CHALMERS
UNIVERSITY OF TECHNOLOGY

Gap analysis of ISO/SAE 21434 – Improving the automotive cybersecurity engineering life cycle

Downloaded from: https://research.chalmers.se, 2024-03-20 12:25 UTC

Citation for the original published paper (version of record):
Grimm, D., Lautenbach, A., Almgren, M. et al (2023). Gap analysis of ISO/SAE 21434 – Improving the automotive cybersecurity engineering life cycle. 2023 IEEE 26th International Conference on Intelligent Transportation Systems (ITSC): 1904-1911.
http://dx.doi.org/10.1109/ITSC57777.2023.10422100

N.B. When citing this work, cite the original published paper.

© 2023 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, or reuse of any copyrighted component of this work in other works.

This document was downloaded from http://research.chalmers.se, where it is available in accordance with the IEEE PSPB Operations Manual, amended 19 Nov. 2010, Sec, 8.1.9. (http://www.ieee.org/documents/opsmanual.pdf).

(article starts on next page)

Gap analysis of ISO/SAE 21434 – Improving the automotive cybersecurity engineering life cycle

Daniel Grimm*, Aljoscha Lautenbach†‡, Magnus Almgren†, Tomas Olovsson† and Eric Sax*
* *Institut für Technik der Informationsverarbeitung (ITIV), Karlsruhe Institute of Technology*, Karlsruhe, Germany
daniel.grimm@kit.edu, eric.sax@kit.edu
† *Chalmers University of Technology*, Gothenburg, Sweden
aljoscha@chalmers.se , magnus.almgren@chalmers.se, tomas.olovsson@chalmers.se
‡ *Evidente AB*, Gothenburg, Sweden
Aljoscha.Lautenbach@evidente.se

***Abstract*— This is the authors' version of this paper, including an additional appendix and acknowledgements that did not have space in the original paper. The final authenticated version of this paper is copyrighted by IEEE and is available online at https://doi.org/10.1109/ITSC57777.2023.10422100.**

Due to the ongoing legislative shift towards mandated cybersecurity for road vehicles, the automotive cybersecurity engineering standard ISO/SAE 21434 is seeing fast adoption throughout the industry. Early efforts are focusing on threat analysis and risk assessment (TARA) in the concept and development phases, exposing the challenge of managing TARA results coherently throughout the supply chain and life cycle. While the industry focuses on TARA, other aspects such as vulnerability or incident handling are receiving less attention. However, the increasing threat landscape makes these processes increasingly important, posing another industry challenge.

In order to better address these two challenges, we analyze the cybersecurity engineering framework of ISO/SAE 21434 for gaps or deficiencies regarding TARA management and vulnerability and incident handling, as well as similar processes for incident handling in IT security. The result is a proposal for modifications and augmentations of the ISO/SAE 21434 cybersecurity engineering framework. In particular, we propose a TARA management process to facilitate the coordination and information exchange between different systems and life cycle phases, and we propose improvements to the vulnerability and incident handling processes in ISO/SAE 21434 so that they are more aligned with established standards. This amounts to 13 new terminology definitions, 4 new process steps, 2 modified process steps and 1 entirely new process.

I. Introduction

With the increasing automation of vehicles and the introduction of external communication, cybersecurity engineering becomes indispensable. For this reason, UN Regulation 155 (UNR 155) [22] came into force in 2022, mandating that manufacturers demonstrate that they consider cybersecurity throughout the life cycle. According to a UNECE interpretation document for UNR 155 [21], compliance with the ISO/SAE 21434 [12] cybersecurity engineering standard is a good way to ensure at least partial compliance with UNR 155. ISO/SAE 21434 introduces a cybersecurity engineering framework, and a key component is a threat analysis and risk assessment (TARA) methodology, which has been addressed in various publications, e.g. [14, 5].

UNR 155 requires that risks are managed throughout the supply chain and are kept up to date (cf. 5.1.1. (a) and 7.2.2.2. (f) [22]). The management of TARA throughout the supply chain and life cycle is a significant challenge (cf. sec. III-A). One challenging aspect is the information exchange between vehicle manufacturers (OEM) and the multi-tier supply industry [13]. This exchange needs to be carefully managed, as risk assessment of a vehicle is difficult without detailed knowledge about suppliers' components. Another challenging aspect is that new information or changes to the vehicle or its environment may affect the risk assessment. Currently, ISO/SAE 21434 is not explicit in how to update TARA results.

Another significant challenge is the ability to react to new vulnerabilities and incidents, which is also required by UNR 155 (cf. 5.1.1. (d)). While such capabilities have been present in IT security for some time, in the automotive sector a standardized approach is not yet established. ISO/SAE 21434 covers aspects such as monitoring and vulnerability management, but compared to its TARA framework, these aspects lack details.

Aim: ISO/SAE 21434 has quickly been established in the industry. However, at least two significant challenges remain. In terms of the management of TARA throughout the life cycle and the supply chain, as well as in the response to vulnerabilities and incidents, the standard should be improved and extended.

Method: Practical experience in the application of TARA is compared with ISO/SAE 21434 to reveal the shortcomings in the standard. Furthermore, we analyze approaches to incident response in IT security, such as the NIST SP 800-61 [3] and CMU/SEI-2004-TR015 [1], to identify gaps to ISO/SAE 21434 regarding continual cybersecurity engineering.

Contribution: We present a methodological gap analysis to identify and discuss challenges and issues, based on which we propose two major improvements to ISO/SAE 21434 that could be incorporated in future versions of the standard:

- A novel management process for TARA to improve risk management over the life cycle and supply chain.
- A revised process for identifying and responding to vulnerabilities and attacks that is better aligned with established processes and more practically feasible.

II. Background: Incident handling in IT security

Processes from IT are increasingly important for automotive applications, as vehicles are becoming smartphones on wheels. Since incident handling has been applied in IT security for over 20 years, they are a relevant subject for inspiration. We describe CMU/SEI-2004-TR01 [1][1] and NIST SP 800-61 [3], to contrast their approaches with automotive practices.

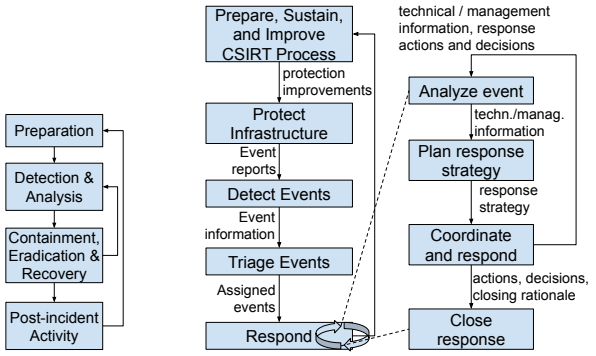
SP 800-61 [3] describes a four-step process (cf. fig. 1a). *Preparation* includes preventive measures to avoid incidents through application of risk assessment, implementation of security measures, user training, and preparations to handle incidents. Resources and tools are prepared, including contact information of relevant people, forensic software, and technical resources for analysis. *Detection & analysis* considers information sources for potential incidents, e.g. intrusion detection system alerts, logs, and public vulnerability information. The analysis includes validation and initial analysis, prioritization, documentation, and notification of relevant actors. The initial analysis should determine a rough scope of the incident to appropriately prioritize and, if necessary, analyze the incident further. The third step includes *containment* to reduce the damage, *eradication* to eliminate the incident, and finally *recovery* to return to normal operations. A re-iteration of the analysis phase is often required to resolve all problems. *Post-incident activity* involves "lessons learned" meetings and collecting subjective and objective measures (e.g., number of incidents handled, time per incident). The identified improvements for incident handling are fed back into *preparation*.

In 2004-TR01 [1] (cf. fig. 1b), the post-incident analysis takes place in the *prepare, sustain and improve* step. It also contains a process for creating an incident response capability from scratch. The subsequent *protect* step is similar to the *prevent incidents* sub-step in the preparation phase of NIST SP 800-61, i.e. ensuring that industry best practices are followed. The *detect events* phase monitors infrastructure and collects external reports, and forwards potential incidents. An initial analysis consisting of validation, filtering and prioritization takes place in a separate *triage events* step. The *respond* phase is iterative with three sub-phases, until the incident is closed. Main goals are to understand the incident, contain it and recover to normal operating conditions, similar to the third phase in NIST SP 800-61. The iterative response phase consists of a detailed analysis, where additional information may be collected, and the response will be planned, coordinated and executed. Relevant information for post-mortem analysis is fed back to the *prepare, sustain, and improve* phase.

III. Gap analysis of ISO/SAE 21434

In the following, we analyze ISO/SAE 21434 from two angles: issues that arise when applying (1) the standard's TARA framework, and (2) the standard's vulnerability and incident handling processes. The issues related to (1) have been identified through several years of experience of the authors working in industry projects, including personal observations as well as many discussions with industry practitioners in at least 7 automotive companies. There is less automotive experience regarding vulnerability and incident handling, so the issues related to (2) have been identified by analyzing related standards and literature and comparing them to ISO/SAE 21434.

[1]abbreviated as 2004-TR01 from here on



(a) NIST SP 800-61 (b) CMU/SEI-2004-TR01

Fig. 1: IT security incident management and handling processes

A. TARA throughout a vehicle's life cycle

ISO/SAE 21434 leaves the TARA methodology to the standard's adopter. Currently, most automotive companies use own adaptations. As experience with TARA increases, common problems have become apparent to industry practitioners. Most of those problems are either related to inconsistent evaluation or to the complex ecosystem of the industry.

1) Abstraction level of TARA: TARA can be done on several levels of abstractions (cf. [5, 15]). ISO/SAE 21434 supports this claim: it states that TARA methods are "generic modules that can be invoked systematically, and from any point in the life cycle of an item or component" [12]. However, ISO/SAE 21434 is not explicit on which levels TARA should actually be applied. A vehicle-level TARA can only cover high-level threats, while more detailed analysis is pushed to the TARA of components and sub-components. Similarly, in the development phase TARA has to adapt to the architectural levels of abstraction as they develop. Therefore, one challenge is to find the right level of abstraction and the correct component or sub-component. *CHALLENGE A1: Identifying the correct level of abstraction for TARA.*

2) Distributed development: Additional problems occur once distributed development is considered, i.e., the work distribution and sharing of information between suppliers and their customers[13, 9]. It begins with the question of whether a component is developed out-of-context which allows the supplier to develop it using generic assumptions about its operating environment, or if it is considered in-context. Then, who is responsible for performing the TARA? The supplier, the customer, or both? And how much information can be shared between the two? TARA results are sensitive, but

some of the results need to be shared with selected parties. Even within an organization this can lead to problems if different teams are responsible for different parts of a TARA. Moreover, if information is shared, how do you ensure it is compatible? To the best of our knowledge, no common TARA exchange format exists. *CHALLENGE A2: Deciding how and what sensitive TARA information to share between customers and suppliers, and within an organization.*

Finally, how do you ensure consistency among different TARAs, both within a single organization, but also across organizations? Which template and methodology will be used to perform the TARA? *CHALLENGE A3: Keeping TARA outcomes consistent within and across organizations.*

3) Complementary cybersecurity requirements: Another potential problem is that the TARA may overlook complementary cybersecurity requirements in support of the continual cybersecurity activities or legal requirements, such as cybersecurity monitoring or forensic capabilities. These requirements must be considered in organizational policy and processes to ensure that required cybersecurity information is monitored for and collected. *CHALLENGE A4: Identifying complementary cybersecurity requirements.*

4) Keeping TARA up-to-date: UNR 155 mandates a process "for ensuring that the risk assessment is kept current" [22]. ISO/SAE 21434 applies the TARA during the concept phase, and only mentions in a side note that threat scenarios can be updated during event evaluation. When are the other artifacts of TARA updated? How can an update of the TARA be implemented, and what information is required for it? *CHALLENGE A5: Keeping TARA up-to-date.*

B. Vulnerability and incident handling in ISO/SAE 21434

ISO/SAE 21434 mandates capabilities for vulnerability and incident handling (cf. sec. I). While the automotive industry is gaining experience in the application of these processes, issues become apparent when comparing with the experience from the more mature IT security industry. Established procedures for incident handling (cf. sec. II) indicate possible improvements for ISO/SAE 21434, including improvements of terminology, process scope, and process workflow.

1) Terminology: Even in IT security, there is no commonly agreed upon incident handling terminology, and yet there are commonalities which ISO/SAE 21434 deviates from. Issue B1: *Terminology for events, incident, incident response plan and triage deviates from established terminology.*

Events. A "security event" is often defined as "an occurrence in a system" that may be security relevant. In contrast, ISO/SAE 21434 defines a cybersecurity event as "cybersecurity information that is relevant for an item or component". Note that according to this definition, an event refers to information, whereas the common definition of "an occurrence in a system" is concretely tied to a system state.

Incident. An "incident" is typically defined similar to "a security event that involves a security violation", whereas ISO/SAE 21434 defines a cybersecurity incident as a "situation in the field that can involve vulnerability exploitation". If "in the field" means "during operations", this definition excludes incidents that happen during development.

Incident response plan. In ISO/SAE 21434 the term incident response plan is to be understood as a per-incident document. In contrast, in the NIST standard the response plan is an overarching strategy and "roadmap for implementing the incident response capability", which also includes metrics for the measurement of that capability.

Triage. As used in ISO/SAE 21434, the term triage is not consistent with the literature. In IT security, the aim is to give the worst incidents the most attention. In ISO/SAE 21434, triage is not used as a term for prioritization which would require a classification or rating, but only for filtering. Issue B2: *Triage does not include prioritization.*

2) Process workflow: Firstly, both 2004-TR01 and NIST SP 800-61 describe the need to prepare for vulnerability and incident handling, including preparing necessary information, a step missing in ISO/SAE 21434. Issue B3: *There is no explicit preparation for incident or vulnerability handling.*

Secondly, incident response is iterative in both NIST SP 800-61 and 2004-TR01. Often, several steps are required to first achieve containment, then eradication, and finally recovery of operations. Moreover, a verification of the effectiveness of the response is performed to decide if an iteration is required. In contrast, ISO/SAE 21434 does not suggest an iterative process. Concrete response actions, such as eradication and recovery, are not part of ISO/SAE 21434. Issue B4: *Incident handling is not iterative.*

An incident or vulnerability handling follow-up ("lessons learned") is another concern. In NIST SP 800-61, post-incident activity is one of the four main phases, emphasizing its importance. 2004-TR01 performs post-incident analysis in the sustain and improve phase to derive requirements for process and technology improvements. In ISO/SAE 21434, learning from previous experiences is covered in [RQ-05-08] as part of cybersecurity culture. However, more guidance of how to integrate this into the continual cybersecurity processes would be beneficial. Issue B5: *There is no post-analysis after incident or vulnerability handling.*

3) Vulnerability and incident handling time frame and interaction: The vulnerability and incident handling process in ISO/SAE 21434 focuses on analysis and resolution of vulnerabilities. Incident handling is only to be invoked as part of vulnerability management, which does not cover all cases. In particular, once cybersecurity monitoring matures, it may be more common that incidents are detected before vulnerabilities, and in those cases incident containment should be more critical than finding the underlying vulnerability. Notice that incident handling may require a higher degree of urgency. Issue B6: *Incident handling may require immediate action, but can only be invoked from within vulnerability handling, and vulnerability handling can not be triggered from incident handling.*

IV. Proposal of a TARA management process

To address the challenges discussed in sec. III-A, we propose a new supporting "TARA management process":

Def. 1. TARA management process: The process of brokering access to and coordinating work on TARA artifacts required for an item, including the coordination of distributed development activities and the definition of appropriate abstraction levels.

Conceptually, it is a continual cybersecurity activity because it spans the entire life cycle of a project and defines an organizational interface for exchanging TARA information across projects. In the following, we describe how this addresses the problems of distributed and multi-level development.

A. Multi-level TARA for cybersecurity engineering

An elementary component of our proposed approach, addressing A1, is to refine TARA over several levels, which we adopt from Dobaj et al. [5]. At the concept level, the technical realization is not yet available, so a TARA can only lead to high-level cybersecurity goals. As soon as the development process proceeds to component or sub-component design, a more detailed TARA can be performed. However, the level of detail required can no longer be represented in a single diagram. A single data flow diagram, which is often used for TARA, would be insufficient to adequately describe a vehicle. Thus, a multitude of diagrams, per component or sub-component, and possibly additional diagrams for modes or variants of the components, must be generated. This requires a management process that governs tracking of the artifacts.

Fig. 2 depicts the interfaces of the TARA management process with the TARA artifacts, including the refinement steps. The cybersecurity concept on level $n+1$ is a refinement of the cybersecurity concept on level n. The TARA management process tracks the refinements of the artifacts. Most TARA artifacts are project specific, but the TARA management process has an organization-wide scope, allowing for information exchange and artifact reuse between projects.

B. Distributed cybersecurity

Another challenge that the management process addresses is the interaction with suppliers. Information shared between customers and suppliers is typically kept to the bare minimum. However, in order to arrive at an accurate risk assessment, certain information must be shared, such as the operational or assumed context, or assumed steps of an attack path. The TARA management process must therefore coordinate which information is shared with suppliers and when. The information to be shared and how to share it should be explicitly specified in the cybersecurity interface agreement, as also suggested by Kiening et al. [13]. If results are also to be shared, the interface agreement should further include which methodology is to be used to derive the results. This partly addresses A2 and A3. In contrast to functional safety, the cybersecurity interface agreement needs to cover a long-lived relationship beyond development (cf. sec. IV-D).

C. TARA management as artifact access broker

The management process also governs access to TARA artifacts, specifically it should outline who has access to which parts of the TARA under which circumstances. As such, it acts as an *artifact access broker* to other processes, such as vulnerability and incident handling (see fig. 2), also helping to address A2.

D. TARA management is a continual activity

Over the life cycle of a vehicle, the TARA artifacts cannot be considered static, so the TARA management process must be continual. This helps to address A5. Fig. 2 shows the relationships of the continual activities from ISO/SAE 21434 with the TARA management process. They depict a subset of our proposed continual security activities (cf. sec. V). TARA updates, as shown in the diagram with arrows pointing in the direction of the management process, are required in several cases, e.g. when a software or hardware update is developed.

TARA updates may also be required based on vulnerability handling findings, since new weaknesses or vulnerabilities directly influence risks. There are two cases to consider:

1) There is at least one attack path known in which the weakness may be exploited, or
2) there is no known attack path that includes the weakness.

In the first case, the attack feasibility rating and risk rating are updated if needed. The second case indicates that a threat was overlooked.

Incident handling can also provide new insights to the TARA, in particular regarding assumptions of exploitability and impact. Mapping events to TARA artifacts is not trivial, since the type of monitored cybersecurity information determines if it affects an attack path or a damage scenario. If the event affects an attack path, the same options apply as for updating TARA artifacts based on new weaknesses. Similarly, two cases can be distinguished for damage scenarios:

1) There is at least one known damage scenario in which the event may be an observable indicator, or
2) there is no known damage scenario related to the observed event.

In the first case, an update of the impact rating takes place. In the second case, a new damage scenario and potentially a new threat scenario with associated risk value must be added.

Finally, the new step of post-analysis may provide information about frequent sources for weaknesses or recent or typical attack modes. Since risk ratings are based on assumptions about frequency and difficulty, post-analysis may yield updates of assumptions based on real-world observations. It may also reveal additional complementary cybersecurity requirements, thus partly addressing A4.

V. Proposal for modifications and augmentations of continual cybersecurity activities

To address the issues discussed in sec. III-B, we propose modifications and augmentations of the continual cybersecurity activities in ISO/SAE 21434, including changes to

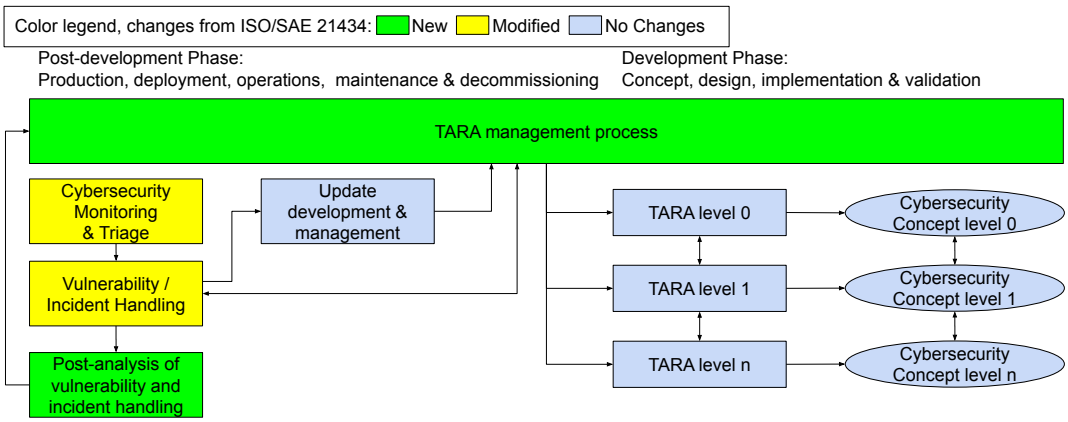


Fig. 2: TARA management process

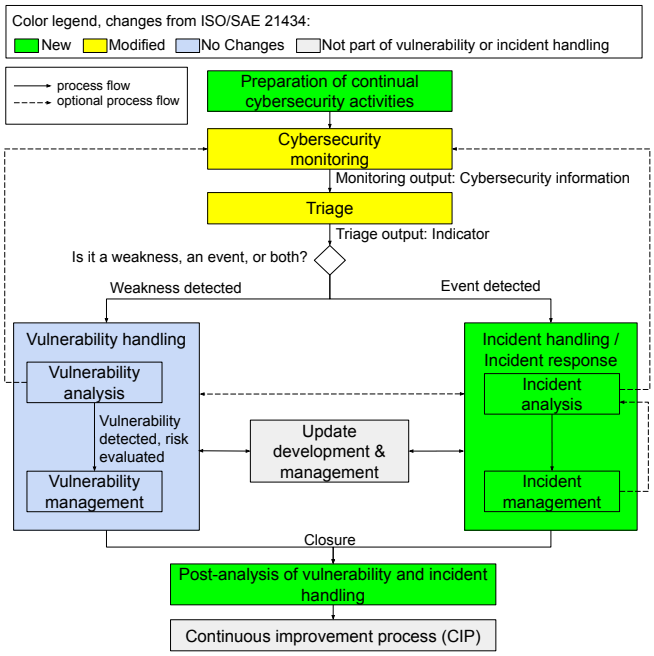


Fig. 3: Proposed vulnerability and incident handling processes

terminology and processes. To align the terminology with similar standards in IT security, we propose updates to the terms of *cybersecurity event*, *cybersecurity incident*, as well as the introduction of the term *cybersecurity indicator* (cf. sec.V-A). Furthermore, the need for a new process that separates the delimitation of vulnerability handling and incident handling is addressed by our proposal depicted in fig. 3. The rationale and procedure will be explained in sec. V-B.

A. Terminology: events, incidents and indicators

To address B1 (cf. sec. III-B.1), some term definitions need to be discussed. Since the terms *vulnerability*, *weakness* and *cybersecurity information* are in close alignment with similar standards, they are retained unchanged. Since cybersecurity information is not usually defined, for completeness we repeat its definition from ISO/SAE 21434:

Def. 2. Cybersecurity information: Information with regard to cybersecurity for which relevance is not yet determined.

However, the terms *cybersecurity event*, *cybersecurity incident*, and *cybersecurity indicator* should be redefined. A full discussion of related standards and guidelines is out of scope, but we compiled tables listing definitions from six different sources in the appendix, cf. tables II, III, IV, V.

While in ISO/SAE 21434 a *cybersecurity event* is generically cybersecurity information that is relevant to an item or component, IT security related documents define events in terms of *an occurrence in a system*. "Relevant cybersecurity information" could be a recently discovered vulnerability in software, but that would not fulfill the definition of an event according to IT security terminology. We propose an adaptation of [19], which is used by CMU/SEI-2004-TR01 [1], and ISO/SAE 21434:

Def. 3. Cybersecurity event: An occurrence in an item / component that is relevant to the cybersecurity of the system.

This redefinition ties an event to something happening in a system, rather than being any kind of cybersecurity information. This makes an event a precursor to an incident, just like a weakness is a precursor to a vulnerability.

In ISO/SAE 21434, a *cybersecurity incident* is defined as a "*situation in the field that can involve vulnerability exploitation*", which we argue is both much too broad and much too narrow at the same time, depending on the interpretation of "can". In IT security, incidents have varied definitions, but a common theme is the concrete breach of a security policy, and it is often tied to security events. We propose the following redefinition:

Def. 4. Cybersecurity incident: A cybersecurity event that involves a violation of product cybersecurity, product safety or organizational cybersecurity policy.

By tying the incident to an event, it is tied to "an occurrence in a system", making it more concrete than the previous definition. By broadening the scope to organizational cybersecurity policy, it also accounts for breaches during development.

With the redefinition of cybersecurity event, there is no longer an overarching term for relevant cybersecurity infor-

mation. We do not challenge the usefulness of a term for this, since it can serve as an umbrella term for both events and weaknesses. We propose to use the term *cybersecurity indicator* for the same definition:

Def. 5. Cybersecurity indicator: Information with regard to cybersecurity that is relevant for an item or component.

B. Processes of continual cybersecurity activities

To address B3 through B6, a comprehensive update to the continual activities in ISO/SAE 21434 is proposed. The new process (cf. fig. 3) introduces preparation and post-analysis activities, and splits vulnerability and incident handling into separate processes. In addition, we rename and clarify "cybersecurity monitoring" and "event evaluation" to resolve B2.

1) Preparation: The new preparation step addresses B3. ISO/SAE 21434 indirectly requires preparation as part of [RQ-05-02] to [RQ-05-05]. However, it is beneficial to explicitly account for the preparation of processes, rules, capabilities and responsibilities for vulnerability and incident handling, because in the broader context of cybersecurity governance where it otherwise fits it may be overlooked.

Based on [3], for vulnerability & incident analysis, we recommend to prepare communication channels, required hardware and software, and access to vehicle configuration data. The resources should cover documentation of the vehicle's network architecture and protocols, operating systems, software, hardware, and its cybersecurity concept. IT security typically uses a network baseline to compare current against historical behavior. In the automotive sector, this would require a per-vehicle model or per-configuration baseline.

For incident management, we recommend to prepare an organization-level template for the incident response plan (cf. III-B.1). We expect that elements *a)* to *c)* of [RQ-13-01] in ISO/SAE 21434 require per-incident planning, whereas *d)* to *g)* can be prepared on an organizational level. Accordingly, the template should define: a method for collecting additional information on an incident, a method for determining progress, and criteria and actions for closing an incident.

2) Cybersecurity monitoring: In ISO/SAE 21434, *cybersecurity monitoring* means "collecting cybersecurity information and analysing it for triage based on defined triggers". We propose a slight scope change by separating triage into its own activity (cf. B2):

Def. 6. Cybersecurity monitoring: The process of collecting, pre-processing and formatting cybersecurity information for subsequent processing.

Pre-processing and formatting result in a uniform data format to facilitate human understanding and automatic processing. Depending on the source, different steps may be required to prepare the information for subsequent processing. For example, a vulnerability report may be parsed manually, whereas production data may be queried from a database.

ISO/SAE 21434 lists examples for internal and external data sources. Internal sources include TARA artifacts, vulnerability analysis results and "information from the field", e.g. vehicle logs, as mandated by UNR 155. Examples in ISO/SAE 21434 for external sources are researchers, commercial or non-commercial sources, suppliers, customers, and governments. One may differentiate between public and private external sources (cf. ISO 30111 [11]), where public sources include social networks, blogs, the dark web [8], etc., and private sources include white-hat hackers, bug bounty programs, closed-access threat sharing platforms such as Auto ISAC[2], and commissioned penetration testers. The distribution status of the information (i.e. public or private) has an implicit effect on the urgency to address it.

Fig. 3 has a feedback loop from vulnerability and incident handling back to cybersecurity monitoring, since new technical details may become available during the handling processes, such as details about the vulnerability or incident, or about additional sources to be monitored.

3) Triage: As discussed in III-B.1, in ISO/SAE 21434 triage does not include prioritization, which clashes with typical definitions. To solve B2, we propose the following definition:

Def. 7. Triage: The process of determining relevance of cybersecurity information and prioritization of resulting indicators to facilitate their appropriate handling.

In essence, we replace the *cybersecurity event evaluation* with *triage*. The input for triage is the pre-processed cybersecurity information, and it has three components: (1) determining relevance, (2) categorization and (3) prioritization. Determining relevance may include searching for or confirming affected assets, assessing confidence in the information source, or verifying the information. If the information is not relevant, i.e. not an *indicator* (cf. sec. V-A), it should still be archived to be analyzed in the continuous improvement process later. Once an indicator has been identified, it should be categorized as being a weakness, a cybersecurity event, or both. In line with [1], triage involves correlation, which groups new indicators with already categorized vulnerabilities or events. Prioritization may be based on metrics such as the number of affected vehicles or potential impact, e.g. a CVSS score. Because detailed information may still be missing, only a preliminary prioritization can be made. Categorization and prioritization may require updates during subsequent activities.

4) Vulnerability Handling: If the outcome of *triage* is a weakness, *vulnerability handling* is triggered. We only propose minor adjustments to ISO/SAE 21434 in this aspect. Vulnerability handling comprises vulnerability analysis and vulnerability management (cf. fig. 3):

Def. 8. Vulnerability handling: The process of performing vulnerability analysis and vulnerability management.

Def. 9. Vulnerability analysis: The process of identifying and assessing vulnerabilities from identified weaknesses, which includes performing the appropriate steps of threat analysis and risk assessment.

Def. 10. Vulnerability management: The process of tracking and treating cybersecurity vulnerabilities.

Vulnerability analysis investigates weaknesses to identify

[2] https://automotiveisac.com/

root causes and risks associated with exploitation, which requires interaction with the TARA management process. While the TARA is refined during development, we expect the reverse during vulnerability analysis: TARA updates require abstraction, from fine-grained to coarse. Vulnerabilities often boil down to a line of code that leads to a potential attack path. From such an attack path at the subcomponent level (detailed), tracking the TARA levels in the TARA management process can infer effects (threats) at the upper levels (e.g. system level). If the analysis detects a vulnerability for which no update is available, the attack should be included in cybersecurity monitoring, to observe potential exploitations. If active exploitation is indicated, vulnerability handling triggers incident handling since an immediate response may be necessary.

Vulnerability management includes vulnerability treatment and tracking its resolution. Implementing a solution, however, is done in the related process *update development and management*. Solutions could include the development of a software or configuration update for existing components, or integration of an available patch. The updated associated risks should determine the urgency of solution deployment.

5) Incident Handling: Incident handling is introduced as a separate process to tackle B6. It is triggered if the outcome of *triage* is an event. The incident response provisions in ISO/SAE 21434 are minimal. We propose an extension that loosely builds on NIST SP 800-61 [3] and 2004-TR01 [1]. Structurally similar to vulnerability handling, it is comprised of incident analysis and incident management:

Def. 11. Incident handling: The process of analysing and managing cybersecurity incidents.

Def. 12. Incident analysis: The process of identifying and assessing cybersecurity incidents from identified cybersecurity events.

Def. 13. Incident management: The process of tracking and treating cybersecurity incidents, including actions for containment, eradication or recovery.

The goal of incident analysis is not to find the root cause, but to understand an event in sufficient detail to determine if it indeed is an incident, and if it is, to collect enough information to be able to prepare a response. This may require additional data collection, for which there is a loop to cybersecurity monitoring.

Once an incident has been identified, incident management determines an action plan and tracks its progress. The actions should include a plan for containment, eradication, and recovery, or a subset that leads to full recovery. Actions may include temporary function degradation. It may also be necessary to come up with alternative, ad-hoc measures, especially if the initial remedial actions turn out to be unsuccessful. Incident handling is an iterative process and additional analysis may become necessary at any point. Accordingly, to address B4, a loop exists from incident management back to analysis (cf. fig. 3). As with vulnerability management, most remedial actions will go through *update and configuration management*.

Incident handling results in an implemented incident response plan, based on the template (cf. sec. V-B.1). Part of the template is a prepared procedure for the loop to monitoring to accelerate access to additional information. Actions, responsibilities, and communication strategy need to be planned and implemented per incident. If an incident is caused by a new vulnerability, vulnerability handling is triggered. In that case, incident and vulnerability handling can run in parallel, although a steady exchange of information is expected.

6) Closure and post-analysis of vulnerability and incident handling: Vulnerability or incident handling is closed when no further action is required, in particular when:

- The incident or vulnerability has been resolved with an update that was successfully rolled out and verified.
- The incident or vulnerability has not been fully resolved, but the accompanying risk is sufficiently low to decide that no further actions are required.
- The event or weakness has been judged as not being an incident or a vulnerability, respectively.

Closure triggers archiving and final notification of stakeholders. What needs to be archived is case-specific.

After closure, a meta-analysis of the processes and results should be performed, which addresses B5. One could argue that the continuous improvement process ([RQ-05-08]) already covers that, but we argue that a separate activity is needed to enable effective continuous improvement:

Def. 14. Post-analysis of vulnerability and incident handling: The process of analysing and measuring incident and vulnerability handling outcomes, including root cause analysis and efficiency measurements.

For post-analysis, we recommend a root cause analysis for incidents and vulnerabilities. For incidents, this is necessary if it was not performed during incident handling. The vulnerability's technical root cause should have been investigated already, but how it was introduced may not be known. This could reveal weaknesses in development or testing processes.

The second recommendation are measurements of process efficiency, process validation and threat intelligence. Appropriate organization-specific measures need to be defined, for example the duration to measure efficiency, measuring the number of identified vulnerabilities for validation, or categorizing the types of incidents for threat intelligence. Drawing conclusions to improve the processes and the vehicle's security architecture takes place in the subsequent continuous improvement process.

VI. Related Work

A number of works analyze the ISO/SAE 21434 standard and highlight practical implications. Macher et al. [16] summarized the draft version of the standard. Recently, Ebert and John present their experience in industrial practice, especially on TARA application [6]. Costantino et al. [4] analyzed the correlation of ISO/SAE 21434 with other standards. Gierl et al. [7] discuss the role of UNR 155 and ISO/SAE 21434 for road-worthiness assessments. Other publications address the challenges of applying TARA in distributed automotive development projects. Dobaj et al. [5] propose an iterative

development life cycle model, introducing threat modeling in different design phases from concept phase to detailed hardware and software design. They align with ISO/SAE 21434 and automotive SPICE and extend the threat model with different levels. Kiening et al. [13] discuss which TARA elements can be shared with suppliers as part of the cybersecurity interface agreement to analyze attack paths across multiple suppliers and exchange incident information. The HEAVENS 2.0 risk assessment model developed by Lautenbach et al. [14] updates the established HEAVENS model to conform with ISO/SAE 21434, including updates to calculations and workflows to adapt it to industry experience. Piątek [17] introduces a process to extend cybersecurity monitoring with safety monitoring. The work aims to align with NIST SP 600-81 [3]; in particular, safety of the intended functionality (ISO/PAS 21448) is considered. In contrast to the works above, we focus exclusively on the interactions of TARA artifacts within the automotive life cycle and supply chain, as well as the vulnerability and incident handling processes in the context of ISO/SAE 21434.

VII. Conclusion

There is a need for clear structures and guidelines around automotive cybersecurity engineering, and ISO/SAE 21434 is largely fulfilling that need. Nevertheless, there are aspects that can and should be improved, in particular around the interaction of TARA processes and other cybersecurity activities, such as vulnerability and incident handling. In line with this, we have proposed a new TARA management process and improvements to the vulnerability and incident handling processes in ISO/SAE 21434, building on existing IT standards and guidelines, as well as on research into TARA improvements. We expect that our proposed improvements will help automotive companies to better coordinate their cybersecurity activities, and that an adoption of the proposed terminology will lead to improved clarity in communication. Hopefully, they can be considered in future versions of ISO/SAE 21434.

Acknowledgements

This work was partially supported by the Swedish Civil Contingencies Agency (MSB) through the projects “RICS2” and “RIOT”, as well as by VINNOVA, the Swedish Governmental Agency for Innovation Systems through the CyReV project under Grant 2019-03071.

References

[1] Christopher J. Alberts et al. *Defining Incident Management Processes for CSIRTs: A Work in Progress*. Ed. by Carnegie Mellon University - Software Engineering Institute. 2004.

[2] N. Brownlee and E. Guttman. *Expectations for Computer Security Incident Response (RFC 2350)*. https://www.ietf.org/rfc/rfc2350.txt. 2000.

[3] Paul Cichonski et al. *Computer Security Incident Handling Guide*. Aug. 2012. DOI: https://doi.org/10.6028/NIST.SP.800-61r2.

[4] Gianpiero Costantino, Marco De Vincenzi, and Ilaria Matteucci. “In-Depth Exploration of ISO/SAE 21434 and Its Correlations with Existing Standards”. In: *IEEE Communications Standards Magazine* 6.1 (2022), pp. 84–92. DOI: 10.1109/MCOMSTD.0001.2100080.

[5] Jürgen Dobaj et al. “Towards a security-driven automotive development lifecycle”. In: *Journal of Software: Evolution and Process* n/a.n/a (2021), e2407. DOI: https://doi.org/10.1002/smr.2407.

[6] Christof Ebert and Jerome John. “Practical Cybersecurity with ISO 21434”. In: *ATZelectronics worldwide* 17 (Mar. 2022). DOI: 10.1007/s38314-021-0741-5.

[7] Mona Gierl, Reiner Kriesten, and Eric Sax. “Security Assessment Prospects as Part of Vehicle Regulations”. In: *SAFECOMP 2022 Workshops*. Ed. by Mario Trapp et al. Cham: Springer International Publishing, 2022, pp. 97–109.

[8] Fay Goldstein et al. “Monitoring Automotive Cyber Risks Throughout The Deep and Dark Web”. In: *escar 2021 EU*. Upstream Security. 2021.

[9] Simon Greiner et al. “A supplier’s perspective on threat analysis and risk assessment according to ISO/SAE 21434”. In: *escar 2022 EU*. 2022.

[10] Houssem Guissouma et al. “Lifecycle Management of Automotive Safety-Critical Over the Air Updates: A Systems Approach”. In: *IEEE Access* 10 (2022), pp. 57696–57717. DOI: 10.1109/ACCESS.2022.3176879.

[11] ISO/IEC. *ISO/IEC 30111 Information technology — Security techniques — Vulnerability handling processes*. Oct. 2019.

[12] ISO/SAE. *ISO/SAE 21434 Road Vehicles - Cybersecurity Engineering*. Aug. 2021.

[13] Alexander Kiening and Daniel Angermeier. “TRADE - Threat and Risk Assessment for Automotive Distributed Engineering”. In: *escar 2021 EU*. 2021.

[14] Aljoscha Lautenbach, Magnus Almgren, and Tomas Olovsson. “Proposing HEAVENS 2.0 – an Automotive Risk Assessment Model”. In: *Computer Science in Cars Symposium*. ACM, 2021. DOI: 10.1145/3488904.3493378.

[15] Thomas Liedtke. “Risk Assessment According to the ISO/SAE 21434:2021 – Experiences, Help and Pitfalls”. In: *escar 2021 EU*. 2021.

[16] Georg Macher et al. “ISO/SAE DIS 21434 Automotive Cybersecurity Standard - In a Nutshell”. In: *SAFECOMP 2020 Workshops*. Ed. by António Casimiro et al. Cham: Springer International Publishing, 2020, pp. 123–135.

[17] Piotr Piątek. “Incident Management Process Model for Automotive CyberSafety Systems Using the Business Process Model and Notation”. In: *2022 26th International Conference on Methods and Models in Automation and Robotics (MMAR)*. 2022, pp. 232–237. DOI: 10.1109/MMAR55195.2022.9874288.

[18] Christoph Schmittner et al. "A Preliminary View on Automotive Cyber Security Management Systems". In: *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. 2020, pp. 1634–1639. DOI: 10.23919/DATE48585.2020.9116406.

[19] R. Shirey. *Internet Security Glossary (RFC 2828)*. http://www.ietf.org/rfc/rfc2828.txt. 2000.

[20] The MITRE Corporation. *CWE Glossary*. https://cwe.mitre.org/documents/glossary/.

[21] UNECE. *Proposals for the Interpretation Documents for UN Regulation No. 155 (Cyber security and cyber security management system)*. Mar. 2021. URL: https://unece.org/sites/default/files/2021-02/ECE-TRANS-WP29-2021-059e_0.pdf.

[22] UNECE. *Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system*. Mar. 2021. URL: https://unece.org/sites/default/files/2021-03/R155e.pdf.

[23] UNECE. *Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system*. Mar. 2021. URL: https://unece.org/sites/default/files/2021-03/R156e.pdf.

[24] Moira West-Brown et al. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. 2nd Edition. 2003. DOI: 10.1184/R1/6574055.v1.

Appendix

The Automotive Development Life Cycle and ISO/SAE 21434 Cybersecurity Engineering

The automotive life cycle is usually conceptualized as several distinct phases, namely concept, product development, production, operations & maintenance, and decommissioning. Although agile development practices are increasingly common in automotive development projects, the overall product development approach uses a traditional V-model with stringent requirements engineering up-front in the concept phase and a strong focus on testing and validation before moving to production.

Fig. 4 shows how the phases of the life cycle (white blocks) are arranged along the V-model, and how they map to the different clauses in ISO/SAE 21434. The first three blocks form the concept phase in which the requirements are determined. After the system design phase, several parallel processes may be applied, e.g. for software, hardware and mechanical engineering. The development phase spans to the start of production, until validation and acceptance testing have been successfully completed. During the operations and maintenance phase, updates may be developed and deployed, e.g. to provide new or improved features, or to fix problems. Since the development of updates must also comply with the relevant standards and regulations, dedicated development life cycle models suitable for this purpose have been and are being researched [18, 10, 5].

Since modern vehicles are technically complex with dozens to hundreds of subsystems and several tiers of suppliers on all levels, development is broken down into more manageable projects, typically per subsystem. Each project usually includes several abstraction levels, such as vehicle, functional, system, software or hardware level. In distributed development with different suppliers, the meaning of an abstraction level may differ. For example, while for a customer the subsystem level can be a specific ECU, from the ECU supplier's point of view, the ECU is the entire system.

ISO/SAE 21434 defines a cybersecurity engineering framework that covers all aspects of the automotive life cycle. Fig. 4 depicts all the processes defined in the standard and places them in the corresponding life cycle phase. The dark blocks show which development life cycle phase is targeted by the corresponding clauses in the standard, while the gray blocks represent selected methods and the gray ellipses depict important work products. Despite the comprehensive nature of the standard, a particular focus is on the threat analysis and risk assessment processes (clause 15) to facilitate the exertion of appropriate effort towards the fulfillment of identified cybersecurity goals (cf. fig. 5). In addition, clause 9 covers the definition of a cybersecurity concept, containing the cybersecurity requirements and requirements on the operational environment on vehicle level functionality. Product development is covered by Clauses 10 and 11, which create the (detailed) cybersecurity specifications and reports for integration, verification, and validation, among other work products.

Clauses 5, 6, and 7 contain overarching requirements and activities, namely organizational and project dependent cybersecurity management (5 and 6), and distributed engineering activities (7). The main work product of clause 7 is the cybersecurity interface agreement, which specifies how customer and supplier will work together.

Moreover, clauses 8 and 13 describe activities required for the secure operation of vehicles. Since the continual cybersecurity activities of clause 8 are not project-specific, and newly discovered vulnerabilities may also influence ongoing development projects, clause 8 covers the whole development life cycle in fig. 4. Fig. 6 shows the procedure of the activities in clauses 5, 8 and 13 in more detail. Clause 5 defines the required processes and rules for the subsequent activities, including clauses 8 and 13, and shall support the continuous improvement of all cybersecurity activities. In cybersecurity monitoring (Clause 8.3), events are generated based on defined information sources and triggers (e.g., keywords in documents). Here, the process step of filtering information by triggers is called triage. Afterwards, each event is analyzed to identify weaknesses (event evaluation, clause 8.4). In vulnerability analysis (8.5), a decision is made whether the weakness is a vulnerability, in which case a risk assessment is performed. Finally, in vulnerability management (clause 8.6), risk-based countermeasures are selected or residual risks are accepted. The remedial actions are documented and implemented in an incident response plan in the incident response step (clause 13.3), which is part of the operations and maintenance clause. This response plan shall be created for each incident and contains further documentation, such as responsibilities, communication strategies, and criteria for determining the progress and closure of the case. Finally, clause 13.4 of ISO/SAE 21434 mandates that the development of updates must conform to ISO/SAE 21434 as well.

Supporting figures and tables

This section contains supporting figures and tables that did not fit into the main paper due to page restrictions. The steps of the ISO/SAE 21434 TARA framework are depicted in fig. 5.

Incident handling is only to be invoked as part of vulnerability management, as depicted in fig. 6.

A relationship diagram of the proposed terminology in the context of ISO/SAE 21434 is depicted in fig. 7.

The work products of the newly introduced preparation phase are shown in tab. I.

The full terminology table is depicted in tables II, III, IV and V.

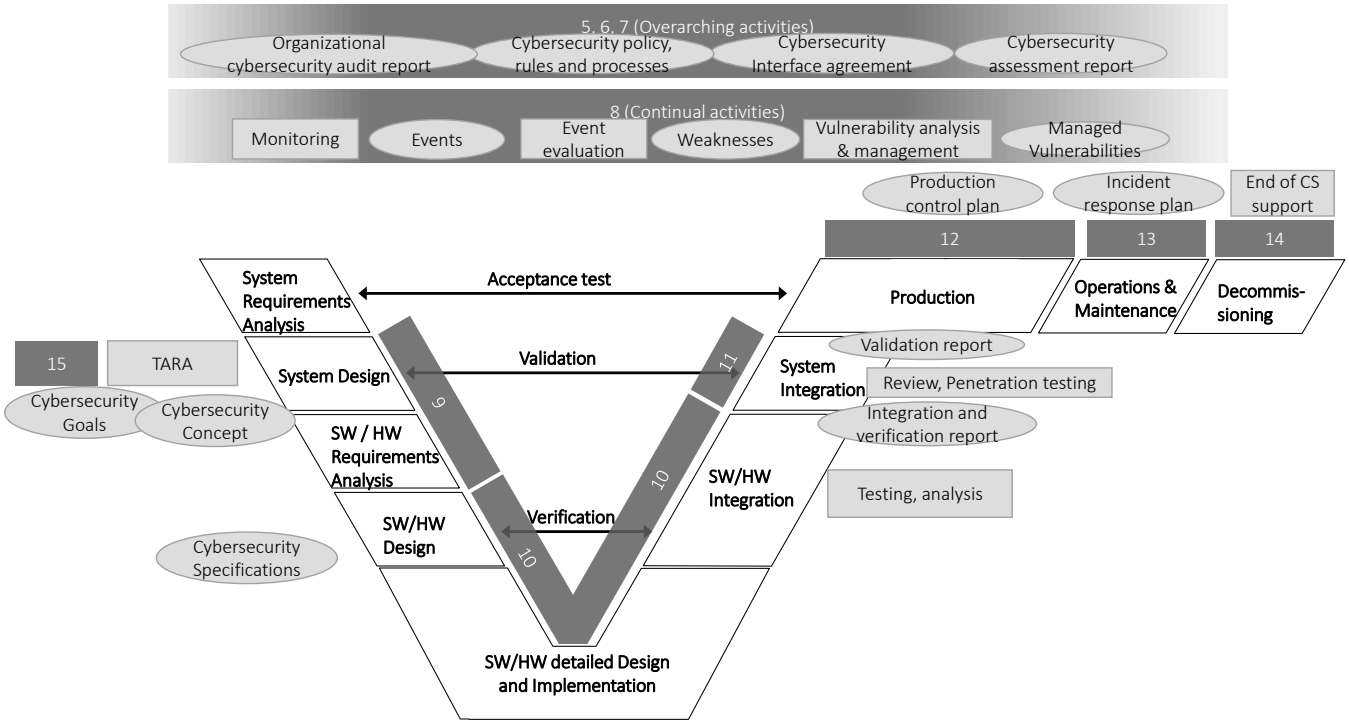


Fig. 4: The Automotive Development Life Cycle based on a V-Model workflow and related phases for cybersecurity engineering according to ISO/SAE 21434.

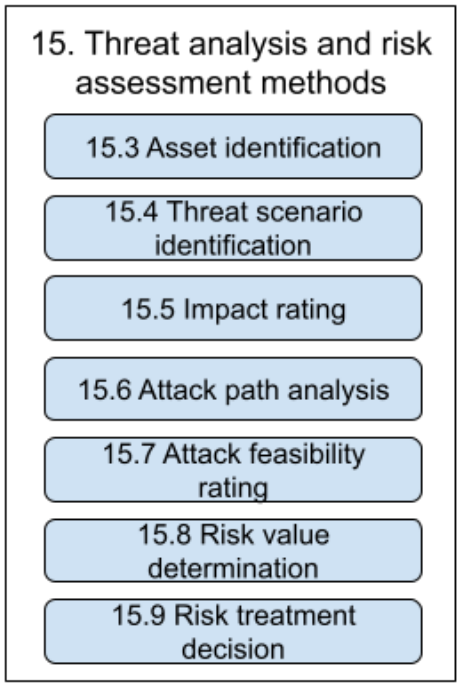


Fig. 5: The elements of TARA as defined in ISO/SAE 21434.

TABLE I: Work products of the Preparation phase

Target phase	Work product
General	Log retention policy, exchange formats and information sharing policy (with TARA mgmt. and externally)
Triage	Triggers for validation, methods for categorization and prioritization
Vulnerability & incident analysis	contact data of internal experts and responsible persons, access to configuration management (build and development environment, SW/HW versions), access to documentation (network diagrams, functions, proprietary protocols, security mechanisms, monitoring)
Incident management	Incident response plan template, response strategies, escalation criteria

TABLE II: Terminology comparison of different standards and reports. UNR 155 and MITRE have no definitions for the terms listed in this table.

Term	ISO/SAE 21434	NIST SP 800-61[a]	CMU/SEI-2004-TR-015	ISO 27035
Attack / Attack path	set of deliberate actions to realize a threat scenario	-	-	attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset
Cybersecurity event	cybersecurity information that is relevant for an item or component	any observable occurrence in a network or system	[19]: an occurrence in a system that is relevant to the security of the system [b]	information security event: occurrence indicating a possible breach of information security or failure of controls
Cybersecurity incident	situation in the field that can involve vulnerability exploitation	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security policies	[19]: a security event that involves a security violation[c]. [2]: computer security incident: any adverse event which compromises some aspect of computer or network security	information security incident: one or multiple related and identified information security events that can harm an organization's assets or compromise its operations
Cybersecurity incident handling	-	The mitigation of violations of security policies and recommended practices (=Incident response)	the processes used for handling an incident; in this text, the term includes the processes for detecting, reporting, triaging, analyzing, and responding to computer security incidents.	actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents
Cybersecurity incident management	-	-	the processes for controlling or administering tasks associated with computer security incidents; in this text, the term implies management of a computer security incident, and includes all of the Detect, Triage, and Respond processes as well as the Prepare (improve, sustain) processes and the Protect processes outlined in this report.	information security incident management: exercise of a consistent and effective approach to the handling of information security incidents
Cybersecurity incident response	-	The mitigation of violations of security policies and recommended practices (=Incident handling)	an answer given or action taken by people designated to react to an incident. It is the process that encompasses the planning, coordination, and execution of any appropriate mitigation and recovery strategies and actions.	actions taken to mitigate or resolve an information security incident, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it
Cybersecurity information	information with regard to cybersecurity for which relevance is not yet determined	-	-	-

[a] appendix C
[b] includes both events that are incidents and those that are not
[c] In other words, a security-relevant system event in which the system's security policy is disobeyed or otherwise breached

TABLE III: Terminology comparison of different standards and reports (ctd.)

Term	ISO/SAE 21434	NIST SP 800-61[a]	CMU/SEI-2004-TR-015	ISO 27035
Indicator	-	A sign that an incident may have occurred or may be currently occurring	-	-
Threat scenario	potential cause of compromise of cybersecurity properties of one or more assets in order to realize a damage scenario	-	-	Threat: potential cause of an unwanted incident, which may result in harm to a system or organization
Triage	analysis to determine the relevance of cybersecurity information to an item or component	-	the process of receiving, initial sorting, and prioritizing of information to facilitate its appropriate handling	-
Update	Not a definition, but a related description: "Updates are changes made to an item or component during post-development and can include additional information, e.g. technical specifications, integration manuals, user manuals."	-	-	-
Vulnerability	weakness that can be exploited as part of an attack path	A weakness in a system application or network that is subject to exploitation or misuse	[2]: a characteristic of a piece of technology which can be exploited to perpetrate a security incident. [24]: the existence of a software weakness, such as a design or implementation error, that can lead to an unexpected, undesirable event compromising the security of a system, application or protocol	weakness of an asset or control that can be exploited by a threat
Vulnerability analysis	Not a definition, but a description: examines weaknesses and assesses if a particular weakness can be exploited.	-	Vulnerability assessment: an act or procedure intended to evaluate or identify the existence of known vulnerabilities (in a computer system or network)	-
Vulnerability management	Not a definition, but a description: tracks and oversees the treatment of identified vulnerabilities in items and components until their end of cybersecurity support.	-	-	-
Weakness	defect or characteristic that can lead to undesirable behavior	-	-	-

[a]appendix C

TABLE IV: Terminology comparison of different standards and reports (ctd.)*

Term	UNR 155 [22]	UNR 156 [23]	MITRE [20], Common Weakness Exposure Project
Threat	"threat" means a potential cause of an unwanted incident, which may result in harm to a system, organization or individual	-	-
Update	-	"software update" means a package used to upgrade software to a new version including a change of the configuration parameters	-
Vulnerability	weakness of an asset or mitigation that can be exploited by one or more threats	-	an occurrence of a weakness (or multiple weaknesses) within a product, in which the weakness can be used by a party to cause the product to modify or access unintended data, interrupt proper execution, or perform incorrect actions that were not specifically granted to the party who uses the weakness.
Weakness	-	-	a type of mistake that, in proper conditions, could contribute to the introduction of vulnerabilities within that product. This term applies to mistakes regardless of whether they occur in implementation, design, or other phases of a product lifecycle.

* The UNR 155 [22], UNR 156 [23] and MITRE [20] definitions were put into its own tables to keep tables II and III readable

TABLE V: Chosen terminology definitions for this paper (cf. tables II, III and IV)

Term	Chosen definition*	ISO/SAE 21434 status**
Attack / Attack path	set of deliberate actions to realize a threat scenario	S
Cybersecurity event	an occurrence in an item/component that is relevant to the cybersecurity of the system	D
Cybersecurity incident	a cybersecurity event that involves a violation of product cybersecurity, product safety or organizational cybersecurity policy	D
Cybersecurity incident analysis	the process of identifying and assessing cybersecurity incidents from identified cybersecurity events	U
Cybersecurity incident handling	the process of analysing and managing cybersecurity incidents	U
Cybersecurity incident management	the process of tracking and treating cybersecurity incidents, including actions for containment, eradication or recovery	U
Cybersecurity incident response	the process of analysing and managing cybersecurity incidents (NOTE: same as incident handling)	P
Cybersecurity information	information with regard to cybersecurity for which relevance is not yet determined	S
Cybersecurity monitoring	the process of collecting, pre-processing and formatting cybersecurity information for subsequent processing	P
Indicator	information with regard to cybersecurity that is relevant for an item or component	U
Post-analysis of vulnerability and incident handling	the process of analysing and measuring incident and vulnerability handling outcomes, including technical root cause analysis and efficiency measurements	U
TARA management process	the process of brokering access to and coordinating work on TARA artifacts required for an item, including the coordination of distributed development activities and the definition of appropriate abstraction levels	U
Threat scenario	potential cause of compromise of cybersecurity properties of one or more assets in order to realize a damage scenario	S
Triage	the process of determining relevance of cybersecurity information and prioritization of resulting indicators to facilitate their appropriate handling	D
Update	a package used to upgrade software to a new version including a change of the configuration parameters	P
Vulnerability	weakness that can be exploited as part of an attack path	S
Vulnerability analysis	the process of identifying and assessing vulnerabilities from identified weaknesses, which includes performing the appropriate steps of threat analysis and risk assessment	P
Vulnerability handling	the process of performing vulnerability analysis and vulnerability management	U
Vulnerability management	the process of tracking and treating cybersecurity vulnerabilities	P
Weakness	defect or characteristic that can lead to undesirable behavior	S

* Could be considered for inclusion in next ISO/SAE 21434 revision

** Status legend: D = Defined differently; P = Process/concept exists without definition; S = Same definition; U = Undefined

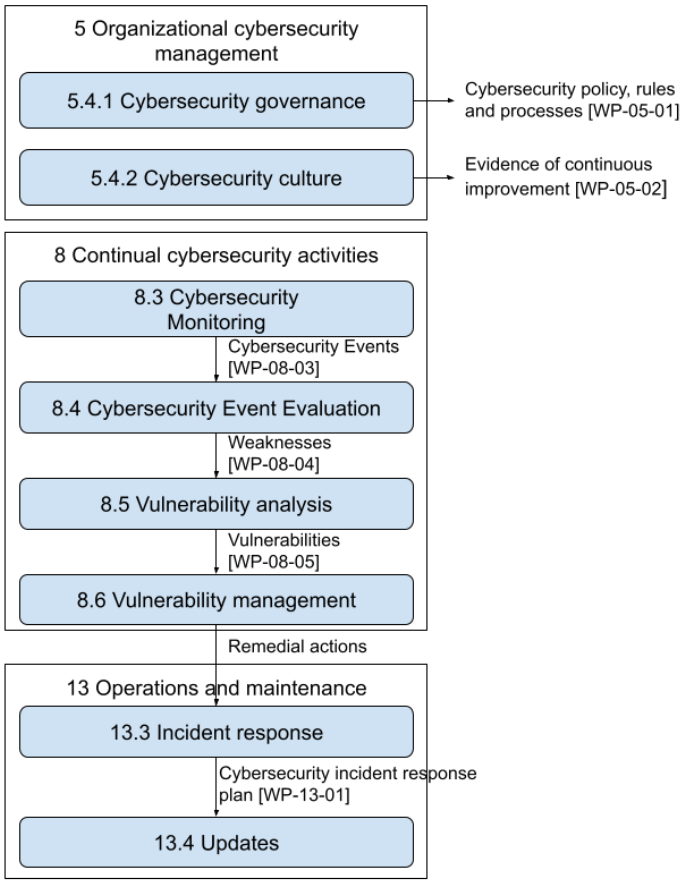


Fig. 6: Vulnerability and incident handling related clauses in ISO/SAE 21434

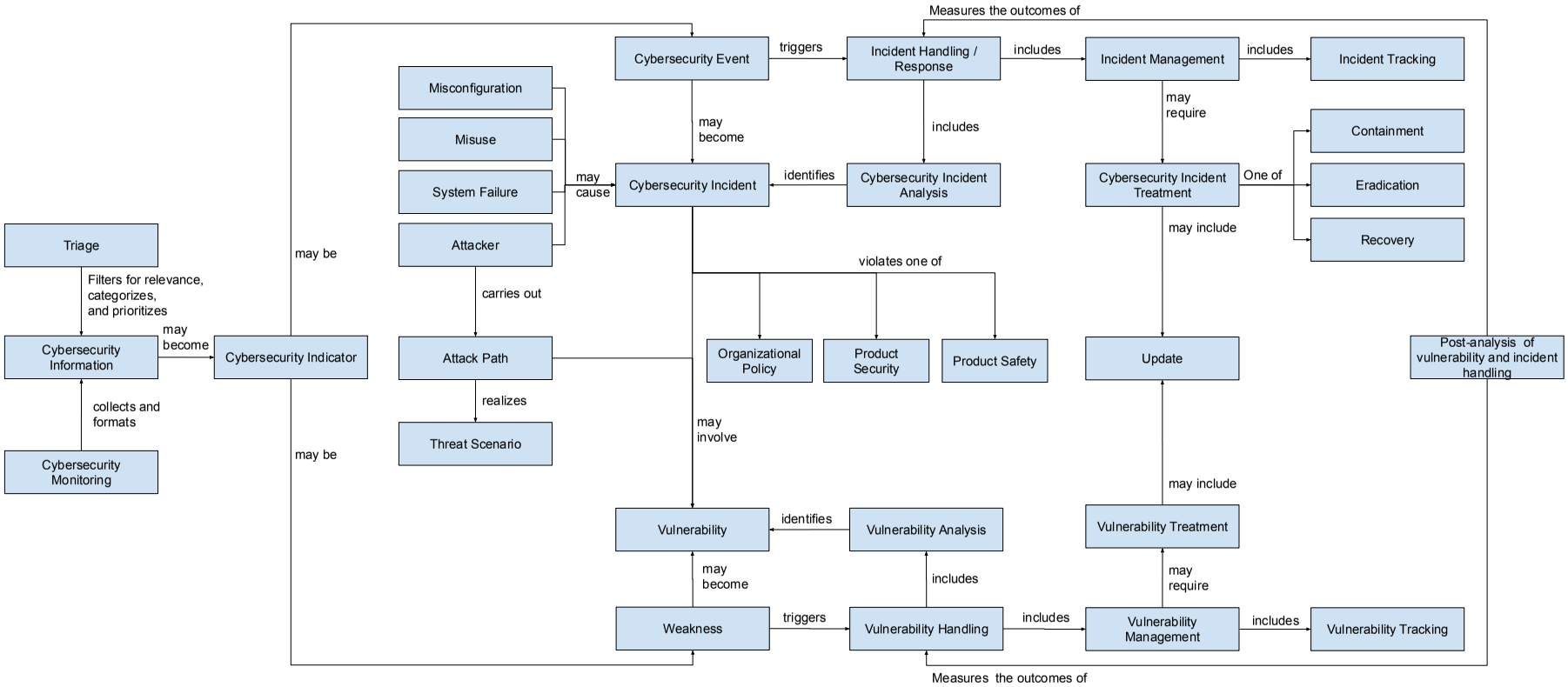


Fig. 7: Terminology relationships