An Adaptable Security by Design Approach for Ensuring a Secured Remote Monitoring Teleoperation (RMTO) of an Autonomous Vehicle

Iyieke, V., Bryans, J., Robinson, T., Kosmas, O., Shipman, A. & Jadidbonab, H

DOI 10.4271/2023-01-0579
ISSN 0148-7191
ESSN 2688-3627

Publisher: SAE International

An Adaptable Security by design approach for ensuring a secured Remote Monitoring Teleoperation (RMTO) of an Autonomous Vehicle

Victormills Iyieke, Hesamaldin Jadidbonab and Jeremy Bryans
Coventry University

Abstract

Remote Monitory and Teleoperation (RMTO) of Autonomous Vehicle (AV) is advancing in pace in the industry. Researchers and industrial partners explore the role RMTO plays in helping AV navigate through complicated situations among many others. At the heart of this, lies the problem of potential pathways and attack vectors or threat surfaces by which a malicious attack can be carried out on a RMTO and on an AV itself. The separation of cybersecurity considerations in RMTO is barely considered, as so far the majority of available research and activities mainly focused on AV. The main focus of this paper is addressing RMTO cybersecurity utilising an adaptable security-by-design approach, although security-by-design is still in the infant state within automotive cybersecurity. An adaptable security-by-design approach for RMTO covers Security Engineering Lifecycle, Logical Security Layered Concept, and Security Architecture. Based on the international automotive cybersecurity standards - ISO/SAE 21434, a Threat Analysis and Risk Assessment (TARA) with a formalisation of the highest level of threats identified from the TARA of the RMTO system is carried out, with corresponding mitigation actions as per UNECE WP29. The adaptable security-by-design approach has been then applied to a prototype RMTO system, developed by an industrial partner. Finally, penetration testing has been carried out where the results verify the capability of the adoptable security-by-design to reinforce the security of the RMTO systems against some of the identified risks and threats.

I. Introduction

A. The rise of Autonomous Vehicles.

The advancement of modern vehicles has necessitated the fitting of Advance Driver Assistance Systems (ADAS) which helps to facilitate many features such as: Safety, Product Efficiency, Off Road Capability, Human Factors, Durability and Robustness, All Weather Comfort and Vision state of Art Automated Driving among several others, which enables the move away from driver control of the vehicle. Figure 1 gives an illustration of several feature that are required to achieve automation driving and assistance driving which forms part of the ADAS, including sensors necessitating the vehicles ability to sense the external environment, decide on the intended vehicle path and control the longitudinal and lateral direction.

The society of automotive Engineers (SAE) categorised 6 level of autonomy in the J3016 standard [1] as shown in table 1. The 6 level of autonomy ranges from level 0 with no automation to level 5 the highest level of automation, hence for reference purpose the AV are referred to level 3 and above as per SAE J3016. SAE level 5 autonomous driving

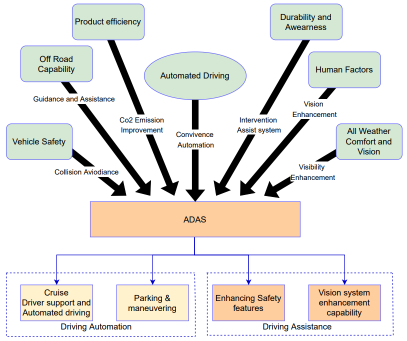


Figure 1: ADAS Illustration

is capable of coping with any imaginable scenario that is not currently feasible and available in use to the public [2], in cases where the automated vehicle is less than level 5, an operator is needed to intervene in certain conditions that surpasses the system's capabilities. Any Level greater than level 3 are feature with several sensors and components such as Lidars, Cameras, Radars, Infrared etc in other to enable autonomous driving in the AV as shown in figure 2, with these sensors or component represented by several colours.

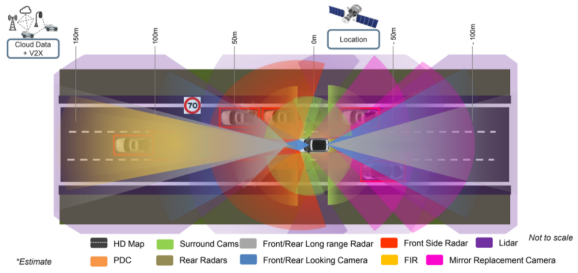


Figure 2: Illustration of Sensors coverage in AV

In the case of operation of a less than level 5 SAE vehicle, the requirement for an on-board operator (Human driver) or RMTO located in a separate location from the AV is required.

B. Remote Monitoring Teleoperation (RMTO).

RMTO or teleoperation represents an approach that enables human to remotely connect to an AV greater than level 3 as defined by SAE J3016, via strong wireless network communication link such as

Table 1: SAE J3016 levels of autonomous vehicle

SAE Level	Automation	Steering Cruise	Environment Monitoring	Fall-back Control	Driving Mode
0	No Automation	Human Driver	Human Driver	Human Driver	N/A
1	Driver Assistance	Human Driver and System	Human Driver	Human Driver	Some Driving Mode
2	Partiial Automation	System	Human Driver	Human Driver	Some Driving Mode
3	Conditional Automation	System	System	Human Driver	Some Driving Mode
4	High Automation	System	System	System	Some Driving Mode
5	Full Automation	System	System	System	All

LTE/4G/5G, which enables the operation of the AV from a distant location [3] different from the AV itself as shown in figure 3.

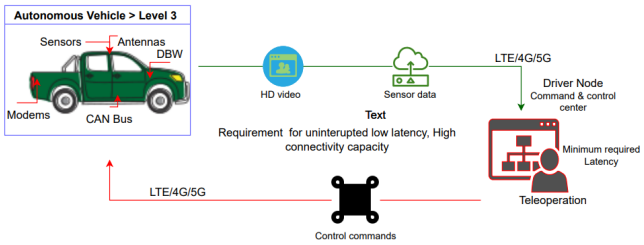


Figure 3: Illustration of RMTO Architecture

The figure 3 gives a high level illustrative architecture for RMTO showing relevant system, components, sensors and interface required for RMTO. Bensoussan [4] in 1997, investigated a teleoperation of road vehicle that was distributed in a car sharing pool in various car park lots. The foundation of this, is based on the concept [5], [6] that teleoperation can only be applied to an AV to assist in certain conditions. This conditions are defined within the Operational Design Domain (ODD) of the Teleoperation, which could be navigation of vehicle in car sharing pool in various car park lots or as Zhang [3] noted these conditions could be requirement for an ODD to be defined as speed ranges, types of roadway, environmental conditions such as weather and visibility, and other limitations. Also noting that this ODD are only applicable or defined in less than level 5 AV, as all level 5 AV are completely able to drive itself regardless of types of the roadway conditions without out human involvement. Though they still require intervention from human safety drivers in the vehicle. Notably in 2019, Waymo replaced some in-car human intervention safety drivers with human teleoperators for its robot taxi trials in Arizona, USA, never the less, it still sees human safety drivers in the cars for the predictable future [7]. The concept of Teleoperation was further subdivided by Lichiardopol [8] into Supervisory control, Coordinate Teleoperation or Indirect control [9] and Directed control, with generic categorization into just indirect teleoperation and direct teleoperation.

C. Cybersecurity in automotive.

The automotive industry is encountering a major transformation necessitated by digital technologies as a result of keeping pace with the sophistication of modern day's vehicles that cater for electrification, intelligence and shared mobility, connectivity and automated/Advance Driver Automation System (ADAS), making way for new concepts and interfaces to be deployed in vehicles. Mobility that used to be limited to the line of sight and habits of the driver is no longer the case or going to be the case as the emergence of automated driving system and digital connectivity have pave the way for information exchange outside of the boundary of the vehicle to the outside world, thereby creating and interlinking the vehicle to other industries such as multimedia, navigation provider, telecommunications and new comers into the industry like Google, Apple and others. According to Juniper Research [10] , by 2023 the availability of new consumer vehicle that will be shipped with connectivity via telematics or in vehicle apps will reach 775 million via the possibility of leveraging localisation services or the Internet adoption of the V2X (Vehicle-to-X) model. This will give way to scalable infrastructures platforms and integrating of (API's) - modern application programming interface, enabling vehicle connectivity such as Vehicle-to-Everything (V2V) capability and autonomous and automated control and driving of the vehicle. This is capable of exposing the vehicle to attack vectors and increased attack surface, thereby creating new cyber risks and threat. No wonder Scalas and Giacinto [11] noted that, the safety of modern vehicles is strictly related to addressing cybersecurity challenges. The vehicle's embedded electronic architecture has been created and standardised as a closed system over the years, with all ECU data stored in the internal network. But presently and future vehicle in the aforementioned new services require data to be disseminated across various networks service including cloud backed services, thereby resulting in a much larger attack surface. As a result, automakers must re-design vehicle architecture using a secure-by-design strategy. Additional, this creates the transformation that modern vehicles will be a well-developed cyber physical system (CPS) that has the capability of a system computational elements collaborating to control physical entities [12]. This definition emphasises the importance of considering both cyber- and physical related aspects of security. An autonomous car, for example, interacts substantially with the real world environment and has the difficulty of ensuring the sensing and actuation equipment' resilience. As a result, Wang et al. [13] pointed out, security in automotive also entails addressing the special difficulties of a CPS, a topic that would be explored in future papers.

D. Security-by-design.

The scrutiny and examination of security characteristics in the design of systems, in this case the RMTO within automotive system is the focus of this security by design, an emphasis in security engineering implementation [14]. This scrutiny and examination of security characteristics in systems is aimed at developing and creating systems that are robust and acceptably against invading threats, hazards and disruptions from malicious entity as Ross et al [15] noted that these approach naturally suggest the implementation of processes that must be applied systematically to the entire development life cycle of the target system covering pre and post-development activities, including testing that is aimed to validate the efficiency of already implemented security controls or identifying existing vulnerability and weaknesses of the system. The effectiveness of improving security practice is better when taken into account from an inception phase of the development process or cycles [16]. The security-by-design method recommends the implementation of proactive measures against known and unknown security threats and the application of the secure-by-default model in the designing of hardware and configuration of software components and access policies. In general, security-by-design entails the need to embed security in the design of systems by adopting both trusted hardware and software security assurance processes. Taking software assurance processes as an example, needs a comprehensive threat analysis, code review repetition and adaptation, include the designing relevant countermeasures against existing threats as part of the system architecture and executing a rigorous security testing to validate the security measure put in place as a holistic process principle viewed as a discipline in system engineering [17]. Several Secure Development Life Cycles (SDL) have recently emerged based on the secure-by-design approach. OWASP, Open SAMM, Cisco SDL and Microsoft SDL and are the most popular. All of these life-cycles incorporate threat modelling at

the start of the development process, as well as ongoing security testing and assessment throughout the software development process. The survey of Geer [18] and Jayaram and Mathur [19] give more detailed information on these topics.

II. Related Works

Several consideration by researchers [3], [20], [21] and industry partners [22] have explored the role RMTO plays in helping AV navigate through complicated situations. This situation are very tricky to be handled by the AV alone. Some AV business case are partly centred around the reduction of operational costs in which the remote monitoring and teleoperation (RMTO) solution allows an operator/supervisor to be responsible for multiple AV vehicles at the same time, as noted in project SAVOR [23]. At the heart of this consideration lies the security of the RMTO which is the focus of this paper.

E. Cybersecurity in AV.

The cyber-attacks these connected AV are exposed to via there different networks and interfaces that are linked to infrastructure within a public network, connected backend and open physical environment has been covered by Cui et al [24], [25] and [26]. In general terms, these are attack surface of the AV that reveals a collection of various attack vectors comprising different entry points that permits attackers to gain asses and attempts to insert malicious data/code to enable extraction of information from the AV, redirection of functions to comprising the security control of the AV. These have been investigated by various researchers such as Torre et al [27] using machine-learning model for driverless vehicle security and Denial-of-Service (DoS) and spoofing attacks dictation by machine learning [28]. Also a formal method for cybersecurity was explored in [29] and in ENISA project for cybersecurity smart cars [30], including Abedi et al foc[31] using on security at the physical layer and vehicle-to-everything (V2X) security through stable system and safe model ensuring integrity in interactions preserved privacy [32] and covering AV cybersecurity attacks feasibility, severity, preventability [33]. For detailed in-depth discussion on industry security challenges [34], [35] and framework for mitigation of VANETs associated security solutions [24] and [36].

F. Cybersecurity in RMTO

Presently, to the best of our knowledge, there are no cybersecurity consideration dedicated to RMTO or Teleoperations as can be seen above for AV. Rather they are considered within the AV and not as a separate system that has it own unique risk and threat. Even vehicle RMTO is still at the infant stage with the focus mainly for aiding lower levels AV navigate through tricky positions that the vehicles are less able to handle on their own, hence current AV reliance on fully human teleoperators. Zhang [3] presented a vision of an intelligent teleoperation based cloud driving by allowing a subset of the automated driving intelligence to be off-loaded from the vehicle into the cloud. While Ket-twich et al [37] Teleoperator work focuses on the creation of a human-machine interface for highly automated vehicles in a user-centered design process, usability and the psychological background of Teleoperating vehicles that requires the remote-operator to engage in multiple tasks as noted by Sheridan [38] listing five general functions that supervisory control requires. While [37] only focusing mainly on monitoring the situation which requires attentiveness, and overriding that requires taking over the AV when the automation is no longer able to do so. A similar work by [39] in developing a human machine-interface (HMI) for the teleoperation of AV that is able to present the sensor data from the vehicle to the operator in such a manner that enables the operator to easily understand the vehicles current state and the vehicle's environment.

III. Motivation

As shown in section II above, there exist a cybersecurity considerations for AV and different ways for RMTO operations in AV, but there remain a gap in all these work with regards to cybersecurity consideration for RMTO as a separate system to the AV. Therefore, in this paper a new adaptable security by design approach for ensuring a secured RMTO is developed. Though the security by design principle is still in the infant state within the automotive cybersecurity and especially in the application of RMTO, hence the novelty of this work.

IV. Methodology.

Our methodology (the design process) basic steps guided by the application of the international automotive cybersecurity standards - ISO/SAE 21434 and the UNECE/TRANS/WP.29/2020/79 (R155) for our adaptable Security-by-design approach for addressing secured RMTO is presented.

G. Security Engineering Lifecycle. worth saying that 21434 only applies to vehicles at SAE level 2

In other to apply our adaptable security-by-design approach to ensure a secured RMTO, we first consider integrating security into the development lifecycle of a RMTO system of an AV by focusing in building security activities into the initial phases of the development lifecycle [20]. These activities comprise of applying ISO 21434 guideline for cybersecurity such as; Organisational cybersecurity management, Project dependent cybersecurity management, Distributed cybersecurity activities, Continual cybersecurity activities, Concept phase, Production development phase, Post development phase and Threat analysis and risk assessment methods, including all the various sub-activities that are contained in each main activities (Product development: Cybersecurity requirement and architectural design and cybersecurity integration and validation). Utilising a well-defined and well-structural automotive cybersecurity engineering process aims to aid in the designing and developing of the RMTO with cybersecurity in mind from the unset. The focus here in this paper is on the concept phase and the product development phase of the security engineering lifecycles as stipulated by ISO 21434 and UNECE WP.29, so as to reduce the likelihood of successful cyberattack on the RMTO against the AV. Our approach start with the concept phase of the development lifecycle, incorporating the systems security engineering by thinking security right from the start when defining requirement of the RMTO [40]. Figure 4 shows the simplified overview approach for our RMTO that is adopted for the steps in Concept and product development phase as stipulated by ISO 21434. It shows the two primary phase around which cybersecurity consideration or design of the RMTO is based upon as per the standard: the concept phase and product development phase.

Here is a summary of what each of these activities comprises;

Concept Phase of the RMTO

The Concept phase of the RMTO is completed prior to initiating the product development phase of the RMTO, however, the information derived during this phase is applicable to all subsequent activities. Normally, the needs for the ODD (e.g. customer requirements) serve as the preliminary point for developing the RMTO concept. The objective of the concept phase is to ensure protection from potential threats or cyberattacks so as minimise losses, prevent damages that might result in functional safety of the AV, operational functions, data losses. It is worth mentioning that our approach do not know all the potential threat scenarios that the RMTO would face, as we cannot foresee the motivation or capabilities of a potential malicious attacker in the future. Hence, in order to mitigate this challenge, we seek solution to questions like whether, where, and how the RMTO is vulnerable, damages associated with any threats, and how we might deal with the impact of

the likely potential threats.

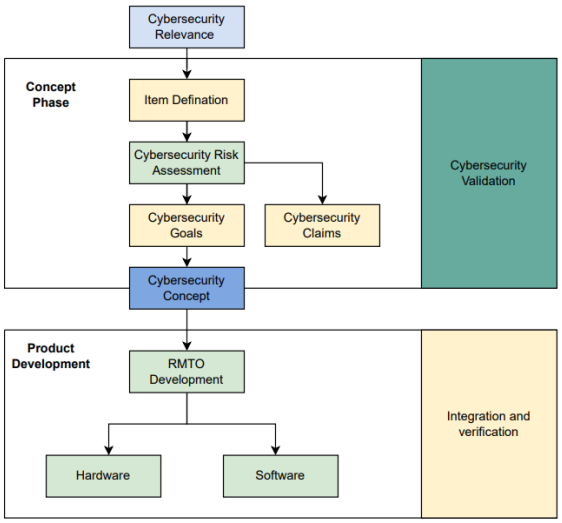


Figure 4: Steps in the concept and product development phase of the RMTO as per ISO 21424

The answer to addressing this challenges or questions is through a cybersecurity risk assessment as stipulated in ISO 21434 shown in the third point of figure 4. A cybersecurity risk assessment necessitates that we first define the Subject of investigation, such as the item and its relevant assets. Further, cybersecurity goals are then stipulated, these are top level cybersecurity requirements for each item based on the cybersecurity risks identified from our methods of cybersecurity risk assessment which would be covered in details in subsequent sections. To mitigate the risk of an Item, we stipulate a cybersecurity requirement to be applied to the Item including any necessary ODD, while the cybersecurity claims are used to elucidate why the risk treatment is well-thought-out appropriately.

Cybersecurity relevance.

As shown in figure 4, our very first step is carrying out a cybersecurity relevance assessment of the RMTO so as not to lead to waste of valuable resources that do not add any value or benefit. That is why ISO 21434 mandates that businesses do an initial study as part of their cybersecurity planning to ascertain whether an automobile road vehicle and its relevant system is cybersecurity relevant as not every part or component of a road vehicle's system is pertinent to cybersecurity. It should be noted that only things and components inside or on the perimeter of the vehicle, including aftermarket and servicing parts that are cybersecurity relevant, are subject to the application of ISO 21434. By us carrying out a cybersecurity relevance evaluation as one of the first steps early in the development process of the RMTO, ISO 21434 and other associated cybersecurity activities can be used in the appropriately, never the less, the standard does not outline or prescribe any particular method, approaches for determining the relevancy of cybersecurity of a vehicle system. Therefore our approach in determining cybersecurity relevance is shown in a decision tree in figure 5.

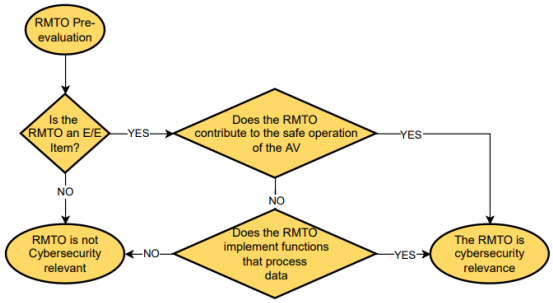


Figure 5: Checking of cybersecurity relevance in RMTO

Once we determine that the RMTO is cybersecurity relevance based on the questions in the decision tree, the application of ISO 21434 is carried out.

Item definition.

The first stage of the concept phase of the RMTO security engineering activities is the item definition. According to ISO 21434 [41], an item is a module, a component or sets of component that makes up a system that implement a function at the vehicle level (e.g. RMTO or infotainment system). The item definition involves a technical description as covered by ISO 21434 requirement in table 2. of the RMTO concerned but also a definition of the ODD of the function ("ODD: refers to the conditions in which the RMTO operates the AV intended function including geography, weather and light conditions, Speed range, road types, etc.…") and it's interaction with the AV, based on the assumptions and constraints in the context of cybersecurity. For details coverage see [41].

Table 2: Item definition requirement.

Item definition section 9.2.1
[RQ-09-01] The following information on the item shall be identified: a) Item boundary; b) Function boundary; c) Preliminary architecture
[RQ-09-02] Information about the operational environment of the item relevant to cybersecurity shall be described.

The item definition is documented by identifying and enumerating all the relevant existing information, such as the subsystems that makes up the AV, the cloud backend services and all interfaces this forms the in-vehicle network, the networks external to the vehicle, the functions of the item and the E/E system architecture etc. Notably, ISO 21434 did not specify and specific solution for defining an item, apart from that the item is always defined at vehicle levels and interface that exist between the different items.

Cybersecurity goals and claims

After all the relevant information about the RMTO has been identified and documented as part of the item definition, we carry out a threat assessment and a risk analysis (TARA) to ensure identification and assessment of the potential threats to the item and determination of the risk related to each of these identified threats [40]. The methodologies for cybersecurity risk assessment takes into account the information provided by the item description as defined in ISO 21434 in order to determine the scope of cybersecurity risk. The outcomes of the cybersecurity risk assessment will guide further analytical activities so that decisions about cybersecurity design for the RMTO are made based on the cybersecurity threats that pose the most risk. This ensures that we providing a risk-based cybersecurity design for the RMTO and not overreact to risks with no or minimal impact which could result in over-engineering solutions and the waste of precious resources. As the en-

lightenment of a risk assessment in accordance with ISO 21434 and equivalent analysis techniques such as the TARA would go beyond the scope of this section, relevant information is explained in detail in the next section (Implementation). Figure 5 illustrate the input and output of the relationship between our Item (RMTO) definitions, cybersecurity goal, cybersecurity claims and TARA.

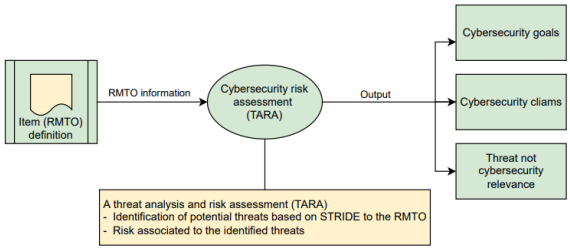


Figure 6: Item (RMTO) definitions, cybersecurity goal, cybersecurity claims and TARA

Cybersecurity goals.

The figure 5 output of cybersecurity goals takes details consideration of table 3 requirement as per [41].

Table 3: Cybersecurity goal requirement

Cybersecurity goals Section 9.4.2
[RQ-09-03] An analysis based on the item definition shall be performed that involves: a) asset identification in accordance with 15.3; b) threat scenario identification in accordance with 15.4; c) impact rating in accordance with 15.5; d) attack path analysis in accordance with 15.6; e) attack feasibility rating in accordance with 15.7; and f) risk value determination in accordance with 15.8
[RQ-09-04] Based on the results of [RQ-09-03], risk treatment options shall be determined for each threat scenario in accordance with 15.9.
[RQ-09-05] If the risk treatment decision for a threat scenario includes reducing the risk, then one or more corresponding cybersecurity goals shall be specified.
[RQ-09-06] If the risk treatment decision for a threat scenario includes: a) sharing the risk; or b) retaining the risk due to one or more assumptions used during the analysis of [RQ-09-03], then one or more corresponding cybersecurity claims shall be specified.
[RQ-09-07] A verification shall be performed to confirm: a) correctness and completeness of the result of [RQ-09-03] with respect to the item definition; b) completeness, correctness and consistency of the risk treatment decisions of [RQ-09-04] with to the results of [RQ-09-03]; c) completeness, correctness and consistency of the cybersecurity goals of [RQ-09-05] and of the cybersecurity claims of [RQ-09-06] with respect to the risk treatment decisions of [RQ-09-04]; and d) consistency of all cybersecurity goals of [RQ-09-05] and cybersecurity claims of [RQ-09-06] of the item.

The cybersecurity goal in essence refers to a damage scenario connected with a threat scenario, or an attack vector. SAE J3061 indicates that when cybersecurity goals are defined for the prospective attacks offering the greatest risks, they may be the inverse of a potential danger at the highest level. For instance, if a potential threat is denial of service (DOS) of the RMTO establishing a connection to the cloud service, the highest-level Cybersecurity goal may be to avoid or decrease the likelihood of DOS, or to mitigate the potential repercussions. This is further illustrated in subsequent section of this paper.

Cybersecurity claims.

A Cybersecurity claim is a declaration about a risk. It can contain a justification for retaining or sharing the risk according to the results shown in the risk assessment. Nevertheless, cybersecurity claims are stipulated for risks with controls outside the item (RMTO), which need to be handled. These situations include those in which the risk is treated by the application of cybersecurity controls in which the risk is lowered to an acceptable level (e.g., a RMTO item uses a dedicated VPN to establish connection to the cloud) or transferring the risk based on cybersecurity justification that the risk is appropriate based on the level of impact or damage. Table 3 [RQ-09-06] (b) stipulates the requirement that is considered in the cybersecurity claims as shown in [41]. Cybersecurity claims require monitoring, therefore, it could be beneficial to keep a list of cybersecurity claims that initially has few or no entries at the start of development and is then regularly updated in accordance with the cybersecurity claims produced during the product lifetime.

Cybersecurity concept.

The cybersecurity concept outlines the cybersecurity strategy for an item or component [42]. According to ISO 21434, the completion of the cybersecurity goals with regards to cybersecurity requirements that are assigned to the components or element of any preliminary architectural design as well as the ODD form the basis for the cybersecurity concept. The ISO 21434 standard describes the concept as a process that incorporates the goals which is steamed off from the requirement inculcating the entirety of Item definition, TARA, goal and claim under one entity as the required prerequisite of inputs that have to be available prior to any design or development. Figure 6 gives an illustration of these prerequisite that is required in our RMTO cybersecurity concept with regards to the ISO 21434 guidelines.

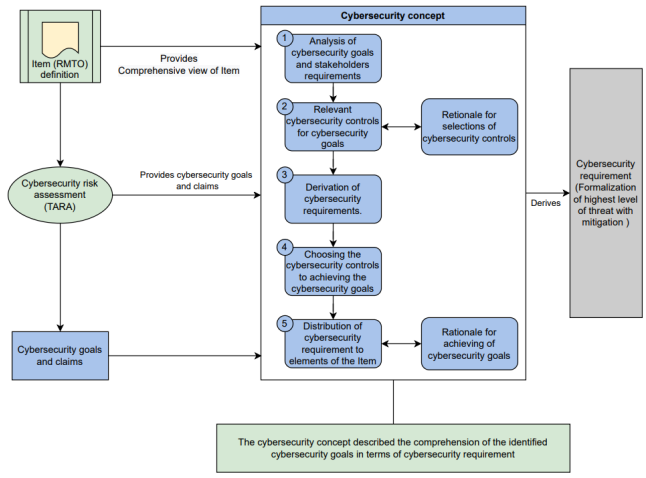


Figure 7: Cybersecurity strategy with prerequisites inputs for process elaboration of cybersecurity concept

This is the outcome of a process that combines inputs from the item definition, the TARA and cybersecurity goals into a single, high-level approach to achieving cybersecurity for the RMTO as the current standard does not specify any particular technologies or solutions for the development of a cybersecurity concept other than the stipulated high level requirement shown at table 4.

Our adapted approach for elaborating the process of cybersecurity concept with regards to ISO/SAE 21434 consideration is shown below [42]:

- Analysis of cybersecurity goals and stakeholders requirements

Table 4: Cybersecurity concept requirement

Cybersecurity concept Section 9.5.2
[RQ-09-08] Technical and/or operational cybersecurity controls and their interactions to achieve the cybersecurity goals shall be described, taking into account: a) dependencies between the functions of the item; and/or b) cybersecurity claims.
[RQ-09-09] Cybersecurity requirements of the item and requirements on the operational environment shall be defined for the cybersecurity goals in accordance with the description of [RQ-09-08].
[RQ-09-10] The cybersecurity requirements shall be allocated to the item, and if applicable to one or more of its components.
[RQ-09-11] The results of [RQ-09-08], [RQ-09-09] and [RQ-09-10] shall be verified to confirm: a) completeness, correctness, and consistency with respect to cybersecurity goals; and b) consistency with respect to cybersecurity claims.

Cybersecurity goals and claims.

- Relevant cybersecurity controls for cybersecurity goals.
- Deriving cybersecurity requirements from related cybersecurity goals.
- Choosing cybersecurity control to achieve the cybersecurity goals by meeting the cybersecurity requirements in order to reduce the risk of the threats.
- Distribution of cybersecurity requirements to elements or components of the RMTO or the ODD etc.

Verification of cybersecurity concept

Our scope of verification is checking that the cybersecurity goals of our RMTO will be met by our cybersecurity requirements as identified in our TARA with addition of controls and also checking the performance of the RMTO for potential problems arising from the implemented controls that are aimed at reducing the risks of threat.

H. Logical Security Layered Concept

Our logical security layered concept is an associated security control mechanism based on the decomposition of threats, vulnerabilities and attack methods as per ECE/TRANS/WP.29/2020/79 (R155) [43]. Security control is implemented in different area of the system like layers or levels based on part of threat identified. R155 annex 5 list threats based on layered concept of security decomposition into areas of impact and corresponding controls to mitigate against this threats in their different security layered in the vehicle, outside of the vehicle, IT backend and communication channels and interface etc. Figure 6 gives an illustration of logical security layered concept as contained annex 5 of ECE/TRANS/WP.29/2020/79 (R155), though R155 did not categorically stipulate how the cybersecurity controls should be implemented, but rather it stipulate requirements for mitigation of the threats, vulnerabilities and attacks. Part A annex of R155 describing the baseline for the threats, vulnerabilities and attack, while Part B annex describing the mitigations of the threats which are intended for vehicle types and Part C describes mitigations to the threats which are intended for areas outside of vehicles, e.g. on IT backends [43]. Figure 8 shows the illustration of the various logical security layered concept and the various security controls that can be applied to mitigate against the threats, vulnerabilities and attacks on a given system and its boundaries that show a full end to end cybersecurity consideration of the system.

Each of the seven layers of cybersecurity is targeted to a specific security are of a system. In our case. The RMTO system cut across several

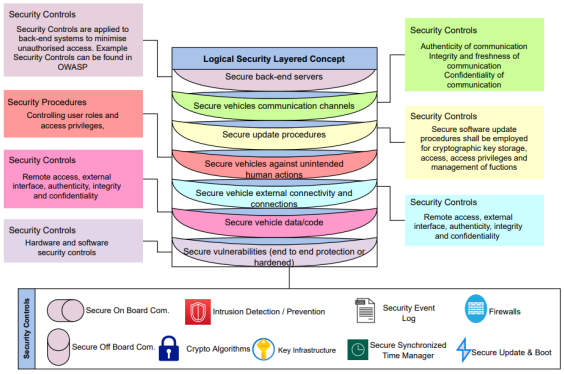


Figure 8: Logical security layered concept adapted from (R155)

areas of the logical security layers, but the focus here would not be to cover each and every area of the security layers for our adaptable security-by-design approach for addressing secured RMTO. The next section of this paper would cover the relevant logical security layers for addressing secured RMTO of an autonomous vehicle.

Product development

As shown in figure 4, the next phase is product development and in our case the RMTO is the product under consideration. Generally this phase incorporates the entire product architecture, as well as the definition of specifications, interfaces and subsystems. In the case of the RMTO, all boundary system such as the AV, the Cloud services and the various subsystem that makes up the RMTO are considered. The most crucial step of development function's occurs at this phase, which formally ends the development process. As noted [42], organizations need to make sure that all needs; such as those related to cybersecurity and those that are relevant to later stages of the product lifecycle, like manufacturing, operation, and decommissioning, have been taken into account during development. Since this process is very specific to automotive companies and the tiers suppliers within the automotive domain having their own internal processes for product development management. Hence for this paper we consider ISO/SAE 21434 two main aspect defining the specification of the cybersecurity requirements and architectural design activities that can be used by any business during the product development phase.

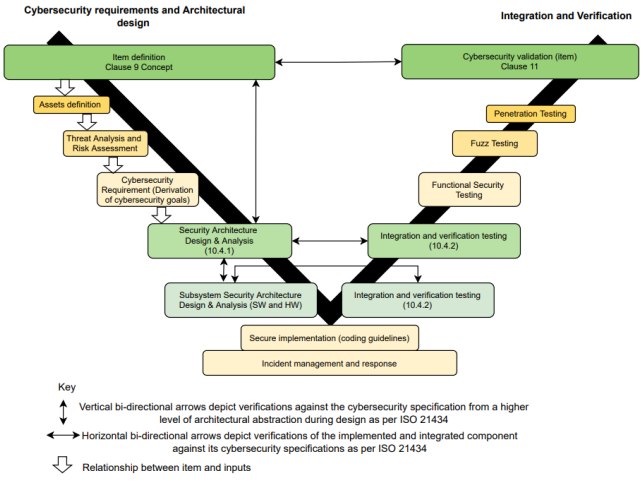


Figure 9: The V-model workflow for product development phase adapted from ISO 21434.

Figure 9, illustrate a work flow for the RMTO development according to ISO/SAE 21424 [41] product development activities applied to a V-model-based workflow, where specification of the cybersecurity

requirements corresponds to the left side of the V-model and architectural design corresponds to the right side. Obviously, it is possible to use development strategies or techniques that diverge from the V-model (such as agile software development). Practically, this is adaptable to organisation specific, but the foundation remains intact as per the standard objective requirement for cybersecurity specification requirement activities and integration and verification activities to be completed despite the organisation specific process of adapting the product development phase.

Cybersecurity specification requirement activities.

The cybersecurity specification requirement comprises of the cybersecurity requirements and the architectural design. The specification needs gradual improvement that is refined incrementally. This aspect is correlated to the left-hand side of the V-model and relate to the incremental integration of components performed in a specific other, though overlapping is required sometimes in the work flow or progression. Cybersecurity specification requirement activities are stipulated in a high level requirement shown in table 5 as required by ISO/SAE 21434 standard regarding the refinement of the cybersecurity specification.

Table 5: Product development requirement.

Product development Section 10.4.1
[RQ-10-01] Cybersecurity specifications shall be defined based on: a) cybersecurity specifications from higher levels of architectural abstraction; b) cybersecurity controls selected for implementation, if applicable; and c) existing architectural design, if applicable.
[RQ-10-02] The defined cybersecurity requirements shall be allocated to components of the architectural design.
[RQ-10-03] Procedures to ensure cybersecurity after the development of the component shall be specified, if applicable.
[RQ-10-04] If design, modelling or programming notations or languages are used for the cybersecurity specifications or their implementation, the following shall be considered when selecting such a notation or language: a) an unambiguous and comprehensible definition in both syntax and semantics; b) support for achievement of modularity, abstraction and encapsulation; c) support for the use of structured constructs; d) support for the use of secure design and implementation techniques; e) ability to integrate already existing components; and f) resilience of the language against vulnerabilities due to its improper use.
[RQ-10-05] Criteria (see [RQ-10-04]) for suitable design, modelling or programming languages for cybersecurity that are not addressed by the language itself shall be covered by design, modelling and coding guidelines, or by the development environment.
[RC-10-06] Established and trusted design and implementation principles should be applied to avoid or minimize the introduction of weaknesses.
[RQ-10-07] The architectural design defined in [RQ-10-01] shall be analysed to identify weaknesses.
[RQ-10-08] The defined cybersecurity specifications shall be verified to ensure completeness, correctness, and consistency with the cybersecurity specifications from higher levels of architectural abstraction.

Independent of the level of abstraction, there are three key inputs that need to be defined and improved during the cybersecurity requirement formulation process [42];

- Cybersecurity requirement s from higher levels of architecture abstraction.
- Cybersecurity controls selected for implementation, if applicable.
- Existing architectural design from the higher levels, if applicable.

Cybersecurity integration and verification activities.

These activities pertain to the gradual integration of parts and objects into ”higher levels of architectural abstraction” and eventually into a goal vehicle, and they correspond to the right leg of the V-model. To confirm that the developed product complies with the specified cybersecurity standards and design specifications as well as the established cybersecurity goals, each increment must be appropriately validated. The cybersecurity integration and verification activities activities are stipulated in a high level requirement shown in Table 6 as required by ISO/SAE 21434 standard regarding the integration and verification activities.

Table 6: Integration and verification requirement.

Integration and verification section 10.4.2
[RQ-10-09] Integration and verification activities shall verify that the implementation and integration of components fulfil the defined cybersecurity specifications.
[RQ-10-10] The integration and verification activities of [RQ-10-09] shall be specified considering: a) the defined cybersecurity specifications; b) configurations intended for series production, if applicable; c) sufficient capability to support the functionality specified in the defined cybersecurity specifications; and e) conformity with the modelling, design and coding guidelines of [RQ-10-05], if applicable.
[RQ-10-11] If verification by testing is adopted, test coverage shall be evaluated using defined test coverage metrics to determine sufficiency of the test activities.
[RC-10-12] Testing should be performed in order to confirm that unidentified weaknesses and vulnerabilities remaining in the component are minimized.
[RQ-10-13] If testing in accordance with [RC-10-12] is not performed, then a rationale shall be provided.

All the specification requirement and architectural design activities in the product development section need to be integrated into the system and verified to confirm reliability and completeness of the RMTO. This include all the subsystems that make up the RMTO, the Cloud Services and the AV integration and verification. Integration involves an integration test and refers to the combination of various components. Aspects of cybersecurity must be taken into account in the entire integration strategy. Corresponding verification operations must be carried out to ensure that the design has been implemented and that the components have been integrated in a way that complies with the established cybersecurity specification. Verification includes ensuring that the combined product satisfies the requirements by checking for correct implementation. It also involves the development of a verification specification, which outlines the intended test cases and outcomes [42].

V. Implementation.

In other to implement our Adaptable Security-by-design approach for addressing secured RMTO of an AV, the basic steps consideration for the implementation is already described in section IV (design process). In this section the first consideration is the high level architecture (subsystems that makes up the RMTO, the cloud service, broadband gateway, and the adaptable AV).

I. Security Architecture.

In other to address our first consideration of high level architecture, before further decomposing into security architecture of the RMTO, we ask the question;

1). How do we generate the high level architecture of our RMTO which is the basic input required for our design implantation of our adaptable security-by-design approach for addressing secure RMTO of an AV?

- According to the facts at hand, the description of the high level architecture contains both logical and physical data flows to and from other objects outside the item as well as internal components and their connections inside the item. The definition of the high level architecture must at least address internal components and data flows within the item as well as across its boundaries in order to be useful in later stages of the cybersecurity development process.
- The high level architecture of our RMTO is an input generated from discussion with several stakeholders including an industrial partner (Conigital) in the project SAVOR (Safely Advancing Vehicle Automation on the Road) [23]. Earlier on in the development phase, we identify the stakeholders that make our RMTO system and the boundaries systems (e.g AV), we align on the subsystem and interfaces requirement taking into account input from functional safety, ODD and communicating with the responsible team of each of this subsystem and interface.

Figure 10 show an illustrative high level architecture that is generated from the question asked above. This architecture has been adapted for illustrative purposes of this paper removing confidential information that would identify the specifics of the RMTO real application, but the architecture is sufficient enough for the purpose of we demonstrating our adaptable security-by-design approach for addressing a secured RMTO of an AV and can be replicable for security-by-design of future automotive systems or automotive RMTO.

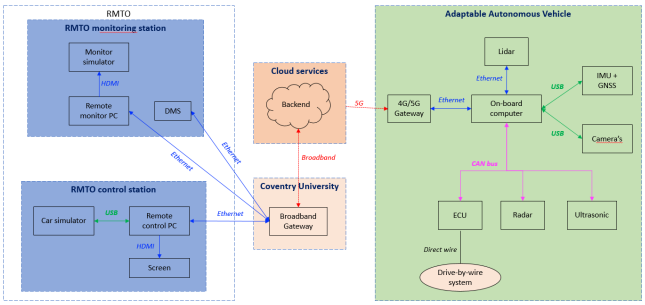


Figure 10: Illustrative high level RMTO architecture.

Looking at the architecture in figure 10, four systems are identified as blocks: the RMTO (RMTO monitoring station and RMTO control station), the Cloud services, Coventry University and the Adaptable Autonomous Vehicle. These listed blocks are both software and hardware related, they all contain software, hardware and interfaces parts that would be accessed and analysis to determine if they can be listed as candidate assets during the translation of the high level architecture into security architecture in the next part of our implementation.

Determination of security architecture.

In other to determine the security architecture of our RMTO, it is necessary to first consider the question of;

2). How do we allocate cybersecurity requirement to systems (subsystem, components and interface) of our RMTO architectural design?

- The answer to the question of allocating a cybersecurity requirement is first addressed on determining if the RMTO is cybersecurity relevant, this is addressed in Section IV design process above, where we illustrated with a decision flowchart in the concept phase of the RMTO that the RMTO is cybersecurity relevant.
- Cybersecurity specifications must therefore include the specification of interface between sub-components of the defined architecture design related to the fulfilment of the defined cybersecurity requirements, including their usage to include static and dynamic part.
- Using an architecture modelling tool (e.g. Enterprise Architect) [sparxEA]. A relationship matrix or a similar tool can be used to allocate the requirements to the architectural model. Not only is it a requirement of the 1SO/SAE 21434 that requirements be linked to architecture, but it is also the current state of the art in systems engineering and the automobile industry.

Following on from the illustrative high level RMTO architecture diagram above, we approach the determination of the RMTO security architecture by utilising an automated plugin within Enterprise Architecture called ThreatGet. ThreatGet [44] is a product developed jointly by the AIT Austrian Institute of Technology and Lieber Group and is targeted at the automotive sector. ThreatGet uses the STRIDE categorisation for threats. STRIDE is formed as a mnemonic, derived from the threat categories associated with each of the letters of the word: (S)poofing, (T)ampering, (R)epudiation, (I)nformation disclosure, (D)enial of Service, (E)levation of Privilege. The STRIDE model is a threat modeling approach proposed by Microsoft, in which six categories of general attack methods are proposed that can be used to derive threat scenarios from damage scenarios. For more information on STRIDE, see [45]. The high level architecture diagram, shown in Figure 10, has been converted to an Enterprise Architect system diagram from which this is modelled into security architecture model (see Figure 11) and analysed using ThreatGet.

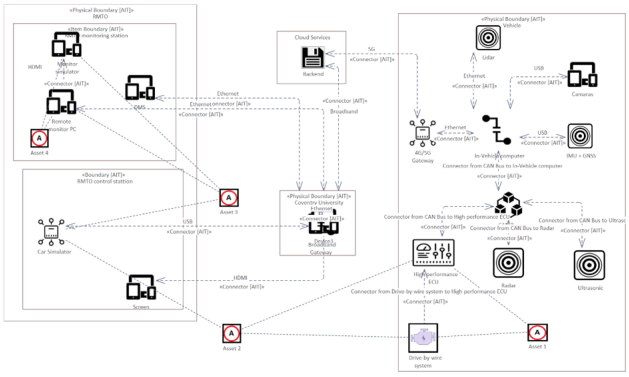


Figure 11: A depiction of Security architecture of RMTO in ThreatGet.

Looking at the depicted security architecture of our RMTO in Figure 11, four systems are identified as blocks: the RMTO (RMTO monitoring station, RMTO control station), the Cloud services, Coventry University and Adaptable Autonomous Vehicle. Internally within these listed blocks, we have the elements (software's and hardware's parts) that makes up these systems or sub-systems. Apart from the four blocks of systems, we have about six instances (Ethernet, Broadband, 5G/4G, HDMI, CAN and USB) of data transfer that can been seen in the depicted security architecture of the RMTO. Finally within the RMTO security architecture are four Assets (Asset1, Asset2, Asset3 and Asset4) in blocks that determine the part of the system that is vital to be protected from threats. As discussed in section IV, this RMTO security architecture culminated from item definition of the concept phase after due determination of the cybersecurity relevance as illustrated in above Figure 4. Following on from this, in other for us to carry out our cybersecurity risk assessment for our RMTO, we pose the below question to help us address this risk assessment;

3). For a given RMTO prototype or automotive system, how do we formulate a standard Threat Assessment and Risk Assessment (TARA) which could be viable for automated, efficient and scalable deployments to enable security-by-design of an automotive system (RMTO)?

- i. We start by looking at the risk assessment process stipulated by ISO/SAE 21434 section 15 [ISO21435]. Figure 12 gives an illustration of the various aspect that needs to be considered.

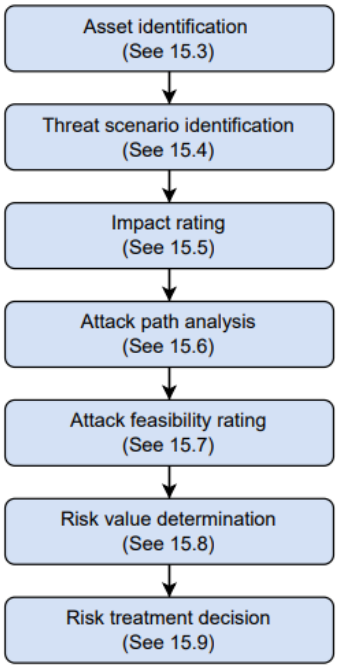


Figure 12: A process of risk assessment according to ISO/SAE 21434 [41]

Asset Identification:- The practice of systematically identifying a system's assets that are relevant to cybersecurity is known as asset identification. A system component or element known as a cybersecurity asset is one for which the loss of cybersecurity capabilities could cause substantial harm to a stakeholder. Such an asset always has at least one cybersecurity feature, whether it be physical or digital (e.g. Confidentiality, Integrity and Availability) [42]. As per [41], creation of damage scenarios is required during the asset consideration as stipulated by requirement [RQ-15-01] and Assets with cybersecurity properties whose compromise leads to a damage scenario shall be identified [RQ-15-02].

Threat scenario identification:- This can apply to the targeted asset, the cybersecurity property that has been hacked, and the activity taken to complete a damage scenario as per the requirement stating the threat scenarios shall be identified [RQ-15-03]. Our approach here for identification is based on the STRIDE model as discussed above [41].

Impact assessment:- Is a method of rating the negative consequences from the damage scenarios of an assets. Considering the damage scenarios gives an insight into the negative consequences of the assets that is compromised. Though they do not provide a means to comparing the relative importance of damage scenarios, therefore a return to the original objective of risk assessment needs to be considered [42]. Hence, to enable an unbiased evaluation of the severity of the harm, an impact assessment rating system—also known as an impact rating method—must be used. Contrasting to asset identification and threat scenario identification, [41] proposes a specific method for carrying out an impact assessments. Table 7, gives the relevant requirements impact assessment.

Table 7: Impact assessment requirement.

Impact assessment section 15.5.2
[RQ-15-04] The damage scenarios shall be assessed against potential adverse consequences for road users in the impact categories of safety, financial, operational, and privacy (S, F, O, P) respectively.
[RQ-15-05] The impact rating of a damage scenario shall be determined for each impact category to be one of the following: — severe; — major; — moderate; or — negligible.
[RQ-15-06] Safety related impact ratings shall be derived from ISO 26262-3:2018, 6.4.3. [PM-15-07] If a damage scenario results in an impact rating and an argument can be made that every impact of another impact category is considered less critical, then further analysis for that other impact category may be omitted.

Attack path analysis: - Attack trees help the function of assisting threat analysis and risk assessment throughout the vehicle's lifecycle [41]. The attack tree can be compared to a fault tree in an automotive setting that is intended to describe intentional and malicious activities made by an adversary in order to compromise the target vehicle, as opposed to the problems that are more passively expressed in fault trees [46]. For several suggestions and usage of attack trees, see [47],[48],[49], [50]. According to [41], a mention of the threat scenarios that the attack path can actualize should be included in the attack path description as noted in requirement [RQ-15-08] The threat scenarios shall be analysed to identify attack paths and [RQ-15-09] An attack path shall be associated with the threat scenarios that can be realized by the attack path. Given that general means of attack have been identified during threat scenario identification, the natural next step would be to estimate the chance of each threat scenario materializing into an actual attack and then use this knowledge to draw a conclusion regarding risk assessment. According to ISO/SAE 21434, a refining process must be performed to reduce this deviation. Attack path analysis is a refinement stage in which the precise steps required by an attacker to carry out threat scenarios are discovered using a formal, documented approach. ISO/SAE DIS 21434 recommends two different methods;

- Bottom-up, in which an initial vulnerability is used as a starting point to determine what additional actions may lead to the execution of at least one threat scenario.
- Top-down, in which the threat scenario is used as the attack goal and further attack paths are determined based on theoretical weaknesses that may exist in the proposed system.

Attack feasibility rating: - The attack likelihood of a component or element is assessed using the attack feasibility rating. To be able to quantify the risks involved, threat scenarios must be developed to identify general attack methods and attack path analysis must be carried out to identify the precise attack actions. Attack path information analysis is also necessary to assess the feasibility of an attack and gauge its likelihood. Simple numerical techniques of risk assessment are made possible by the determination of a quantitative value for the probability of attack, which may be paired with a quantitative measure of impact [42]. From table 8, we can see the ISO/SAE 21424 requirement governing the principle of attack feasibility rating.

Risk value determination:- Impact assessment and attack feasibility assessment outputs must be combined into a single risk level once both

Table 8: Attack feasibility rating requirement.

Attack feasibility rating section 15.7.2
[RQ-15-10] For each attack path, the attack feasibility rating shall be determined as described in Attack feasibility ratings and respective descriptions. See below High - The attack path can be accomplished utilizing low effort. Medium - The attack path can be accomplished utilizing medium effort. Low - The attack path can be accomplished utilizing high effort. Very low - The attack path can be accomplished utilizing very high effort.
[RC-15-11] The attack feasibility rating method should be defined based on one of the following approaches: a) attack potential-based approach; b) CVSS-based approach; or c) attack vector-based approach.
[RC-15-12] If an attack potential-based approach is used, the attack feasibility rating should be determined based on core factors including: a) elapsed time; b) specialist expertise; c) knowledge of the item or component; d) window of opportunity; and e) equipment.
[RC-15-13] If a CVSS-based approach is used, the attack feasibility rating should be determined based on the exploitability metrics of the base metric group, including: a) attack vector; b) attack complexity; c) privileges required; and d) user interaction.
[RC-15-14] If an attack vector-based approach is used, the attack feasibility rating should be determined based on evaluating the predominant attack vector (cf. CVSS [24] 2.1.1) of the attack path.

procedures are complete in order to achieve a TARA's primary objective of identifying priorities for cybersecurity assurance efforts and resources. ISO/SAE 21434 requirements and recommendation stated in section 15.8.2 [RQ-15-15] "For each threat scenario the risk value shall be determined from the impact of the associated damage scenarios and the attack feasibility of the associated attack paths" and in [RQ-15-16] "The risk value of a threat scenario shall be a value between (and including) 1 and 5, where a value of 1 represents minimal risk"[41].

Risk treatment decision: - The overall objective of risk assessment, i.e., the best distribution of cybersecurity assurance resources, has thus far been explored in the context of comprehending threat prioritisation in order to determine which threats to handle first. The risk level determined as a result of the earlier activities indicates which risks should be addressed in the order they should be addressed, but it does not offer any advice on how to do so. Section 15.9.2 of ISO/SAE 21423 gives a requirements and recommendation for treating in [RQ-15-17] such as [44];

- Avoiding the risk by removing the risk sources, or deciding not to start or continue with the activity that gives rise to the risk,
- Reducing the risk,
- Sharing or transferring the risk (e.g. through contracts, buying insurance),
- Accepting or retaining the risk.

ii.) After initially utilising ISO/SAE 21434 in 3i what is this? to address the question for a given RMTO prototype or automotive system, how do we formulate a standard TARA which could be viable for automated, efficient and scalable deployments to enable security-by-design of an automotive system (RMTO)?. We carry out an automated analysis via ThreatGet plugin in Enterprise Architecture, with the basic input been the security architecture model in Figure 11 above. The various section in the risk assessment process stipulated by ISO/SAE 21434 section 15 as illustrated in above Figure 12 is automated. Appendix A gives a screen sort of the RMTO security architecture model in Enterprise Architecture utilising ThreatGet[51], [44].

The RMTO automated TARA analysis we performed using ThreatGet identified a total of 148 threats, these threats are categorised as per STRIDE model. The Threats are also drawn from the UNECE WP29 Vehicle Threat List, ETSI (European Telecommunications Standards Institute), ITU (International European Union), expert knowledge from AIT analysis and extant academic discourse. A break down of summary of threats and severity levels as recommended by ISO/SAE 21423 is shown in figure 13.

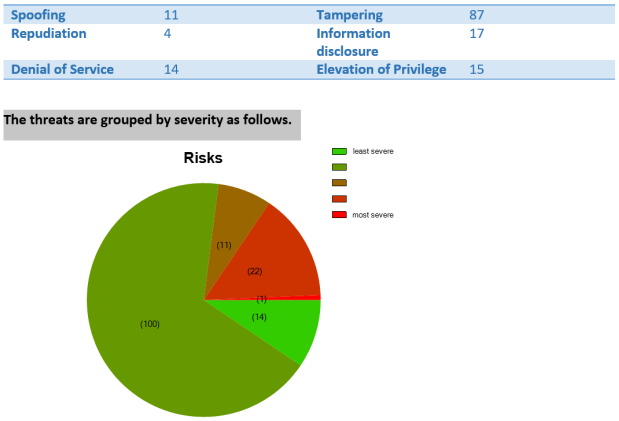


Figure 13: RMTO TARA threats and severity summary [41]

Each of the threats in the list of threat scenarios is given an impact and likelihood, based on the information extracted from the ThreatGet knowledge base and they are also grouped by severity as shown in Figure 13.

In Figure 14, we show the RMTO system risk matrix, generated from the ThreatGet to assign a risk level to the identified threats based on their impact and likelihood. The risk matrix in the Figure 13 is in accordance with ISO/SAE 21434 [44]. With ThreatGet, we evaluates the RMTO risk that a threat poses on a scale between one and five based on this risk matrix.

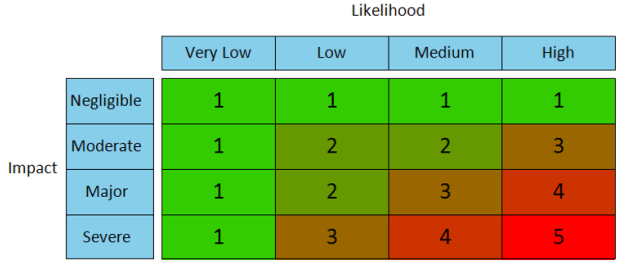


Figure 14: RMTO Security risk matrix from ISO/SAE 21434 [4]. The range of risk severity is from 1 and 5.

J. Formalisation of the highest level of threats discovered in the RMTO system with a corresponding mitigation action.

The formalisation of the highest level of threats discovered in the RMTO system with a corresponding mitigation action is considered as a cybersecurity goal, which in essence is a concept level cybersecurity requirement linked with one or several threat scenarios, that is then applied to the RMTO asset i.e. the RMTO cybersecurity property that is likely to be compromised as identified by the STRIDE model of threats discussed above and the corresponding mitigation could be the application of cybersecurity controls as illustrated in our logical security layered concept section shown in Figure 8 above. use two or three sentences! Following on from the ThreatGet TARA drawn out from section i of this paper in line with the UNECE WP29 (Annex 5, List of threat and corresponding mitigation, part B) [43]. From the total identified 148 threats generated automated via ThreatGet, we formalised the highest levels of threat narrowing it down to 34 threats with the most severity of risk from level 3 to 5 per the STRIDE categories of threats, see Figure 15.

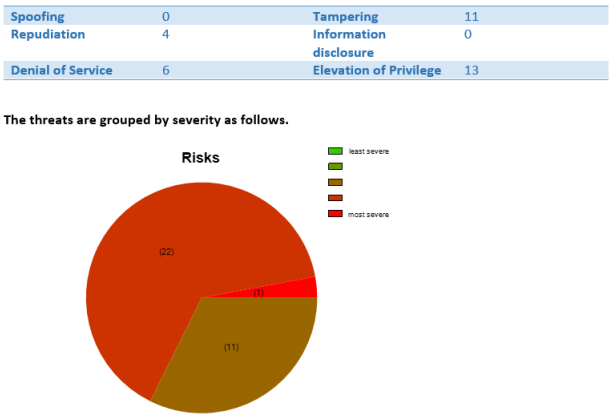


Figure 15: Formalisation of the threats analysis according to risk level scale from 3 to 5 and per each STRIDE category

From this generated threats list of 34 most severe threats, a list of requirements as stipulated in UNECE WP29 (Annex 5, List of threat and corresponding mitigation, part B) [43] is recommended in consideration with our Logical Security Layered Concept in section H above.

Verification.

Some aspects (e.g. the 5th layer –secure vehicle external connectivity and connection) of our logical security layered concept of our adoptable security-by-design capability to reinforce the security of the RMTO systems against some of the identified risks and threat (Denial of service) is verified by a cybersecurity penetration testing on the cloud base system (NTGR) that connect the RMTO and the AV to the cloud server of an industrial partner (Conigital). The RMTO and the AV both interface with this NTGR via a wireless communication (see figure 10 above). We carried out a SYN flood denial of service (DOS) attack on the NTGR that connect the RMTO and the AV to the backend service in the cloud. A SYN flood denial of service (DOS) attack, is when an attacker sends a flood of malicious data packets to a target system, with the intention of overloading the target and stop it working as it should [52]. The target machine sends back a SYN acknowledgment in response to the request and waits for the SDK (software development kit) to complete session setup. The target machine does not get the response because the source address is fake. For the case of our penetration testing, a Syn DOS attack was chosen as the cybersecurity pen test to verify the requirement and use case, sample illustration of (requirement and use case) in figure 16,

odd to cut a sentence up with a Figure. so as to reinforce the security

2 Linked Requirements and Use Case

The following requirements are tested against denial of service (DOS) attack to cover below use cases.

Requirement ID	Requirement Text	Comment
HLR_SAV _04	Communication with RMTO Rig	The SAVOR vehicle shall continuously communicate its status and other dynamic data to the RMTO Rig.
HLR_SAV _07	Observing and assigning AV to remote control	A fleet manager shall receive remote operation request from the SAVOR AV and assign an operator for remote control
HLR_SAV _9	Perception	The remote-control operator shall receive the perception information of the controlled vehicle
HLR_SAV_11	Environment model creation	The RMTO Rig shall receive the perception data from the NTGR and create an environment model precise enough to allow the remote operator to control the vehicle.

Use Case

Use Case	Use Case description	Comment
Denial of service (M13)	Cause the Target to Crash or Stop or disabling functions	It is possible to launch a denial-of-service (DoS) attack against essential units within the vehicular network, which can have multiple consequences for the target, including the interruption of functionalities, malfunctioning or even decreasing its performance (i.e., performance degradation). In all circumstances, failing to ensure the availability of critical units in a vehicle, such as the ECU, could result in various adverse outcomes.
Denial of service (M13)	Disruption of systems or operations	Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging.
Denial of service	Sam Monitors Single Vehicle with No Override Issues	Denial of service on the use case of the functional specification 2.1 Relevant section to which this DOS impact are (2 -4), (9), (10), (14 -16), (19-20) etc.

Figure 16: Requirment and use case for penetration testing illustration

of the RMTO systems against some of the identified risks and threats (DOS). The verification is carried out on the DOS threats due to the attack coverage of the DOS to several attack vectors to the RMTO system on our first testing (among many others).

Result

The SYN DOS attack was only successful in our machine (the attacker machine) preventing the target host cloud based system (NTGR) from loading. The NTGR is the user interface admin panel that enables the RMTO to control the AV after connecting to the cloud server. Several drawbacks were noted (due to security controls implementation that reinforce the security of the RMTO systems against some of the identified risks and threats (DOS)) such as the attack was only possible by we obtaining the network credential from authorised source and the SYN DOS attack was only possible on the attacker host machine and not possible on other machine connected to the same router and network.

Conclusion

In this paper, an adaptable security-by-design approach for ensuring a secured RMTO of an AV level 4 is proposed. The proposed adaptable security-by-design for securing a RMTO against cyber-attack and ensuring cyber resilience in the role RMTO plays in aiding or helping AV navigate through complicated situations among many others. At the heart of our approach is a consideration of the problem of potential pathways and attack vectors or threat surfaces by which a malicious attack can be carried out on a RMTO and impacting the AV itself. Therefore to address this, we employ an adaptable security-by-design approach for RMTO that covers Security Engineering Lifecycle. This started with a concept phase of the RMTO by us looking at the cybersecurity relevance as an initial phase of analysis to determine if our

proposed methodology is worth pursuing. After establish cybersecurity relevance for our RMTO, we explored and covered various cybersecurity activities such as item definition, cybersecurity goals and claims cybersecurity goals, cybersecurity claims cybersecurity concept and verification of cybersecurity concept as required by ISO/SAE 21424. Based on establishing the first aspect of our methodology, we proceeded in establishing our second aspect the Logical Security Layered Concept, which is guided by ISO/SAE 21423. In our proposed logical security layered concept, 7 layers of associated security control mechanism based on the decomposition of threats, vulnerabilities and attack methods as per ECE/TRANS/WP.29/2020/79 (R155) is designed and presented. A key aspect of this is the implementation of security controls based on the aspect of threats identified as per the 7 security layers proposed, we also looked at the cybersecurity activities within the product development using the v-cycle starting off with cybersecurity specification requirement activities and concluding at cybersecurity integration and verification activities. Our third and last aspect of our methodology is the Security Architecture. The security architecture is the implementation of our design process following on from coverage of the Security Engineering Lifecycle and Logical Security Layered Concept. The implementation, started off my addressing 3 questions such as; how do we generate the high level architecture of our RMTO which is the basic input required for our design implantation of our adaptable security-by-design approach for addressing secure RMTO of an AV? how do we allocate cybersecurity requirement to systems (subsystem, components and interface) of our RMTO architectural design and lastly for a given RMTO prototype or automotive system, how do we formulate a standard Threat Assessment and Risk Assessment (TARA) which could be viable for automated, efficient and scalable deployments to enable security-by-design of an automotive system (RMTO)?. The answers to this questions forms the basis of our implementation as we started by looking at an adaptable illustrative high level architecture for the RMTO which covers the various systems, subsystems, interface etc. this was then translated into security architecture utilising ThreatGet a plugin in Enterprise architecture and a detailed TARA analysis as stipulated by ISO/SAE 21434 covering various TARA activities such as Asset Identification, Threat scenario identification, Impact assessment, Attack path analysis, Attack feasibility rating, Risk value determination and Risk treatment decision. Lastly a formalisation of the highest level of threats discovered in the RMTO system with a corresponding mitigation action is considered as a cybersecurity goal, which in essence is a concept level cybersecurity requirement linked with one or several threat scenarios, that is then applied to the RMTO asset i.e. the RMTO cybersecurity property that is likely to be compromised as identified by the STRIDE model of threats discussed above and the corresponding mitigation could be the application of cybersecurity controls as illustrated in our logical security layered concept and in addition, a simple verification penetration testing result was presented. For future papers, we will discuss the application of our unique Logical Security Layered Concept presented in section H, figure 8 to other automotive systems to ensure security-by-design as well as our adopted approach in this paper

Recommendation

For future papers, we will discuss the application of our unique Logical Security Layered Concept presented in section H, figure 8 to other automotive systems to ensure security-by-design as well as our adopted approach in this paper.

References

1. "Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems." Accessed on 2022.04.21.

2. "The east-adl architecture description language for automotive embedded software springerprofessional.de." https://www.springerprofessional.de/en/11-the-east-adlarchitecture-description-language-for-automotive/3381892, note=Accessed on 2022.03.17.

3. T. Zhang, "Toward Automated Vehicle Teleoperation: Vision, Opportunities, and Challenges," 2020.

4. S. Bensoussan and M. Parent, "Computer-aided teleoperation of an urban vehicle," *1997 8th International Conference on Advanced Robotics. Proceedings. ICAR'97*, pp. 787–792, 1997.

5. M. Bout, A. Pernestål, M. Klingegård, A. Habibovic, and M.-P. Böckle, "A head-mounted display to support teleoperations of shared automated vehicles," pp. 62–66, 09 2017.

6. J. Feiler, S. Hoffmann, and F. Diermeyer, "Concept of a control center for an automated vehicle fleet," *2020 IEEE 23rd International Conference on Intelligent Transportation Systems, ITSC 2020*, 9 2020.

7. I. B. BRUSTEIN and JOSHUA, "Waymo's long-term commitment to safety drivers in autonomous cars," Jan 2020.

8. S. Lichiardopol, "Figure 17 from a survey on teleoperation: Semantic scholar," Jan 1970. Accessed on 29.03.2022.

9. C. Kettwich, A. Schrank, and M. Oehl, "Teleoperation of highly automated vehicles in public transport: User-centered design of a human-machine interface for remote-operation and its expert usability evaluation," 05 2021.

10. "In-vehicle commerce opportunities drive total connected cars to exceed 775 million by 2023." Accessed on 2022.04.13.

11. M. Scalas and G. Giacinto, "Automotive cybersecurity: Foundations for next-generation vehicles," in *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*, pp. 1–6, 2019.

12. D. R. Roberto Minerva, Abyi Biru, "Towards a definition of the internet of things (iot)." Accessed on 2022.04.13.

13. E. K. Wang, V. Profile, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui, K. P. Chow, and O. M. A. Metrics, "Security issues and challenges for cyber physical system: Proceedings of the 2010 ieee/acm int'l conference on green computing and communications & int'l conference on cyber, physical and social computing," Dec 2010. Accessed on 2022.04.13.

14. R. Anderson, 2008. Accessed on 25.07.2022.

15. R. S. Ross, M. McEvilley, and J. C. Oren, "Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems — nist," 2016.

16. K. C. Toth, A. Cavoukian, and A. Anderson-Priddy, "Privacy by design identity architecture using agents and digital identities," in *APF*, 2020.

17. Accessed on 2022.04.11.

18. D. Geer, "Are companies actually using secure development life cycles?," 07 2010. Accessed on 2022.04.11.

19. Accessed on 2022.04.11.

20. N. Khan and N. Ikram, "Security requirements engineering: A systematic mapping (2010-2015)," pp. 31–36, 08 2016. Accessed on 2022.04.12.

21. D. S. H. S. e. a. Mutzenich, C., "Updating our understanding of situation awareness in relation to remote operators of autonomous vehicles." Accessed on 2022.02.07.

22. Research and Markets, "Global teleoperation and telerobotics market (2021 to 2026) - by technologies, solutions and applications," 2021. Accessed on 2022.02.08.

23. "Home - project savor."

24. J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," *Ad Hoc Networks*, vol. 90, p. 101823, 2019. Recent advances on security and privacy in Intelligent Transportation Systems.

25. M. Hashem Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 45–51, 2017.

26. J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015.

27. G. De La Torre, P. Rad, and K.-K. R. Choo, "Driverless vehicle security: Challenges and future research opportunities," *Future Generation Computer Systems*, vol. 108, pp. 1092–1111, 2020.

28. Ángel Manuel Guerrero-Higueras, N. DeCastro-García, and V. Matellán, "Detection of cyber-attacks to indoor real time localization systems for autonomous robots," *Robotics and Autonomous Systems*, vol. 99, pp. 75–83, 2018. Accessed on 2022.04.22.

29. J. A. Jaskolka and J. Villasenor, "Identifying implicit component interactions in distributed cyber-physical systems," 2017. Accessed on 2022.04.22.

30. "Gellish: A generic extensible ontological language — ios press." https://www.iospress.com/catalog/books/gellish-a-generic-extensible- ontological-language, note = Accessed on 2202.1.23.

31. M. R. Abedi, N. Mokari, H. Saeedi, and H. Yanikomeroglu, "Robust resource allocation to enhance physical layer security in systems with full-duplex receivers: Active adversary," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 885–899, 2017.

32. S. Karnouskos and F. Kerschbaum, "Privacy and integrity considerations in hyperconnected autonomous vehicles," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 160–170, 2018.

33. J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015.

34. A. Khalid, P. Kirisci, Z. H. Khan, Z. Ghrairi, K.-D. Thoben, and J. Pannek, "Security framework for industrial collaborative robotic cyber-physical systems," *Computers in Industry*, vol. 97, pp. 132–145, 2018. Accessed on 2022.04.22.

35. L. Monostori, "Cyber-physical production systems: Roots, expectations and r&d challenges," *Procedia CIRP*, vol. 17, p. 9–13, 12 2014.

36. R. Mishra, A. Singh, and R. Kumar, "Vanet security: Issues, challenges and solutions," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 1050–1055, 2016.

37. C. Kettwich, A. Schrank, and M. Oehl, "Teleoperation of highly automated vehicles in public transport: User-centered design of a human-machine interface for remote-operation and its expert usability evaluation," May 2021.

38. "collaborative control a robot-centric model for vehicle teleoperation." Accessed on 2022.04.26.

39. J.-M. Georg, J. Feiler, F. Diermeyer, and M. Lienkamp, "Teleoperated driving, a key technology for automated driving? comparison of actual test drives with a head mounted display and conventional monitors," in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, pp. 3403–3408, 2018. Accessed on 2022.04.26.

40. "Cybersecurity guidebook for cyber-physical vehicle systems - sae international."

41. "Iso/sae 21434:2021," Aug 2021.

42. "The essential guide to iso/sae 21434. out now!." Accessed on 2022.02.08.

43. "Proposal for a new un regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system." https://unece.org/fileadmin/DAM/trans/doc/2020/wp29grva /ECE-TRANS-WP29-2020-079-Revised.pdf.

44. Accessed on 13.10.2022.

45. D. S. Fowler, "Project bearcat : Baselining, automation and response for cav testbed cyber security : Connected vehicle amp; infrastructure security assessment," Mar 2020.

46. K. Sowka, L.-P. Cobos, A. Ruddle, and P. Wooderson, "Requirements for the automated generation of attack trees to support automotive cybersecurity assurance," Mar 2022.

47. A. Ruddle, B. Weyl, S. Idrees, Y. Roudier, M. Friedewald, T. Leimbach, A. Fuchs, S. Gürgens, O. Henninger, R. Rieke, M. Ritscher, H. Broberg, L. Apvrille, R. Pacalet, and G. Pedroza, "Security requirements for automotive on-board networks based on dark-side scenarios. deliverable d2.3: Evita. e-safety vehicle intrusion protected applications," *Fraunhofer ISI*, 01 2009.

48. S. Mahmood, H. N. Nguyen, and S. A. Shaikh, "Systematic threat assessment and security testing of automotive over-the-air (ota) updates," *Vehicular Communications*, vol. 35, p. 100468, 2022.

49. M. Cheah, S. Shaikh, O. Haas, and A. Ruddle, "[pdf] towards a systematic security evaluation of the automotive bluetooth interface: Semantic scholar," Jan 1970.

50. J. Dürrwang, J. Braun, M. Rumez, R. Kriesten, and A. Pretschner, "Enhancement of automotive penetration testing with threat analyses results," Nov 2018.

51. *Sparx Systems*.

52. "Syn flood attack: Variants and countermeasures."

Contact Information

Victormills Iyieke
iyiekev@coventry.ac.uk

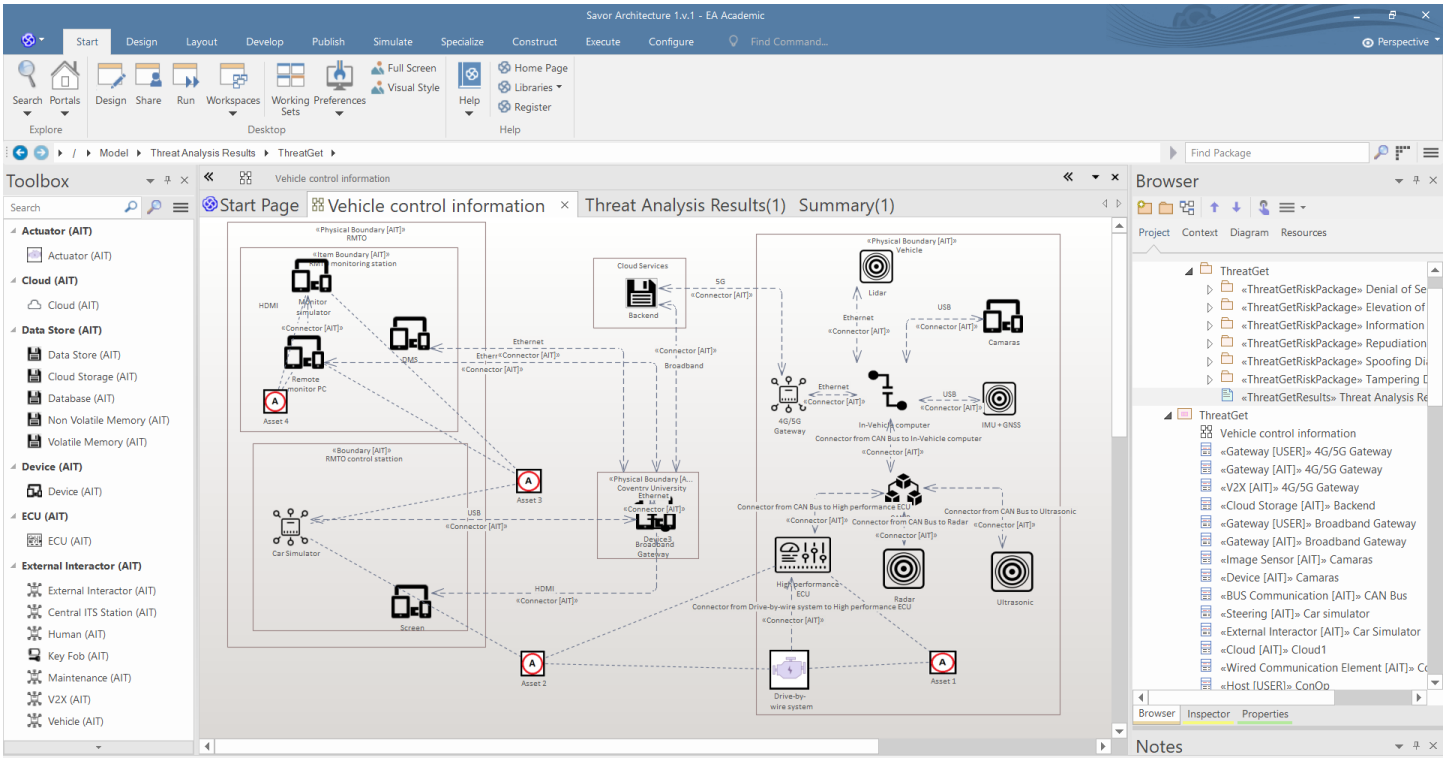
Acknowledgments

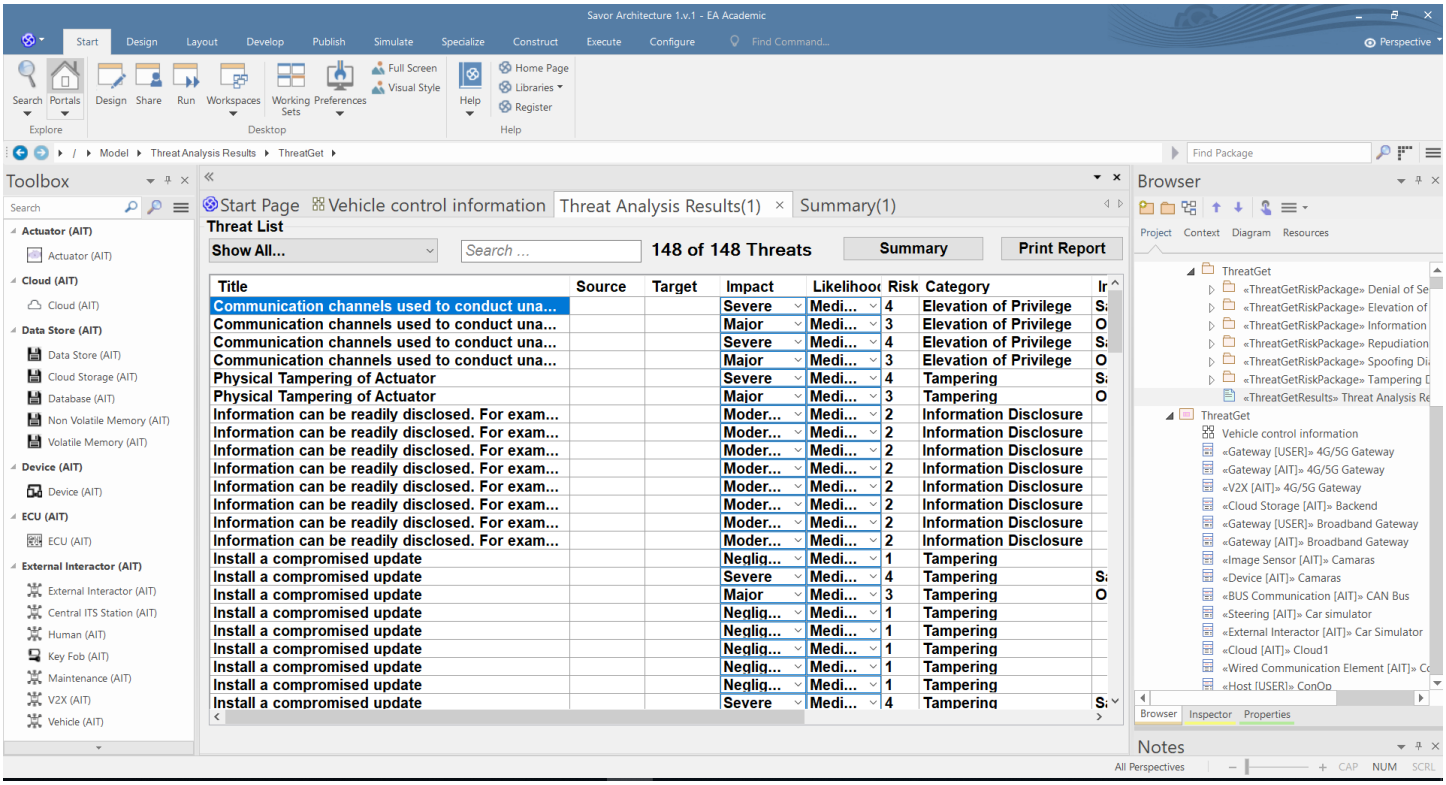
Part of this research was done in collaboration with CONIGITAL LTD under the project SAVOR (Safely Advancing Vehicle Automation On Roads) agreement under student PhD sponsorship. This publication reflects only the authors' view, exempting the CONIGITAL LTD from any liability.
This research has also benefitted from discussions with previous members of the Systems Security Group (SSG) such as; Prof Siraj Shaikh, Dr Hoang Nga Nguyen and Dr Giedre Sabaliauskaite at the Centre for Future Transport and Cities (CFTC) at Coventry University (UK).

Definitions, Acronyms, Abbreviations

RMTO - Remote Monitory and Teleoperation. TARA - Threat Analysis and Risk Assessment. AV - Autonomous Vehicle. SAVOR - Safely Advancing Vehicle Automation On Roads. DOS - Denial-of-service.

APPENDIX A





Screen short of the RMTO security architecture model in Enterprise Architecture utilising ThreatGet.

APPENDIX B

Threat Category	Threat Scenarios	Affected Element/Asset/Connection	Description	Impact Level	Risk value	Ref.	Top level security mitigation requirment	Total Threat category	Total Threat Scenarios
Tampering	Physical Tampering of Electronic Control Unit	High performance ECU, Vehicle control information	ECU may be manipulated by accessing the hardware	Severe	5	M9	R1. Measure to prevent and detect unauthorised access shall be employed.	11	2
	Install a compromised update	Monitor simulator, Vehicle location 1 & 2, Remote monitor PC, High performance ECU, Vehicle control information 1 & 2.	Compromise the software or firmware updates process locally includes fabricating system update programs or firmware, could have a negative consequence on the critical points in the vehicle. This includes fabricating system update program or firmware.	Severe	4	M16	R2. Secure Software update procedures shall be employed.		6
	Physical Tampering of Actuator	Drive-by-wire system, Vehicle control information 1 & 1	An attacker could tamper critical units inside the vehicle, particularly the actuators. This could lead to different potential consequences, such as affect the safe operation of the car and other critical safety issues	Severe	4	M9	R3. Measure to prevent and detect unauthorised access shall be employed		2
	Physical loss of data can occur	High performance ECU, Vehicle control information	Damage caused by a third party. Sensitive data may be lost or compromised due to physical damages in cases of traffic accident or theft. Loss from DRM (digital right management) conflicts. User data may be deleted due to DRM issue. The (integrity of) sensitive data may be lost due to IT components wear and tear, causing potential cascading issues (in case of key alteration, for example).	Severe	4	M24	R4. Best practices for the protection of data intergrity and confidentiality shall be followed for storing personal data.		1
Repudiation	Man in the middle attack	CAN Bus; High performance ECU; Vehicle control information 2; Remote monitor PC; Monitor simulator; Vehicle location 2; HDMI; Drive-by-wire system;	Man in the middle attack attempts to access the vehicle system illegally by directly influencing the vehicle network across the communication networks. This attack could directly affect the confidentiality and integrity of the vehicle's data.	Severe	4	M10	R5. The vehicle shall verify the authenticity and intergrity of massages it receives.	4	3
	Manipulation of vehicle parameters	High performance ECU; vehicle control information 2	Unauthorized access of falsify the configuration parameters of vehicle's key functions, such as brake data, airbag deployed threshold, etc. Unauthorized access of falsify the charging parameters, such as charging voltage, charging power, battery temperature, etc.	Severe	4	M9	R6. Measures to prevent and detact unauthorized access shall be employed.		1
Denial of service	Disruption of systems or operations	High performance ECU; vehicle control information; Monitor simulator; Vehicle location;Remote monitor PC, Car simulator; Drive-by-wire system.	Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging.	Severe	4	M13	R7. Measures to detect and recover from a denial of service attack shall be employed.	6	5
	Cause the Target to Crash or Stop or disabling functions	Drive-by-wire system; High performance ECU;Vehicle control information	It is possible to launch a denial-of-service (DoS) attack against essential units within the vehicular network, which can have multiple consequences for the target, including the interruption of functionalities, malfunctioning or even decreasing its performance (i.e., performance degradation). In all circumstances, failing to ensure the availability of critical units in a vehicle, such as the ECU, could result in various adverse outcomes.	Severe	3	M13	R8. Measures to detect and recover from a denial of service attack shall be employed.		1
levation of Privileg	Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data.	Drive-by-wire system; High performance ECU;Vehicle control information 2; CAN Bus; High performance ECU	Communications channels permit code injection, for example tampered software binary might be injected into the communication stream. Communications channels permit manipulate, eresure, overwriten and introduction of vehicle held data/code.	Severe	4	M7	R9. Access control techniques and designs shall be applied to protect system data/code.	10	4
	Gain access to ECUs or gain higher privileges.	High performance ECU; Vehicle control information 1 & 2;	Gain access to ECUs or obtain higher privileges could be happening by using remainders from development (e.g., debug ports, JTAG ports, microprocessors, software certificates, developer passwords, etc.).	Severe	4	M8 M9	R10. The system design and access control should not be possible for unauthorised personnel to access personal or system critical data. R11. Measures to prevent and detect unauthorised access shall be employed.		2
	Manipulation of vehicle data/code	Remote monitor PC; RMTO monitoring station; Vehicle location 2; Monitor simulator; Vehicle; High performance ECU; Vehicle control information 2; Drive-by-wire system;	Illegal/unauthorised changes to vehicle's electronic. Identity fraud. For example if a user wants to display another identity when communicating with toll systems, manufacturer backend. Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs. Data manipulation to falsify vehicle's driving data (e.g. mileage, driving speed, driving directions, etc. Unauthorised changes to system diagnostic data.	Severe	4	M10 M8 M7 M10	R12. The vehicle shall verify the authenticity and integrity of massages it received. R13. The system design and access control should not be possible for unauthorised personnel to access personal or system critical data. R14. Access control techniques and designs shall be applied to protect system data/code. R15. The vehicle shall verify the authenticity and integrity of massages it receives.		4