shall be identified.	Fully covered with THROP	Fully covered with STRIDE	Partly covered	Partly covered	Fully covered	Fully covered with STRIDE(LC)	Fully covered with SARA (Fully covered with STRIDE(LC))
[RQ-08-02] Assets with cybersecurity properties whose compromise leads to a damage scenario shall be enumerated.	Fully covered with THROP	Fully covered	Partly covered	Partly covered	Fully covered	Fully covered	Fully covered with SARA
8.4 Threat Scenario Identification							
[RQ-08-03] Threat scenarios shall be identified.	Fully covered	Fully covered	Partly covered	Not covered	Partly covered	Fully covered	Fully covered with SARA

ISO/SAE JWG 21434 requirements	EVITA (+THROP)	HEAVENS (+STRIDE)	SAHARA (HARA+STRIDE +DREAD)	BRA	TARA Intel	SARA (+STRIDE(LC))	TARA+ (TARA+SARA +STRIDE(LC) +HEAVENS)
	COVERAGE	COVERAGE	COVERAGE	COVERAGE	COVERAGE	COVERAGE	COVERAGE
8.5 Impact Rating							
[RQ-08-04] The damage scenarios shall be assessed against potential adverse consequences for stakeholders in the independent impact categories of safety, financial, operational, and privacy (S, F, O, P).	Fully covered with THROP	Fully covered	Partly covered	Not covered	Not covered	Fully covered	Fully covered with HEAVENS and SARA
[RQ-08-05] If further impact categories are considered beyond S, F, O and P, then those categories shall be documented.	Not covered	Fully covered	Not covered	Not covered	Not covered	Fully covered	Fully covered with TARA+, HEAVENS and SARA
[RQ-08-06] The impact rating of the damage scenario shall be determined to be one of the following:	Fully covered	Fully covered	Partly covered	Not covered	Not covered	Fully covered	Fully covered with HEAVENS and SARA
Safety Impact Rating - **Severe** S3: Life-threatening injuries (survival uncertain), fatal injuries - **Major** S2: Severe and life-threatening injuries (survival probable) - **Moderate** S1: Light and moderate injuries - **Negligible** S0: No injuries	Fully covered	Fully covered	Fully covered	Not covered	Not covered	Fully covered	Fully covered with HEAVENS and SARA
Financial Impact Rating - **Severe** The financial damage leads to catastrophic consequences which the affected stakeholder might not overcome. - **Major** The financial damage leads to substantial consequences which the affected stakeholder will be able to overcome. - **Moderate** The financial damage leads to inconvenient consequences which the affected stakeholder will be able to overcome with limited resources. - **Negligible** The financial damage leads to no effect, negligible consequences or is irrelevant to the stakeholder.	Fully covered	Fully covered	Not covered	Not covered	Not covered	Fully covered	Fully covered with HEAVENS and SARA
Operational Impact Rating - **Severe** The operational damage leads to a vehicle not working, from non-intended operation up to the vehicle being non-operational. - **Major** The operational damage leads to the loss of a vehicle function. - **Moderate** The operational damage leads to partial degradation of a vehicle function or performance. - **Negligible** The operational damage leads to no effect or indiscernible degradation of a vehicle function or performance.	Fully covered	Fully covered	Not covered	Not covered	Not covered	Fully covered	Fully covered with HEAVENS and SARA
Privacy Impact Rating - **Severe** The privacy damage leads to significant or even irreversible impact to the road user. In this case, the information regarding the road user is highly sensitive and easy to link to a PII (Personally identifiable information) principal. - **Major** The privacy damage leads to serious impact to the road user. In this case, the information regarding the road user is: a) highly sensitive and difficult to link to a PII principal, or b) sensitive and easy to link to a PII principal. - **Moderate** The privacy damage leads to significant inconveniences to the road user. In this case, 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** The privacy damage leads to no effect or can create few inconveniencies to the road user. In this case, the information regarding the road user is not sensitive and difficult to link to a PII principal.	Fully covered	Fully covered	Not covered	Not covered	Not covered	Fully covered	Fully covered with HEAVENS and SARA
[RQ-08-07] Safety related impacts shall be derived from ISO 26262-3:2018, 6.4.3 Classification of hazardous events.	Fully covered	Fully covered	Fully covered	Not covered	Not covered	Fully covered	Fully covered with HEAVENS and SARA

ISO/SAE JWG 21434 requirements	EVITA (+THROP)	HEAVENS (+STRIDE)	SAHARA (HARA+STRIDE +DREAD)	BRA	TARA Intel	SARA (+STRIDE(LC))	TARA+ (TARA+SARA +STRIDE(LC) +HEAVENS)
	COVERAGE	COVERAGE	COVERAGE	COVERAGE	COVERAGE	COVERAGE	COVERAGE
8.6 Attack Path Analysis							
[RQ-08-08] The threat scenarios shall be analyzed to describe possible attack paths.	Fully covered	Partly covered with STRIDE	Partly covered	Not covered	Not covered	Fully covered	Fully covered with SARA
[RQ-08-09] The attack path analysis approach applied shall be documented.	Fully covered	Partly covered with STRIDE	Partly covered	Not covered	Not covered	Fully covered	Fully covered with SARA
[RC-08-01] The attack path description should include a reference to the threat scenarios that can be realized by the attack path.	Not covered	Partly covered with STRIDE	Partly covered	Not covered	Not covered	Fully covered	Fully covered with SARA
8.7 Attack Feasibility Rating							
[RQ-08-10] For each attack path the attack feasibility rating shall be determined as one of the following: - **high** Highly feasible utilizing minimal effort: It is easy or almost certain to accomplish the attack path. - **medium** Quite feasible utilizing moderate effort: It is feasible and not unusual to accomplish the attack path. - **low** Conceivably feasible utilizing significant effort: It is feasible to accomplish the attack path. - **very low** Mostly infeasible utilizing reasonable effort: It is difficult or almost never possible to accomplish the attack path.	Fully covered	Not covered	Not covered	Not covered	Not covered	Fully covered	Fully covered with SARA
[RC-08-02] The defined rating method should be based on one of the following assessment approaches: a) attack potential-based approach; b) CVSS based approach; or c) attack vector-based approach.	Fully covered	Fully covered	Partly covered	Not covered	Not covered	Fully covered	Fully covered with SARA and TARA+
[RC-08-03] If an attack potential-based approach is used, it should be determined based on core factors including elapsed time, specialist expertise, knowledge of the item or component, window of opportunity, and equipment.	Fully covered	Fully covered	Not covered	Not covered	Not covered	Fully covered	Fully covered with SARA and TARA+
[RC-08-04] If a CVSS based approach is used, it should be determined based on the exploit metrics group of the base metrics, including attack vector, attack complexity, privileges required, and user interaction.	Not covered	Not covered	Not covered	Not covered	Not covered	Not covered	Not covered
[RC-08-04] If a CVSS based approach is used, it should be determined based on the exploit metrics group of the base metrics, including attack vector, attack complexity, privileges required, and user interaction.	Not covered	Not covered	Not covered	Not covered	Not covered	Not covered	Not covered
[RC-08-05] If an attack vector based approach is used, it should evaluate the predominant attack vector (cf. CVSS) of the attack path.	Not covered	Not covered	Partly covered	Not covered	Not covered	Not covered	Not covered
8.8 Risk Determination							
[RQ-08-11] The risk value of a threat scenario shall be determined from the impact of the associated damage scenario and the attack feasibility of the associated attack paths.	Fully covered	Partly covered	Partly covered	Not covered	Not covered	Fully covered	Fully covered with SARA

Coverage metrics:
Fully covered 67-100%
Partly covered 34-66%
Not covered 0-33%

APPENDIX 2 SECURITY RISK ANALYSIS FOR SPIDER USE CASE

From **3.4.1 Use Case Creation**

The need with the use case was to apply cybersecurity in a vehicle level with two different threat scenarios: communication in application level with Operator Panel, and communication in transport/network level with WiFi AP. Two cyberattack scenarios (CAS) were distinguished: CAS1 and CAS2.

The description of the Cyberattack Scenario 1 is: *The hacker could have stolen the laptop/tablet and acquired the employee ID (username and password)*. In this scenario the human attacker has committed a company theft and stolen both the equipment and login credentials from an Operating Engineer.

The description of the Cyberattack Scenario 2 is: *The hacker uses remote equipment (laptop/tablet)*. In the second scenario the human attacker is using his/her own equipment to gain access to the SPIDER HLC. The attacker has been able to make a breach into the company's systems and has primary and secondary targets to cause damage of any kind.

A0 Item Definition

CAS1 = AS_01
CAS2 = AS_02

Add the use case(s) into this sheet below/next to the Item Definition table for documentation.

Component	Function	Input Interface (signal)	Output Interface	Asset ID	Asset
Operator Panel	**Vehicle Control & Monitoring**	**HMI (Operator Parameters)**	**WiFi channel (Control commands)**	**AS_01**	**Laptop/ Tablet**
	Path Generation & Tracking	**HMI (Intended path of the vehicle)**	**WiFi channel (Trajectory)**		
WiFi AP	**Receive and transmit WiFi communication**	**WiFi channel to the Operator Panel (control commands; trajectory)**	**Ethernet connection to HLC (control commands; trajectory)**	**AS_02**	**WiFi AP**
*HLC **	*To process the control signals for SPIDER movement to actuate commands*	*Ethernet connection from the WiFi AP (control commands; trajectory)*	*Low Level Controller (SPIDER motion commands)*	*AS_03*	*HLC*

* HLC is an example but the focus will be in the first two components focusing on remote communication.

A1 Assets

A1 Assets					
				Damage Scenarios	
Asset ID	Asset category	Asset	Comments	Category	Description / Rational
AS_01	External Entity	Laptop/Tablet	Laptop/Tablet used to provide access to an Operating Engineer to use the SPIDER Vehicle Control & Monitoring.		
				Spoofing	Impersonating an Operating Engineer.
				Tampering	Not applicaple as data remains unmodified.
				Repudiation	The violating actions cannot be traced back.
				Information Disclosure	When using SPIDER for customer testing, company confidential information gets jeopardized.
				Denial of Service	*Not applicaple by using the standard equipment.*

A2 Threat Scenarios

A2 Threat Scenarios		
Attack classes	**Threat Scenario ID**	**Threat Scenario description**
Impersonate	TS_01	Action: Pretending to have a role of an Operating Engineer.
Alter		
Dispute	TS_02	Action: Executing commands/requests by using the stolen Operating Engineer ID.
Listen	TS_03_01	Action 1: Access sensitive and confidential information.
	TS_03_02	Action 2: Download and publish sensitive and confidential data.
Disable		

A3 Impact

A3 Impact									
FIRST ITERATION									
Impact category									
Severity for Safety (Ss)	Justification	Severity for Financial (Sf)	Justification	Severity for Operational (So)	Justification	Severity for Privacy (Sp)	Justification	Impact Value (IV)	Impact Factor (IF)
1	**Justification**: SPIDER could run in unauthorized path or pedestrian area causing light injuries.	0	**Justification**: No damage to the SPIDER.	1	**Justification**: Partial degradation of the path planning function.	0	**Justification**: Privacy does not get affected in this damage category.	5	**1**
3	**Justification**: High speed could cause malfunction in steering and cause severe injuries.	1	**Justification**: Damage of the SPIDER is minimal as it is a prototype.	2	**Justification**: Loosing the control of the speed control function.	0	**Justification**: Privacy does not get affected in this damage category.	14	**3**
3	**Justification**: It is enough to have the role of the OE to possess a threat to safety by causing an accident with the SPIDER. The hacker has entered the system with the role and gives commands which can cause safety issues.	1	**Justification**: Damage of the SPIDER is minimal as it is a prototype.	3	**Justification**: The role grants the Operator to stop the SPIDER. All possible funtionalities are enabled for the Operator.	0	**Justification**: Privacy does not get affected in this damage category.	16	**3**

A4 Attack Path

A4 Attack Path	
Attack Path ID	**Attack Path Description**
AP_09 (Disable)	1. Attacker has his/her own equipment (laptop/tablet). 2. Attacker is using his/her equipment to get privileged access to the remote communication. 3. Attacker is blocking the remote communication. 4. Remote communication to WiFi AP. 5. WiFi AP to SPIDER HLC. 6. SPIDER HLC does not receive data.
AP_10 (Violate (authority))	1. Attacker has his/her own equipment (laptop/tablet). 2. Attacker is using his/her equipment to get privileged access to the remote communication. 3. Attacker changes the parameters of the SPIDER via the remote communication. 4. Remote communication to WiFi AP. 5. WiFi AP to SPIDER HLC. 6. SPIDER HLC is changing the range of collision avoidance from 2 meters to 1 meter.
AP_11 (Forge)	1. Attacker has his/her own equipment (laptop/tablet). 2. Attacker is using his/her equipment to get privileged access to the remote communication. 3. Attacker changes the parameters of the SPIDER via the remote communication. 4. Remote communication to WiFi AP. 5. WiFi AP to SPIDER HLC. 6. SPIDER HLC is changing the range of collision avoidance from 2 meters to -1 meter.

A5 Attack Feasibility

A5 Attack Feasibility											
Expertise	Justification	Knowledge	Justification	Equipment	Justification	Opportunity	Justification	Elapsed time	Justification	Attack Potential (APo)	Attack Probability (AP)
2	**Justification**: Expert Able to perform a remote attack to attain a company ID.	1	**Justification**: Restricted information Special expertise is required. One needs to be familiar with the HW, SW, how to use Operator Panel to control SPIDER.	1	**Justification**: Specialized A special equipped laptop/tablet. Acquiring a company UI can be gained with simple attacking scripts.	1	**Justification**: Easy Remote access without physical presence.	1	**Justification**: Less than 1 month	6	2
2	**Justification**: Expert Able to modify commands.	2	**Justification**: Confidential information Special expertise is required. One needs to be familiar with the HW, SW, how to use Operator Panel to control SPIDER.	1	**Justification**: Specialized A special equipped laptop/tablet. Acquiring a company UI can be gained with simple attacking scripts.	1	**Justification**: Easy Remote access without physical presence.	1	**Justification**: Less than 1 month	7	2
2	**Justification**: Expert Able to modify commands.	2	**Justification**: Confidential information Special expertise is required. One needs to be familiar with the HW, SW, how to use Operator Panel to control SPIDER.	1	**Justification**: Specialized A special equipped laptop/tablet. Acquiring a company UI can be gained with simple attacking scripts.	1	**Justification**: Easy Remote access without physical presence.	1	**Justification**: Less than 1 month	7	2
2	**Justification**: Expert Able to modify commands.	2	**Justification**: Confidential information Special expertise is required. One needs to be familiar with the HW, SW, how to use Operator Panel to control SPIDER.	1	**Justification**: Specialized A special equipped laptop/tablet. Acquiring a company UI can be gained with simple attacking scripts.	1	**Justification**: Easy Remote access without physical presence.	1	**Justification**: Less than 1 month	7	2

A6 Risk Determination

A6 Risk Determination
Risk Value
Medium = 3
Low = 2
Medium = 3
Medium = 3
Low = 2
Low = 2
Medium = 3
Medium = 3
QM = 1
Medium = 3

A7 Risk Treatment

A7 Risk Treatment					
The target value of the cybersecurity risk is set in the project to level:					
Low = 2					
Risk Treatment ID	Risk Treatment Option				
		Rational for option A	Rational for option B	Rational for option C	Rational for option D
RT_04	[ ] a) avoiding the risk; **[X] b) reducing the risk;** [ ] c) sharing the risk; [ ] d) retaining the risk.		b) reducing the risk: Having specific security measures for reducing spoofing attacks.		
RT_02	[ ] a) avoiding the risk; [ ] b) reducing the risk; [ ] c) sharing the risk; **[X] d) retaining the risk.**				d) retaining the risk: No risk treatment needed.
RT_05	[ ] a) avoiding the risk; **[X] b) reducing the risk;** [ ] c) sharing the risk; [ ] d) retaining the risk.		b) reducing the risk: Having specific security control against tampering attacks.		
RT_06	[ ] a) avoiding the risk; **[X] b) reducing the risk;** [ ] c) sharing the risk; [ ] d) retaining the risk.		b) reducing the risk: Having specific security control against repudiation attacks.		

APPENDIX 3 VIRTUAL VEHICLE - ACKNOWLEDGEMENT

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 783119. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Netherlands, Austria, Belgium, Czech Republic, Germany, Spain, Finland, France, Hungary, Italy, Poland, Portugal, Romania, Sweden, United Kingdom, Tunisia." In Austria the project was also funded by the program "IKT der Zukunft" of the Austrian Federal Ministry for Climate Action (BMK).

The publication was written at Virtual Vehicle Research GmbH in Graz and partially funded within the COMET K2 Competence Centers for Excellent Technologies from the Austrian Federal Ministry for Climate Action (BMK), the Austrian Federal Ministry for Labour and Economy (BMAW), the Province of Styria (Dept. 12) and the Styrian Business Promotion Agency (SFG). The Austrian Research Promotion Agency (FFG) has been authorised for the programme management.

They would furthermore like to express their thanks to their supporting scientific project partners, namely University of Jyväskylä / Faculty of Information Technology.