In-depth exploration on ISO/SAE 21434 and its correlations with existing standards

Gianpiero Costantino, Marco De Vincenzi, and Ilaria Matteucci

***Abstract*—In recent years, the evolution of road vehicles has strongly required common rules to manage cybersecurity in automotive. In this paper, we summarise the standard ISO/SAE 21434, focusing on the main requirements, work products, and innovations. We identify with an ego-network the possible correlation of ISO/SAE 21434 with the already existing standards in automotive, reporting a strong correlation with the safety standard ISO 26262. Following, we discuss the relationship between safety and security in automotive, and between ISO/SAE 21434 and regulation UNECE WP.29 R155. Then we focus on possible limits and implementations of the standard like the introduction of application methods or specific thresholds for the required security risk analysis. Finally, we propose a structured list of documents that can be used as a landmark to achieve compliance with the cybersecurity standard and an example of the application of ISO/SAE 21434 to an electric window power regulator system.**

***Index Terms*—Automotive, cybersecurity, risk analysis, safety, ISO/SAE 21434, ISO 26262, UNECE WP.29 R155.**

INTRODUCTION

THE constant increase of electronic and software components in the vehicles requires continuous development to ensure the safety and security of the users. In particular, the growing complexity of such communications has needed common standards and rules among the different actors of the road infrastructure. In the last years, different standards have been developed for automotive like ISO 26262 or SAE J3061 to assure respectively safety and security. However, the increasing demand for a common and shared standard of cybersecurity led in 2016 the International Organization for Standardization (ISO) and the Society of Automotive Engineers (SAE) to work on the ISO/SAE 21434:2021, released in August 2021. It will be the new cybersecurity standard in automotive, alongside the regulation UNECE WP29 R155.

A. Contributions and Motivations

In this paper, we carefully analyse the ISO/SAE 21434 standard to ease the comprehension and the application in a complex environment. Moreover, we highlight some limitations and, then we propose possible improvements. Analysing the standard, we create an ego-system to show the relationship between ISO/SAE 21434 and the other standards with a focus on safety and security in automotive. Besides, we define a document list that is compliant with ISO/SAE 21434, for E/E (Electrical/Electronic) components, taking as baseline the same structure of a Part Production Approval Process (PPAP), largely used in automotive for mechanical components. Finally, we provide an example of ISO/SAE 21434 application on a window power regulator system.

This study is motivated by the recent emerging of the ISO/SAE 21434 and its application timing in the automotive domain. Our work is one of the few studies dedicated to ISO/SAE 21434 and it provides a significant contribution to the discussion on this standard, especially focusing on the open debate on safety and security of items' design. On this aspect, carmakers are required to design and sell secure new vehicles type starting from July 2022 as required by the regulation UNECE WP29 R155.

B. Related Work

Although ISO/SAE 21434 was just released in its final version in August 2021, some academic and industrial-related works have been already published. For example, [1] proposes a security engineering approach that can ease compliance with this standard. It develops a rigorous security and incremental maintenance assessment to increase production efficiency and enable continuous security development. The authors of [2] review the draft version of ISO/SAE DIS 21434 dated September 2020, describing the structure of the standard and reviewing the achieved results and the open questions. This paper can be considered a position paper for discussion and exchange between industry experts and researchers. In [3] Annex G of ISO/SAE 21434, which proposes three different attack feasibility methods, is investigated. In particular, this work shows that the three methods are neither equivalent nor interchangeable with the possible consequence of misinformed risk-based decisions. The author suggests a more in-depth study on the applicable attack feasibility methods.

Concerning the previous academic works, our study is not focused on the application methods like [1], it goes beyond the review of the ISO like [2], and it does not address only a specific norm of the standard like [3]. Our study provides a critical analysis of possible limits and implementation of the standard in addition to the comparison with other standards.

From a more industrial point of view, in an insights paper [4], the British Standards Institution (BSI) analyses the general framework where ISO/SAE 21434 will be inserted and proposes methods to be compliant. In addition, private industries like in [5] and [6] are interested in the coming cybersecurity rules. They analyse the standard and propose proprietary solutions and products to be compliant with it. Concerning industrial works, our study provides a unique comparison of the largely applied automotive quality document PPAP, used

The authors are with Italian National Research Council.

for mechanical components, with the documents required for cybersecurity of E/E components.

To the best of our knowledge, until now, Japs' research [7] is one of the few works related to the application limits and implementations of ISO/SAE 21434. The author states that the standard only prescribes what must be done, but does not define how this is supposed to be done methodically. For this reason, the author proposes a model-based systems engineering approach divided into four papers, two of which still have to be published. Our work focuses more on the comparison with other standards and not on the possible application process.

ISO/SAE 21434 Purpose and Structure

ISO/SAE 21434 aims to be the cybersecurity standard in the engineering of E/E systems within road vehicles. The document provides original equipment manufacturer (OEM) and their suppliers (e.g. Tier 1, Tier 2) guidelines to manage cybersecurity culture, policies, and risks in every phase of the engineering process. The standard does not prescribe specific technical solutions. However, it represents a general framework to manage cybersecurity risks for several types of road vehicles. Automotive is on the road to completely autonomous vehicles. Even if these types of vehicles are not mentioned directly, the standard could be considered a baseline to increase the safety and security of critical Cyber-Physical Systems (CPS) like the E/E items of autonomous vehicles. On the other side, as stated in [8], autonomous vehicles could require a different and deeper approach to cybersecurity, which should be addressed in the standard.

The ISO/SAE 21434 document is composed of the introduction, fifteen sections, and eight annexes. The first two sections define the scope and the normative references. Section 3 contains a series of word definitions to create a common glossary for automotive cybersecurity, which was one of the main expected innovations of ISO/SAE 21434. The subsequent sections are called "clauses", where the requirements (RQ), recommendations (RC), and work products (WP) are defined. In clause 5 an important novelty is the definition and the request of a strong cybersecurity culture [RQ-05-06] where cybersecurity and safety have the highest priority [Annex B - Table B.1], defining also in [RQ-05-09] the procedures of information sharing. Clause 9 defines cybersecurity goals, resulting from a threat analysis and risk assessment of the item. In particular, the clause defines several documents based on clause 15: an asset identification, a threat scenario, an impact rating, an attack path analysis, an attack feasibility rating, and a risk value definition [RQ-09-03]. Clause 13 requires a cybersecurity incident response plan, including remedial actions, to determine and implement quick actions in case of cybersecurity incidents [RQ-13-01]. Clause 14 defines the operations to end the support of a cybersecurity item or component and for decommissioning. Clause 15 is a baseline to other clauses, requiring to determine the possible threats to which a user and a vehicle are exposed, using, for example, the threat agent risk assessment (TARA) method.

Correlation with other standards

The ISO/SAE 21434 [2], as declared in the foreword of the standard, cancels and supersedes the previous cybersecurity standard SAE J3061:2016. Automotive is a highly standardised environment, where several standards like ISO 9001 or ISO 26262 are already largely applied. ISO/SAE 21434 application in automotive has to face and relate with the already existing standards, in particular with the quality, safety, and security rules. For this reason, we analyse the correlation between ISO/SAE 21434 and the other already existing automotive standards. As *correlation* we mean the connections or relationship between two standards: a strong correlation means that ISO/SAE 21434 has similarities with the previous standard and/or it has inherited some elements. To identify the possible correlations among documents we use the number of direct citations in the ISO/SAE 21434 text. As stated in [9], citing papers could have a high degree of relevance and may represent works that are crucial or significant antecedents to the present work. Thus, citations can be used as a correlation metric.

As the first step, we analyse the ISO/SAE 21434 document. Using Python language, we identify the direct citations of the other standards in the text. Some of them, like ISO 26262 or ISO 9001 are cited several times in ISO/SAE 21434, while others like ISO/TR 4804 only one time. Then, using the Python library NetworkX, we generate the ego-network graph, as shown in Fig. 1, with ISO/SAE 21434 as ego node in the centre. Ego-networks are frequently used to analyze social connections, correlations, or relationships. In our case, we measure the correlation of the ego node with the other nodes, called alters. The greater the alter node distance from the ego node is, the smaller the correlation is. We group together correlated standards with similar correlation degrees: *strongly* correlated (in red in Fig. 1), *moderate* correlated (in orange), and *weak* correlated (in yellow). In Fig. 1 it is also reported on the lines, connecting the ego node with the alters, the number of citations of the alter standard in ISO/SAE 21434 document. The thickness of the edges is directly proportional with the number of citations: more citations, more thickness, while less thickness means fewer citations, so less correlation.

We can notice the strict correlation between ISO/SAE 21434 and ISO 26262, the automotive standard for the safety of road vehicles, first published in 2011 and cited fifteen times in the ISO/SAE 21434 text. Confirming our network analysis, both standards have several main common required elements as shown in Table I.

Beyond the similarities between ISO/SAE 21434 and ISO 26262, we can find also some significant differences like the tool management or the management of out-of-context components that ISO/SAE 21434 explicitly covers in Section 5.4.5, that, however, are not covered by ISO 26262. Moreover, ISO/SAE 21434 seems to be more detailed than ISO 26262, because it covers all the aspects of item creation and maintenance. For example, the relationship between customers and suppliers is covered in Section 7.4 of ISO/SAE 21434, while

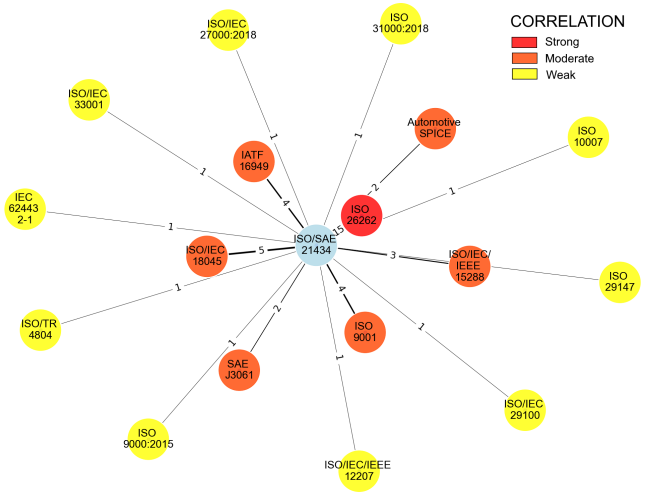

Fig. 1. Correlation ego-network of ISO/SAE 21434.

TABLE I
MAIN COMMON ELEMENTS BETWEEN ISO/SAE 21434 AND ISO 26262-2:2018

	Sections	
Element	**ISO/SAE 21434**	**ISO 26262**
Creation of a [security or safety] culture	5.4.2	5.4.2
Organization competencies	5.4.2	5.4.4
Responsibility definition	6.4.1	6.4.2
Information sharing	5.4.3	5.4.2.3
Impact analysis	15.5	6.4.3
A [security or safety] plan	6.4.1 to 6.4.6	6.4.5 to 6.4.13
Tailoring activities	6.4.3	6.4.5
Reuse activities	6.4.4	6.4.4
Request of audit	5.4.7	6.4.11
[security or safety] Assessment	6.4.8	6.4.12
A case example	6.4.7	6.4.8
A rigor level [CAL for ISO/SAE 21434 / ASIL for ISO 26262]	Annex E	4,.4

ISO 26262 does not address this topic.

Referring to Fig. 1, unexpectedly, the standard SAE J3061, which was published in 2016, dedicated to cybersecurity and superseded by ISO/SAE 21434, is cited directly only two times. However, ISO/SAE 21434 inherited some elements from SAE J3061 such as the continuous cybersecurity management process with a cybersecurity culture development. Another related security standard is ISO/IEC 18045:2008, which specifies the methodology for IT security evaluation. This standard is cited and applied in ISO/SAE 21434 for the definition of the attack feasibility rating and the definition of the attack potential-based approach.

Some quality standards like IATF 16949 and ISO 9001 with four citations each are quite strongly correlated with ISO/SAE 21434. This confirms the close relationship between quality and cybersecurity. Thus, in Section -D, we use a standard automotive quality document, PPAP, to define a unified and complete document for ISO/SAE 21434 compliance.

ISO/SAE 21434 is also correlated to ISO/IEC/IEEE 15288:2015, which defines a framework to describe the life cycle of a system. The ISO/IEC/IEEE 15288:2015 gives specific definition of some terms through a glossary. For instance, ISO/SAE 21434 inherits from this standard the definition of "validation" and "verification".

C. Safety-Security Relationship

The strongest correlation is between ISO/SAE 21434 and ISO 26262. This relation requires a deep analysis of the relationship between safety and security in automotive to provide a general overview to motivate the continuing discussion about this topic. On this subject, the authors of [10] analyse the opportunity to have safety and security approaches in automotive comparing ISO 26262 and ISO 15408. The work in [11] reports the following Fig. 2 to show the different possible relationships between safety and security.

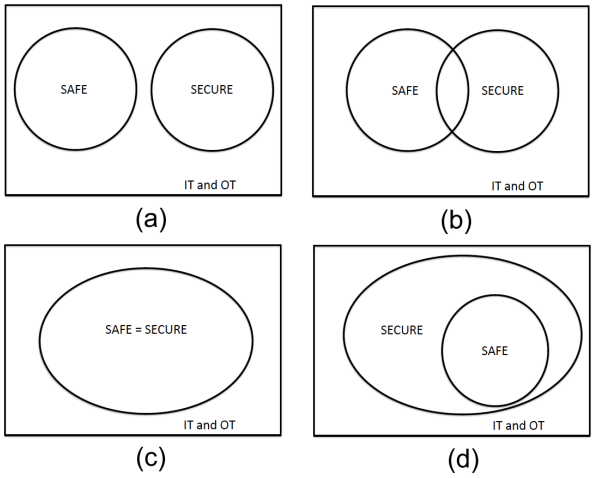

Fig. 2. Correlation between safety and security [11].

As stated in [11], the current situations of this relationship can be represented with diagram *a* and *b* of Fig. 2, even if there is an open debate about this point. Our analysis of ISO/SAE 21434 suggested that the diagram *b* may be the nearest to the reality of standards. The other two diagrams, *c* and *d*, in Fig. 2, should describe a possible near future relationship, but the debate is even more open: diagram *c* appears to be wrong [11] because there could be differences between safety and security. Diagram *d* is mainly supported by commentators from the security sector, that have questioned if a system can be safe if it is insecure [11].

In our opinion, the most representative diagram of the current reality and for the future could be diagram *b* with a growing intersection area. We think that safety and security are different areas of interest, so diagram *c* can be excluded,

while diagram *a* is not real because there is an indisputable correlation between the two areas. Diagram *d* could also be the correct representation when we have a macro vision of the automotive world where all the functionalities of vehicles will become purely electronic. However, we think that in some situations safety will maintain its application distinct from security, e.g., in vehicles where mechanical or electrical systems can still work autonomously from software control. In this debate, ISO/SAE 21434 defines only cybersecurity and it does not address directly the safety. Instead, at the same time, it seems to intersect safety with standard ISO 26262, to confirm again the strong relationship between the two areas.

D. UNECE WP.29 R155 and ISO/SAE 21434 Relationship

UNECE WP.29 is a world forum for harmonization of vehicle regulations of the Sustainable Transport Division of the United Nations Economic Commission for Europe (UNECE). This forum provides a legal framework, concerning the cybersecurity of connected vehicles, with a timeline to be implemented by the automotive companies. Despite what we might expect, UNECE WP.29 regulation R155 is not directly cited in the standard ISO/SAE 21434. Nevertheless, we can shortly investigate the relationship between the regulation and the standard.

The main difference between the two documents is that R155 is a regulation, defined as a legally binding directive for over 55 countries belonging to UNECE, while ISO/SAE 21434 is a standard, which is not mandatory for automotive industries, but it is expected to be largely accepted like ISO 26262 is today. R155 defines the term of July 2022 to be implemented in the new European Union (EU) vehicle types and July 2024 for the first registration vehicles in the EU. Instead, ISO/SAE 21434 does not provide any timeline.

R155 and ISO/SAE 21434 answer the question "what" and not "how" to deal with cybersecurity issues. They do not provide specific actions, but a framework and guidelines to mitigate and treat risks and exposed vulnerabilities. Both documents cover security by design in all vehicle lifecycle: R155 requires a certified cybersecurity management system (CSMS) with risk identification, security tests, audits, and continuous cybersecurity monitoring and improvement. ISO/SAE 21434 inherits all these concepts and introduces more elements like the uniform terminology for automotive cybersecurity, the cybersecurity assurance levels (CALs) classification, and the out-of-context components processing. In addition, R155 provides a list of possible threats as possible risk baseline. On the other side, ISO/SAE 21434 focuses on the cybersecurity company responsibilities and provides an application of the proposed methods for cybersecurity analysis like TARA. Summarizing our opinion, the regulation and the standard are superimposed in some cases, e.g., the risk identification, but, in general, can be considered complementary and both can provide relevant rules for the cybersecurity of connected vehicles.

LIMITS AND IMPLEMENTATIONS OF ISO/SAE 21434

ISO/SAE 21434 is a standard that has required several years to be developed, showing the open debate and the difficulties that are present to define a common standard for cybersecurity in automotive. In our opinion, ISO/SAE 21434 seems to be a quite complete and structured standard that is well inserted in a highly standardized environment, as shown in Section -B. It deepens several concepts inherited from previous works like regulation UNECE WP.29 R155. Moreover, ISO/SAE 21434 provides a process composed of different steps and documents that covers all the life cycle of an E/E item from the agreement between customer and supplier to the decommissioning. However, we can find some possible limits and implementations of ISO/SAE 21434, which should be addressed and deeper investigated by the standard organisations and by the automotive community.

In Table II, we summarise our findings and we assign a possible occurrence value to the consequences of a specific limit, referred as *Occurrence Probability* (OP), and a value to define the *Impact* on security (I). For example, in the first row we describe a possible limit: as shown in [7], the standard does not provide technologies, methods or solutions to be implemented to have secure vehicles' components. From one side, this situation is intended to leave the producer free to adopt the best suitable solutions for each item. On the other side, this lack of defined technologies and methods can create some situations where each company decides to use its proprietary solution, creating a partitioned situation in a highly connected environment. This event has a high probability to occur and could lead to problems of compatibility in the network with a possible high impact on cybersecurity. To mitigate this risk, it could be necessary to define some common system engineering approaches, for example, according to the specific vehicle domain application, e.g., chassis, powertrain and so on.

CYBERSECURITY ITEM APPROVAL PROCESS : A STRUCTURE DOCUMENTS LIST

One of the most significant possible implementations of ISO/SAE 21434 is the organic definition of required documents for cybersecurity compliance of E/E items. ISO/SAE 21434 standard lists only the WPs. The strict correlation with IATF 16949 suggests the comparison with a structured quality document like the production part approval process (PPAP) to obtain conformity in cybersecurity. PPAP, defined by the Automotive Industry Action Group (AIAG), is the most common automotive document list for mechanical components to ensure engineering design and product specification requirements are met. PPAP standard is used worldwide in the automotive to certify the process of production of every item. The document is divided into 18 parts, which are not all mandatory, but the requested documents depend on the required level of PPAP. There are 5 possible levels, from the less demanding, level 1, to the more demanding, level 5.

Table III defines 16 possible documents to obtain the conformity of an E/E item with ISO/SAE 21434. All the listed documents are not mandatory and the required documents can be set according to the cybersecurity assurance level (CAL) as defined in Annex E of ISO/SAE 21434. We divided all the 21434 documents into several sections:

TABLE II
MAIN POSSIBLE LIMITS AND IMPLEMENTATIONS OF ISO/SAE 21434

Limits	Consequences	OP	I	Implementations
The standard only provides what must be done and not how.	It can create some fragmented situations in a highly connected environment like automotive, where each company uses its proprietary solutions without any control of compatibility and reliability of the adopted solutions.	High	High	Definition of possible application approaches and methods like in [7].
Absence of specific intervention thresholds for each analysis like TARA.	It can lead to different concepts of cybersecurity activities from one company to another. For example, for the same item type, each company can freely decide which risk treatment applies to a detected risk. The consequence could be the adoption of insecure standards from a company, that can fulfil the risk assessment and all required documents according to its own will.	High	High	Definition of guidelines for thresholds not for specific item type, but different for each vehicle domain, e.g., chassis, powertrain and so on.
The lack of ad-hoc defined cybersecurity standards for a complete road infrastructure, including vehicles and Road Side Units (RSUs), and for each road infrastructure component like electric vehicle chargers.	ISO/SAE 21434 may secure in-vehicle items, but, since the vehicle is part of an infrastructure, the lack of security of other components and the interaction with them may compromise security and safety of the user and the vehicle.	High	High	For a complete road network infrastructure and for each of its components, definition of security standards, evaluating the integration with ISO/SAE 21434.
The lack of the definition of a list of threat modes and corresponding mitigations for connected vehicles.	Each car maker can define its own list of possible threats. There is the risk of missing some possible threats with the consequence of different cybersecurity levels for the same item.	High	Moderate	Definition of a list of threat modes like the list of UNECE WP29 R155 or the adoption of this list within the ISO/SAE 21434.
The lack of common document templates for the different analysis and assessments.	This lack can lead to customised proprietary documents, causing fragmentation and a decrease in the effectiveness of a common standard of cybersecurity communication and analysis.	Moderate	Low	Definition of common document templates like for the incident response plan, required by clause 13. As plan, it could be used the *Eight Disciplines* problem solving standard [12], which is a reactive problem-solving approach already largely applied in automotive.
As shown in [3], the approaches (attack potential-based, CVSS-based, attack vector-based) for the attack feasibility rating, proposed in Annex G, are not interchangeable.	The wrong choice of one approach can lead to misinformed risk-based decisions [3].	Moderate	Moderate	Further developments need to investigate which method is closest to real-world attack feasibility for each application domain.

1) *Requirements*: Number 1 defines the cybersecurity requirements for the item or component.
2) *Organization definition*: Number 12, 15 and 16 define the context where the item will be developed and maintained. Document 12 defines the tool management policy. Document 15 describes the company organization from the point of view of cybersecurity, while Document 16 describes the agreements between the customer and the supplier for the development of the item.
3) *Concept*: Number 2, 3, 4, and 5 defines the item structure, goals, and responsibilities for the development.
4) *Product development*: Number 7, 8, and 9 are the cores of the list. These documents model the cybersecurity of the item and they analyze each aspect of cybersecurity. Moreover, a control plan is required.
5) *Testing*: Number 13 and 14 define respectively the verification and the validation activities for the item.
6) *Operations*: Number 10 defines the incident response plan that should be used during the implementation phase and for all life cycles of the item.
7) *Maintenance*: Number 3.2 reports how to tailor or reuse the item. Note that, during the item life, all the documents in the list can be revised if necessary.
8) *Decommissioning*: Number 6 and 11 define the decommissioning procedures.

EXAMPLE OF APPLICATION OF ISO/SAE 21434

Following the structured documents list defined earlier, we would like to apply some ISO/SAE 21434 requirements on a real vehicle item like an Electronic Control Unit (ECU) of an electric window power regulator. In this example, we test a simplified version of the electric window system. This component has the main function to raise and lower door glasses and the emergency function to lower the window if the sensor in the door detects a closure force larger than 100 N, caused by the presence of an object (e.g. a hand) between the window and the door closure [13].

Hereafter, we briefly describe the cybersecurity analysis that we performed for our example. Other analyses, as defined in Table III, can be performed, but in our work, we provide only a simplified version of the ISO/SAE 21434 document

TABLE III
PPAP - ISO/SAE 21434 COMPARISON AND POSSIBLE CYBERSECURITY DOCUMENT STRUCTURE

21434= ISO/SAE 21434:2021; n.= number						
PPAP n.	**PPAP DOCUMENT**	**21434 n.**	**21434 DOCUMENT**	**21434 sub n.**	**21434 CLAUSE**	**21434 WP**
1	Design Record	1	Cybersecurity specifications and post-development requirements	1.1	Design (10.4.1)	[WP-10-01][WP-10-02]
/	/	2	Concept documents	2.1	Item definition (9.3)	[WP-09-01]
				2.2	Cybersecurity goals (9.4) - Goals	[WP-09-03]
				2.3	Cybersecurity goals (9.4) - Threat analysis and risk assessment (TARA) composed by documents of point 8	[WP-09-02]
				2.4	Cybersecurity goals (9.4) - Claims	[WP-09-04]
				2.5	Cybersecurity goals (9.4) - Verification report	[WP-09-05]
				2.6	Cybersecurity concept (9.5) - Concept	[WP-09-06]
				2.7	Cybersecurity concept (9.5) - Verification report of cybersecurity concept	[WP-09-07]
/	/	3	Cybersecurity plan	3.1	Cybersecurity responsibilities (6.4.1) - Cybersecurity planning (6.4.2)	[WP-06-01]
2	Engineering Change Document			3.2	Tailoring (6.4.3) - Reuse (6.4.4) - Component out-of-context (6.4.5) - Off-the-shelf component (6.4.6)	
/	/	4	Cybersecurity case	4.1	Cybersecurity case (6.4.7)	[WP-O6-02]
/	/	5	Cybersecurity assessment report	5.1	Cybersecurity assessment report (6.4.8)	[WP-O6-03]
/	/	6	Cybersecurity for post-development report	6.1	Release for post-development (6.4.9)	[WP-O6-04]
3	Customer Engineering Approval	/	/	/	/	/
4	Design FMEA	/	/	/	/	/
5	Process Flow Diagram	7	Documentation of modelling, design, or programming language and coding guidelines	7.1	Design (10.4.1)	[WP-10-03]
6	Process FMEA	8	Cybersecurity analysis	8.1	Cybersecurity monitoring (8.3)	[WP-08-01][WP-08-02][WP-08-03]
				8.2	Cybersecurity event evaluation (8.4)	[WP-08-04]
				8.3	Vulnerability analysis (8.5)	[WP-08-05]
				8.4	Vulnerability management (8.6)	[WP-08-06]
				8.5	Asset identification (15.3)	[WP-15-01][WP-15-02]
				8.6	Threat scenario identification (15.4)	[WP-15-03]
				8.7	Impact rating (15.5)	[WP-15-04]
				8.8	Attack path analysis (15.6)	[WP-15-05]
				8.9	Attack feasibility rating (15.7)	[WP-15-06]
				8.10	Risk value determination (15.8)	[WP-15-07]
				8.11	Risk treatment decision (15.9)	[WP-15-08]
7	Control Plan	9	Control plan	9.1	Production (12)	[WP-12-01]
/	/	10	Incident response plan	10.1	Cybersecurity incident response (13.3)	[WP-13-01]
/	/	11	Procedures end of support	11.1	End of cybersecurity support (14.3)	[WP-14-01]
8	Measurement System Analysis (MSA)	12	Tool Management	12.1	Tool Management (5.4.5)	[WP-05-04]
9	Dimensional Results	13	Verification and integration report	13.1	Design (10.4.1) - Integration and verification (10.4.2)	[WP-10-04] [WP-10-05][WP-10-06][WP-10-07]
10	Material, Performance, Test Results	/	/	/	/	/
11	Initial Process Studies	14	Validation report	14.1	Cybersecurity validation (11)	[WP-11-01]
12	Qualified Laboratory Doc.	15	Organization qualification	15.1	Cybersecurity governance (5.4.1) - Information sharing (5.4.3)	[WP-05-01]
				15.2	Cybersecurity culture (5.4.2)	[WP-05-02]
				15.3	Management system (5.4.4)	[WP-05-03]
				15.4	Information security management (5.4.6)	[WP-05-03]
				15.5	Organizational cybersecurity audit (5.4.7)	[WP-05-05]
13	Appearance Approval Report	/	/	/	/	/
14	Sample Product	/	/	/	/	/
15	Master Sample	/	/	/	/	/
16	Checking Aids	/	/	/	/	/
17	Records of Compliance	/	/	/	/	/
18	Part Submission Warrant (PSW)	16	Supplier Agreement	16.1	Distributed cybersecurity activities (7.4.1/2/3)	[WP-07-01]

list. In Table IV we summarised all the performed analyses in our example. It is noted that each analysis should generate a single document/table, while in our case we use a single table (Table IV) for better readability.

E. Item definition [Document 2.1 - ISO/SAE 21434 Clause 9.3]

The simplified version of an electric window system is composed of the input system of the driver or passengers, the electronic control unit (ECU), the virtual box of the possible actions, and the box of the power window, containing the motor and the sensors that measure the position and the force,

made by the window during the closure. In this scenario, the ECU receives inputs from the driver/passenger switch and the position/force sensors. On the other hand, the ECU can perform actions like *up*, *down*, *cancel up*, or *cancel down*.

F. Asset identification [Document 8.5 - ISO/SAE 21434 Clause 15.3]

Among the possible documents addressed by point 2.3 of Table III, ISO/SAE 21434 requires to identify the assets of the item and the possible damage scenario as reported in Table IV. The security properties that we decided to study, as defined in Annex H of ISO/SAE 21434, are confidentiality, integrity, and availability, but other properties could be added and studied. This analysis contributes to Table IV with the columns *asset*, *C*, *I*, *A* and *damage scenario*.

G. Threat scenario identification with attack path analysis [Document 8.6 - ISO/SAE 21434 Clause 15.4 and Document 8.8 - ISO/SAE 21434 Clause 15.6]

Table IV shows possible threat scenario. Besides, Table IV reports possible attack paths with the assumption that the vehicle is connected to a network to exploit the connection for an attack. As possible attack vector, the onboard diagnostics (OBD) port is considered for direct physical access. This analysis contributes to Table IV with the columns *threat scenario* and *attack path*.

H. Impact rating [Document 8.7 - ISO/SAE 21434 Clause 15.5]

Following ISO/SAE 21434 example, impact rating identifies the impact category (safety, financial, operational, privacy) and the impact level scale (from low to high impact: negligible, moderate, major, severe) of the damage scenarios. This analysis contributes to Table IV with the columns *Impact category* and *Impact rating*.

I. Attack feasibility rating [Document 8.9 - ISO/SAE 21434 Clause 15.7]

According to Clause 8 of ISO/SAE 21434, the attack feasibility rating analysis can be performed following three different methods. In our example, we applied the attack potential-based approach because it seems the most complete and suitable for our scenarios. The values in the Table IV are assigned following the guidelines of Annex G of ISO/SAE 21434. In particular, we defined the following values:

1) Elapsed Time (ET): time to identify a vulnerability, develop and successfully apply an exploit. Scale: 1 for $\leq$ 1 week, 2 for $\leq$ 1 month, 3 for $\leq$ 6 months, 4 for $>$ 6 months.
2) Specialist Expertise (SE): the required expertise of the attacker. Scale: 1 = Layman, 2 = Proficient, 3 = Expert, 4 = Multiple experts.
3) Knowledge of the item (KN): the required amount of information and knowledge of the item and its connections. Scale: 1 = Public Information, 2 = Restricted information, 3 = Confidential information, 4 = Strictly confidential information.
4) Window of Opportunity (WO): Access conditions like time (unlimited or limited) and type (logical or physical) to successfully perform an attack. Scale: 1 = Unlimited, 2 = Easy, 3 = Moderate, 4 = Difficult.
5) Equipment (EQ): Required tools to successfully perform the attack. Scale: 1 = Standard, 2 = Specialized, 3 = Bespoke, 4 = Multiple bespoke.
6) Rating: Feasibility rating value is retrieved from the total sum of all previous values (ET+SE+KN+WO+EQ) and mapped in the ranges as: i) 0-5: High; ii) 6-10: Medium; iii) 11-15: Low; iv) 16-20: Very low.

J. Analysis conclusion

Regarding the impact rating results in Table IV, we found that the window controlled by the attacker and disabling of the force sensor are the most significant threats because they have an impact on driver/passengers safety with severe consequences. The attack that caused the loss of window functionality is mainly operational with a moderate impact on driver/passengers, and in our opinion, less dangerous than the previous ones.

Regarding the feasibility rating results in Table IV, we obtained a *very low* feasibility risk for the attack that involves the full control of the windows, exploiting the vehicle network connections. Instead, we obtained a *low* feasibility risk for those attacks that need the injection of a malicious message that can compromise a property, without the need to continually communicate with the ECU like in the previous attack. The highest feasibility risk is *medium* and it comes from the attack using the OBD port since, even if the attack feasibility is limited to its physical access, the disabling of a sensor using the OBD port may be considered a relative simple operation but with a severe impact on passengers' safety.

Finally, analysing the impact rating and feasibility results, as defined in Clause 15.9 of ISO/SAE 21434, a risk treatment decision analysis should be performed to reduce risks and to avoid the possibility for an attacker to combine two attacks like the disabling of the force sensor and the window control. In our scenarios, where it is performed an injection of malicious messages or commands using distance connections, a reduction of risks could be achieved by applying an Intrusion Prevention System (IPS) for CAN messages like in [14]. Regarding the physical attack via the OBD port, a risk reduction is possible by applying countermeasures (e.g. anti-theft) to avoid possible external introductions in the vehicle, giving access only to trusted specialists or to apply a security gateway between the port and the related ECU.

CONCLUSION AND FUTURE WORK

ISO/SAE 21434 is going to be the main standard for cybersecurity of E/E items in the automotive. Thus, in our work, we describe the standard, giving the reader an overview of the main contents of the norm. Then, we focus on three main possible correlations: a) with the ISO 26262 standard, b) with the regulation UNECE WP.29, and c) with the document list PPAP used for mechanical items in automotive. We identify

TABLE IV
ITEM SECURITY ANALYSIS

Cybersecurity property: C=Confidentiality I=Integrity A=Availability															
Total = ET+SE+KN+WO+EQ															
Asset	**C**	**I**	**A**	**Damage scenario**	**Threat scenario**	**Attack path**	**Impact category**	**Impact rating**	**ET**	**SE**	**KN**	**WO**	**EQ**	**Total**	**Feasibility Rating**
ECU function	-	X	X	The attacker disables any window action. The glass door is blocked in the position where it was during the attack. Loss of comfort of the driving because windows are blocked. If windows are partially or totally open, possible unfeasibility to drive or to leave the vehicle unattended.	Denial-of-service attack with the injection of malicious message in the ECU that can compromise the functionality. The attacker exploits the CAN protocol weaknesses like shown in [15].	Vehicle network connection → inject malicious message or command with CAN to ECU → ECU compromised.	Operational	Moderate	3	2	3	3	2	13	Low
Windows control	X	X	X	The driver/passengers can not control the windows, that are controlled by the attacker, so the driver must stop because the driving can be heavily disturbed with high safety risks.	Using CAN protocol weaknesses, the attacker injects messages to move the windows with `Up` and/or `Down` command.	Vehicle network connection → inject malicious commands with CAN to ECU → ECU compromised.	Operational	Severe	3	3	3	4	3	16	Very low
Force sensor function	-	X	X	The attacker disables the force sensor of the window. The window will not stop the closure even if there is an object (e.g. a hand) between the glass and the door closure, causing severe injuries to the person.	In the ECU, the attacker disables the function that receives the sensor signals.	Vehicle network connection → inject malicious message with CAN to ECU to disable sensor function → ECU compromised.	Safety	Severe	3	2	2	3	2	12	Low
						OBD port physical access → compromise the ECU which receives the sensor signal of the window.			1	2	2	4	1	10	Medium

possible limits and implementations and finally, we provide an example of the application of the ISO/SAE 21434 document list on a real system like an electric window power regulator.

Our work could be a starting point for a deep debate in the automotive community to solve the challenges that will arise in the next future about cybersecurity. For instance, it could be necessary a combined cybersecurity study on the relationship between the vehicle and the vehicular network. Another future study may be the definition of required documents according to each level of severity required for a specific item, e.g. starting from the CAL concept of ISO/SAE 21434.

ACKNOWLEDGMENT

This research work has been partly funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No 883135 (E-Corridor).

REFERENCES

[1] Y. G. Dantas, V. Nigam, and H. Ruess, "Security engineering for ISO 21434," *CoRR*, vol. abs/2012.15080, 2020. [Online]. Available: https://arxiv.org/abs/2012.15080

[2] G. Macher *et al.*, "ISO/SAE DIS 21434 automotive cybersecurity standard - in a nutshell," in *SAFECOMP 2020 Workshops, Lisbon, Portugal, September 15, 2020, Proceedings*, ser. LNCS, vol. 12235. Springer, 2020, pp. 123–135.

[3] S. Powley *et al.*, "Comparative evaluation of cybersecurity methods for attack feasibility rating per iso/sae dis 21434." Coventry University, 2021. [Online]. Available: https://www.researchgate.net/publication/339390034, accessed July, 2021.

[4] M. Brown, "Addressing the challenges of a sector in transformation and preparing to meet new cyber compliance burdens (ISO/SAE 21434)." BSI Group, 2020. [Online]. Available: https://www.bsigroup.com/en-GB/our-services/Cybersecurity-Information-Resilience/Resources/Whitepapers/automotive-cybersecurity/, accessed July, 2021.

[5] V. Sembera, "Iso/sae 21434 setting the standard for connected cars' cybersecurity." Trend Micro Research, 2020. [Online]. Available: https://documents.trendmicro.com/assets/white_papers/wp-setting-the-standard-for-connected-cars-cybersecurity.pdf, accessed July, 2021.

[6] Ultrasoc, "Cybersecurity and functional safety: the case for embedded analytics. an integrated approach to iso 26262 and iso 21434 compliance." Ultrasoc, 2019. [Online]. Available: https://semiengineering.com/cybersecurity-and-functional-safety-the-case-for-embedded-analytics/, accessed July, 2021.

[7] S. Japs, "Towards the development of the cybersecurity concept according to iso/sae 21434 using model-based systems engineering," in *2021 IEEE 29th International Requirements Engineering Conference (RE)*, 2021, pp. 486–491.

[8] Geobridge, "ISO SAE 21434 Compliance for Automotive Security." Geobridge, 2021. [Online]. Available: https://www.geobridge.net/sae-21434-explained/, accessed December, 2021.

[9] D. W. Aksnes, L. Langfeldt, and P. Wouters, "Citations, citation indicators, and research quality: An overview of basic concepts and theories," *SAGE Open*, vol. 9, no. 1, p. 2158244019829575, 2019. [Online]. Available: https://doi.org/10.1177/2158244019829575

[10] C. Schmittner and Z. Ma, "Towards a framework for alignment between automotive safety and security standards," in *Computer Safety, Reliability, and Security - SAFECOMP 2015 Workshops, ASSURE, DECSoS, ISSE, ReSA4CI, and SASSUR, Delft, The Netherlands, September 22, 2015, Proceedings*, 2015, pp. 133–143. [Online]. Available: https://doi.org/10.1007/978-3-319-24249-1_12

[11] C. Hankin. (2017) The interaction between safety and security. [Online]. Available: https://blogs.imperial.ac.uk/security-institute/2017/01/03/the-relationship-between-safety-and-security/, accessed July, 2021.

[12] A. Zarghami and D. Benbow, *Introduction to 8D problem solving : including practical applications and examples*. ASQ Quality Press, 2017.

[13] The MathWorks, Inc. Power window. [Online]. Available: https://www.mathworks.com/help/simulink/ug/power-window-example-case-study.html, accessed July, 2021.

[14] G. Costantino, I. Matteucci, and D. Morales, "EARNEST: A challenge-based intrusion prevention system for CAN messages," in *2020 IEEE International Symposium on Software Reliability Engineering Workshops, ISSRE Workshops, Coimbra, Portugal, October 12-15, 2020*. IEEE, 2020, pp. 243–248. [Online]. Available: https://doi.org/10.1109/ISSREW51248.2020.00080

[15] G. Costantino and I. Matteucci, "CANDY CREAM - hacking infotainment android systems to command instrument cluster via can data frame," in *2019 IEEE International Conference on Computational*

Science and Engineering, CSE 2019, and IEEE International Conference on Embedded and Ubiquitous Computing, EUC 2019, New York, NY, USA, August 1-3, 2019, M. Qiu, Ed. IEEE, 2019, pp. 476–481. [Online]. Available: https://doi.org/10.1109/CSE/EUC.2019.00094

Gianpiero Costantino (gianpiero.costantino@iit.cnr.it) is a researcher at the Italian National Research Council (CNR). Currently, he has been working for the Trust, Security and Privacy group within the Institute of Informatics and Telematics located in Pisa. From November 2007 to March 2011 he was a Ph.D. student at the University of Catania. He is co-author of about fifty scientific articles. He has more than 10 years' experience in cybersecurity research and, in the last five years has focused on Automotive Cybersecurity. Dr. Costantino is involved in the C3ISP, SPARTA — H2020 Projects — and WEBREPUTO — National Project —, he worked for the following project: Coco Cloud, NESSOS — FP7 — HC@WORKS-2, HC@WORKS, Trust in the Cloud — EIT Digital — Securing Smart Airport — ENISA.

Marco De Vincenzi (marco.devincenzi@iit.cnr.it) received his M.Sc. degree in Data Science and Business Informatics from the University of Pisa in 2020. He has worked in the automotive industry for the past six years with focus on quality management systems like ISO 9001:2015 and IATF 16949:2016, data analysis, and network security. He participated in European projects like NGI-Trust COSCA and E-Corridor, respectively for privacy policy analysis and information security. Actually, his research interests include data privacy and security in Intelligent Transportation System (ITS), and automotive standards analysis like ISO 21434.

Ilaria Matteucci (ilaria.matteucci@iit.cnr.it) received her M.Sc. in Mathematics in 2003, and her Ph.D. in Logic Informatics and Mathematics in 2008. She is a researcher of the Trust, Security and Privacy group within the Institute of Informatics and Telematics of CNR. Her main research interests include formal methods for the synthesis of secure systems, analysis of data sharing and policies on personal data privacy. Currently, the research interest is focused on Automotive defensive and offensive cybersecurity, with particular reference to security properties of the CAN-bus protocol and possible vulnerabilities of in-vehicle network. She participates in national and European projects in the field of information security, such as FP6 EU S3MS, FP7 EU CONNECT, Consequence, Aniketos, NeSSoS, CocoCloud, Artemis EU SESAMO, H2020 C3ISP, NGI-Trust COSCA, PRIN TENACE and GAUSS.