VDA German Association of the Automotive Industry

Position

Automotive Cyber Security

Recommendation for Cyber Security Interface Agreement (CSIA), with reference to ISO/SAE 21434

Berlin, March 2021

General

More than 675 companies from the automobile sector – including manufacturers of motor vehicles, manufacturers of their engines, trailers, superstructures and containers, and manufacturers of motor vehicle parts and accessories – have banded together in Germany within the framework of the German Association of the Automotive Industry (VDA).

The international ISO/SAE 21434 standard was released in 2021. It defines requirements that are relevant to UNECE R 155 (obligatory for the type approval of motor vehicles).

With regard to a Cyber Security Management System (CSMS), it supports the implementation of the certification of the vehicle manufacturers which is necessitated by UNECE R 155 ‘Cyber security and cyber security management system’. The use of ISO/SAE 21434 serves as a building block in the sense of a reference implementation of a CSMS, in order to simplify the required certification. ISO PAS 5112 defines a corresponding certification scheme.

ISO/SAE 21434 is made up of chapters 1 through 15, as well as annexes A through H. Its area of applicability relates to the lifecycle of the electronic and software components in motor vehicles – This covers everything from development, production, operations and maintenance to decommissioning.

This document contains recommended actions, and serves as a resource for chapters 5 through 15 of ISO/SAE 21434.

Specification of responsibilities in the Cyber Security Interface Agreement within the supply chain

The goal is to implement a security-by-design approach for vehicle systems and components, as well as backend systems. The ‘implementation’ is carried out the processes involving the corresponding work products. Vehicle systems’ cyber-security risk can thus be controlled through the entire service life, from the concept and design phase onwards.

Overview and explanation of the RASI matrix

The other individual topics relate to the current ISO/SAE 21434. They are processed in individual sections in conjunction with a particular recommended action. This is done within the framework of a RASI matrix. This matrix defines the roles of both the manufacturer (OEM or system integrator as C = Customer) and the suppliers (S = Supplier) for ten chapters, and is oriented towards the so-called work products (WP) in ISO/SAE 21434.

RASI stands for:
R = is responsible for conducting the activities resulting in the work product
A = approves the work product provided by the other party
S = supports the other party for the activities resulting in the work product
I = (informed): the organization that is informed of the progress of the activity and any decisions being made

(Organizational) Overall Cyber Security Management

Chapter 5 of ISO/SAE 21434 describes organizational measures of the company with regard to the lifecycle phases stretching up to decommissioning. For example, this includes processes and specific roles for employees.

ISO-Chapter		ISO/SAE 21434:2021	R	A	S	I	Interchange Agreement	Notes
5	Organizational Cybersecurity Management							
5 Cybersecurity Management	Cybersecurity policy, rules and processes	[WP-05-01]	S			C	short as deliverable and full at location	
	Evidence of competence management, awareness management, awareness management and continuous improvement	[WP-05-02]	S			C	short as deliverable and full at location	
	Organizational cybersecurity audit report	[WP-05-05]	S			C	short as deliverable and full at location	
	Evidence of the organization’s management systems	[WP-05-03]	S			C	short as deliverable and full at location	
	Evidence of tool management	[WP-05-04]	S			C	short as deliverable and full at location	

Project Dependent Cyber Security Management

This chapter (6) contains the requirements pertaining to the management of cyber-security-related development activities, and assigns the following roles in the matrix.

ISO-Chapter		ISO/SAE 21434:2021	R	A	S	I	Interchange Agreement	Notes
6	Project Dependent Cybersecurity Management							
6 Project Management	Cybersecurity plan	[WP-06-01]	S/C				short as deliverable and full at location	definition of deliverables and activities accoding to the OEM milestones
	Cybersecurity case	[WP-06-02]	S			C	short as deliverable and full at location	short: Summary: – evidence of Supplier that appropriate measures according Customer requirementes are implemented – reason why a case is rated without unreasonable risk
	Cybersecurity assessment report	[WP-06-03]	S			C	short as deliverable and full at location	
	Release for post-development report	[WP-06-04]	S			C	short as deliverable and full at location	

Distributed Cyber Security Activities

Chapter 7 explains the collaboration between suppliers and customers, and covers the incorporation of an agreement regarding the tasks and responsibilities into a so-called Cyber Security Interface Agreement (CSIA). A service interface agreement (LSV) can also take effect at this point. An LSV is primarily used for development projects in the automobile industry. The LSV is a document that describes the distribution of tasks and responsibilities associated with the different phases of product development across the customer, the supplier and other project participants.

Internal suppliers can be managed in the same way as external suppliers.

ISO-Chapter		ISO/SAE 21434:2021	R	A	S	I	Interchange Agreement	Notes
7	Distributed cybersecurity activities							
7 Distributed cybersecurity activities	Cybersecurity interface agreement	[WP-07-01]	S/C	S/C			full as deliverable	Supplier: Customer SDIA for delivered component/SW/HW (this document) e.g. TIER X+Supplier: Supplier SDIA for delivered component/SW/HW

Continual Cyber Security Activities

Chapter 8 defines continual cyber security activities that should be considered to be independent of a specific development project. This group includes monitoring, the evaluation of cyber security and its events, a weak-point analysis and the associated management.

ISO-Chapter		ISO/SAE 21434:2021	R	A	S	I	Interchange Agreement	Notes
8	Continual cybersecurity activities							
8 Continous Cybersecurity activities	Selected sources for cybersecurity monitoring	[WP-08-01]	S/C					Supplier: selected the sources Customer: selected the sources
	Triggers	[WP-08-02]	S/C					What degree of information is sufficient to trigger an event / incident shall be informed or aligned
	Cybersecurity events	[WP-08-03]	S/C					triage if it is an event or already an incident
	Weaknesses from cybersecurity events	[WP-08-04]	S/C			S/C	short as deliverable	weakness, vulnerability, and incident
	Vulnerability analysis	[WP-08-05]	S/C			S/C	short as deliverable	weakness, vulnerability, and incident
	Evidence of managed vulnerabilities	[WP-08-06]	S/C			S/C	short as deliverable and full at location	

Concept

The respective discoveries should be made in the concept chapter (9) through an analysis of the product's cyber security risks.

ISO-Chapter		ISO/SAE 21434:2021	R	A	S	I	Interchange Agreement	Notes
9	Concept							
9 Concept	delivered component/SW/HW definition	[WP-09-01]	S/C		S/C		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1: Out-of-context TARA performed on delivered component/SW/HW only to verify customer Security Goals/Requirements
	Threat analysis and risk assessment	[WP-09-02]	S/C		S/C		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1: Verifcation of OEM TARA of delivered component/SW/HW based on out-of-context, generic TIER1 TARA.
	Cybersecurity goals	[WP-09-03]	S/C		S/C		short as deliverable and full at location	OEM: Security Goals under responsibility of the OEM TIER1: Verifcation of OEM Security Goals of delivered component/SW/HW based on out-of-context, generic TIER1 TARA.
	Cybersecurity claims	[WP-09-04]	S/C		S/C		short as deliverable and full at location	OEM: Security Claims and Transfer under responsibility of the OEM TIER1: Verifcation of OEM Security Claims and Transfer of delivered component/SW/HW based on out-of-context, generic TIER1 TARA.
	Verification report	[WP-09-05]	S/C		S/C		short as deliverable and full at location	OEM: Verification of TARA under responsibility of the OEM TIER1: Verifcation of OEM TARA of delivered component/SW/HW based on out-of-context, generic TIER1 TARA.
	Cybersecurity concept	[WP-09-06]	S/C		S/C	S	short as deliverable and full at location	OEM: Security Concept under responsibility of the OEM, break down on individual components: („Lastenheft") TIER1: Verifcation of OEM Security Concept of delivered component/SW/HW based on out-of-context, generic TIER1 Security Concept.
	Verification report for cybersecurity concept	[WP-09-07]	S/C		S/C		short as deliverable and full at location	OEM: Verification of Security Concept under responsibility of the OEM TIER1: Verifcation of OEM Security Concept of delivered component/SW/HW based on out-of-context, generic TIER1 Security Concept.

Product development

Chapter 10 is geared towards product development. It defines requirements and tasks for product development. For example, this includes the running and checking of system analyses, the development activities, as well as specification and design. This recommendation only serves to facilitate communications, so that a common understanding can be reached at the system level. Other detailed technical requirement specifications are explicitly not envisaged.

ISO-Chapter		ISO/SAE 21434:2021	R	A	S	I	Interchange Agreement	Notes
10	Product development							
10 Product Development	Cybersecurity specifications	[WP-10-01]	S	C	C		full as deliverable	„Pflichtenheft" For mutual approval it is recommended to share the specification. (However, it might be challenging to overcome technical restrictions)
	Cybersecurity requirements for post-development	[WP-10-02]	S			C	short as deliverable	TIER1: Product Requirements according TIER1 process, delivered component/SW/HW only
	Documentation of the modelling, design, or programming languages and coding guidelines	[WP-10-03]	S			C	short as deliverable and full at location	TIER1: Guidelines, etc according TIER1 System Engineering and SW process
	Verification report for the refined cybersecurity specification	[WP-10-04]	S			C	short as deliverable and full at location	TIER1: System FMEA for Security Architecture according TIER1 process, delivered component/ SW/HW only
	Weaknesses found during product development	[WP-10-05]	S			C	short as deliverable and full at location	
	Integration and verification specification	[WP-10-06]	S		C	C	short as deliverable and full at location	TIER1: Test Specifications according TIER1 process, delivered component/SW/HW only If needed the OEM may contract suppliers to perfom additional verification tests
	Integration and verification reports	[WP-10-07]	S			C	short as deliverable and full at location	TIER1: Test Reports according TIER1 process, delivered component/SW/HW only – e.g.: – Requirements tests – Fuzz-Testing of vehicle interfaces – Penetration-Test – Vulnerabilty Report – Information on HW-/SW-BOM

Cyber Security Validation

Chapter 11 describes the activities for validating cyber security either at the vehicle level or within the vehicle. This is done after the components have been finalised, and it includes trials if trials can be carried out during operation.

ISO-Chapter		ISO/SAE 21434:2021	R	A	S	I	Interchange Agreement	Notes
11	Cybersecurity Validation							
11 Cybersecurity Validation	Validation report	[WP-11-01]	C		S		short as deliverable and full at location	OEM: Validation of Security Goals under responsibility of the OEM OEM may perfom own Penetration-Test

Production

Product includes the manufacturing and assembly of an item or component, and is explained further in chapter 12. Requirements and tasks are defined for production, in order to implement measures following from product development in the product. This is also supposed to result in more protection against subsequent cyberattacks, and strengthen the product.

ISO-Chapter		ISO/SAE 21434:2021	R	A	S	I	Interchange Agreement	Notes
12	Production							
12 Production	Production control plan	[WP-12-01]	S/C			C	short as deliverable and full at location	TIER1: Manufacturing Control Plan according TIER1 process, delivered component/SW/HW only – e.g.: – Line Control Plan – Special Characteristics List – TISAX

Operations and Maintenance

Chapter 13 deals with reactions to cyber security incidents and necessary updates.

ISO-Chapter		ISO/SAE 21434:2021	R	A	S	I	Interchange Agreement	Notes
13	Operations and Maintenance							
13 Operations and Maintenance	Cybersecurity incident response plan	[WP-13-01]	S			C	short as deliverable and full at location	

End of Cyber Security Support and decommissioning

The next-to-last chapter – clause 14 – regulates the end of support for cyber security.

ISO-Chapter		ISO/SAE 21434:2021	R	A	S	I	Interchange Agreement	Notes
14	End of Cybersecurity Support and decommissioning							
14 End of Cybersecurity Support and de-commissioning	Procedures to communicate end of cybersecurity support	[WP-14-01]	S/C		S/C	S/C	short as deliverable and full at location	TIER1+OEM: mutual information on changes in support abilities due to external factors which limits the ability to react

Threat analysis and risk assessment (TARA) methods

The matrix's final chapter – viz. number 15 – contains different risk analysis methods like attack routes, potential damages and threat type.

ISO-Chapter		ISO/SAE 21434:2021	R	A	S	I	Interchange Agreement	Notes
15	Threat analysis and risk assessment methods							
15 Threat analysis and risk assessment methods	Damage Scenarios	[WP-15-01]	C		S		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1: Out-of-context TARA performed on delivered component/SW/HW only to verify customer Security Goals/Requirements
	Assets with cybersecurity properties	[WP-15-02]	C		S		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1: Out-of-context TARA performed on delivered component/SW/HW only to verify customer Security Goals/Requirements
	Threat scenarios	[WP-15-03]	C		S		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1 (S): Out-of-context TARA performed on delivered component/SW/HW only to verify customer Security Goals/Requirements
	Impact ratings with associated impact categories	[WP-15-04]	C		S		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1 (S): Out-of-context TARA performed on delivered component/SW/HW only to verify customer Security Goals/Requirements
	Attack paths	[WP-15-05]	C		S		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1 (S): Component TARA performed on delivered component/SW/HW only to verify customer Security Goals/Requirements
	Attack feasibility ratings	[WP-15-06]	C		S		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1 (S): Component TARA performed on delivered component/SW/HW only to verify customer Security Goals/Requirements
	Attack feasibility ratings	[WP-15-07]	C		S		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1 (S): Component TARA performed on delivered component/SW/HW only to verify customer Security Goals/Requirements
	Risk treatment decisions	[WP-15-08]	C		S		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1: component TARA under responsibility of the TIER1

Annex

The scope of this agreement covers the following workproducts and the corresponding activities with respect to the framework given on sheet overview

ISO-Chapter		ISO/SAE 21434:2021	R	A	S	I	Interchange Agreement	Notes
5	Organizational Cybersecurity Management							
5 Cybersecurity Management	Cybersecurity policy, rules and processes	[WP-05-01]	S			C	short as deliverable and full at location	
	Evidence of competence management, awareness management, awareness management and continuous improvement	[WP-05-02]	S			C	short as deliverable and full at location	
	Organizational cybersecurity audit report	[WP-05-05]	S			C	short as deliverable and full at location	
	Evidence of the organization's management systems	[WP-05-03]	S			C	short as deliverable and full at location	
	Evidence of tool management	[WP-05-04]	S			C	short as deliverable and full at location	
6	Project Dependent Cybersecurity Management							
6 Project Management	Cybersecurity plan	[WP-06-01]	S/C				short as deliverable and full at location	definition of deliverables and activities accoding to the OEM milestones
	Cybersecurity case	[WP-06-02]	S			C	short as deliverable and full at location	short: Summary: – evidence of Supplier that appropriate measures according Customer requiremenes are implemented – reason why a case is rated without unreasonable risk
	Cybersecurity assessment report	[WP-06-03]	S			C	short as deliverable and full at location	
	Release for post-development report	[WP-06-04]	S			C	short as deliverable and full at location	
7	Distributed cybersecurity activities							
7 Distributed cybersecurity activities	Cybersecurity interface agreement	[WP-07-01]	S/C	S/C			full as deliverable	Supplier: Customer SDIA for delivered component/SW/HW (this document) e.g. TIER X+Supplier: Supplier SDIA for delivered component/SW/HW
8	Continual cybersecurity activities							
8 Continous Cybersecurity activities	Selected sources for cybersecurity monitoring	[WP-08-01]	S/C					Supplier: selected the sources Customer: selected the sources
	Triggers	[WP-08-02]	S/C					What degree of information is sufficient to trigger an event / incident shall be informed or aligned
	Cybersecurity events	[WP-08-03]	S/C					triage if it is an event or already an incident
	Weaknesses from cybersecurity events	[WP-08-04]	S/C			S/C	short as deliverable	weakness, vulnerability, and incident
	Vulnerability analysis	[WP-08-05]	S/C			S/C	short as deliverable	weakness, vulnerability, and incident
	Evidence of managed vulnerabilities	[WP-08-06]	S/C			S/C	short as deliverable and full at location	
9	Concept							
9 Concept	delivered component/SW/HW definition	[WP-09-01]	S/C		S/C		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1: Out-of-context TARA performed on delivered component/SW/HW only to verify customer Security Goals/Requirements
	Threat analysis and risk assessment	[WP-09-02]	S/C		S/C		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1: Verifcation of OEM TARA of delivered component/SW/HW based on out-of-context, generic TIER1 TARA.
	Cybersecurity goals	[WP-09-03]	S/C		S/C		short as deliverable and full at location	OEM: Security Goals under responsibility of the OEM TIER1: Verifcation of OEM Security Goals of delivered component/SW/HW based on out-of-context, generic TIER1 TARA.
	Cybersecurity claims	[WP-09-04]	S/C		S/C		short as deliverable and full at location	OEM: Security Claims and Transfer under responsibility of the OEM TIER1: Verifcation of OEM Security Claims and Transfer of delivered component/SW/HW based on out-of-context, generic TIER1 TARA.
	Verification report	[WP-09-05]	S/C		S/C		short as deliverable and full at location	OEM: Verification of TARA under responsibility of the OEM TIER1: Verifcation of OEM TARA of delivered component/SW/HW based on out-of-context, generic TIER1 TARA.
	Cybersecurity concept	[WP-09-06]	S/C		S/C	S	short as deliverable and full at location	OEM: Security Concept under responsibility of the OEM, break down on individual components: („Lastenheft") TIER1: Verifcation of OEM Security Concept of delivered component/SW/HW based on out-of-context, generic TIER1 Security Concept.
	Verification report for cybersecurity concept	[WP-09-07]	S/C		S/C		short as deliverable and full at location	OEM: Verification of Security Concept under responsibility of the OEM TIER1: Verifcation of OEM Security Concept of delivered component/SW/HW based on out-of-context, generic TIER1 Security Concept.

ISO-Chapter		ISO/SAE 21434:2021	R	A	S	I	Interchange Agreement	Notes
10	Product development							
10 Product Development	Cybersecurity specifications	[WP-10-01]	S	C	C		full as deliverable	„Pflichtenheft“ For mutual approval it is recommended to share the specification. (However, it might be challenging to overcome technical restrictions)
	Cybersecurity requirements for post-development	[WP-10-02]	S			C	short as deliverable	TIER1: Product Requirements according TIER1 process, delivered component/SW/HW only
	Documentation of the modelling, design, or programming languages and coding guidelines	[WP-10-03]	S			C	short as deliverable and full at location	TIER1: Guidelines, etc according TIER1 System Engineering and SW process
	Verification report for the refined cybersecurity specification	[WP-10-04]	S			C	short as deliverable and full at location	TIER1: System FMEA for Security Architecture according TIER1 process, delivered component/ SW/HW only
	Weaknesses found during product development	[WP-10-05]	S			C	short as deliverable and full at location	
	Integration and verification specification	[WP-10-06]	S		C	C	short as deliverable and full at location	TIER1: Test Specifications according TIER1 process, delivered component/SW/HW only If needed the OEM may contract suppliers to perfom additional verification tests
	Integration and verification reports	[WP-10-07]	S			C	short as deliverable and full at location	TIER1: Test Reports according TIER1 process, delivered component/SW/HW only – e.g.: – Requirements tests – Fuzz-Testing of vehicle interfaces – Penetration-Test – Vulnerabilty Report – Information on HW-/SW-BOM
11	Cybersecurity Validation							
11 Cybersecurity Validation	Validation report	[WP-11-01]	C		S		short as deliverable and full at location	OEM: Validation of Security Goals under responsibility of the OEM OEM may perfom own Penetration-Test
12	Production							
12 Production	Production control plan	[WP-12-01]	S/C			C	short as deliverable and full at location	TIER1: Manufacturing Control Plan according TIER1 process, delivered component/SW/HW only – e.g.: – Line Control Plan – Special Characteristics List – TISAX
13	Operations and Maintenance							
13 Operations and Maintenance	Cybersecurity incident response plan	[WP-13-01]	S			C	short as deliverable and full at location	
14	End of Cybersecurity Support and decommissioning							
14 End of Cybersecurity Support and de-commissioning	Procedures to communicate end of cybersecurity support	[WP-14-01]	S/C		S/C	S/C	short as deliverable and full at location	TIER1+OEM: mutual information on changes in support abilities due to external factors which limits the ability to react
15	Threat analysis and risk assessment methods							
15 Threat analysis and risk assessment methods	Damage Scenarios	[WP-15-01]	C		S		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1: Out-of-context TARA performed on delivered component/SW/HW only to verify customer Security Goals/Requirements
	Assets with cybersecurity properties	[WP-15-02]	C		S		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1: Out-of-context TARA performed on delivered component/SW/HW only to verify customer Security Goals/Requirements
	Threat scenarios	[WP-15-03]	C		S		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1 (S): Out-of-context TARA performed on delivered component/SW/HW only to verify customer Security Goals/Requirements
	Impact ratings with associated impact categories	[WP-15-04]	C		S		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1 (S): Out-of-context TARA performed on delivered component/SW/HW only to verify customer Security Goals/Requirements
	Attack paths	[WP-15-05]	C		S		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1 (S): Component TARA performed on delivered component/SW/HW only to verify customer Security Goals/Requirements
	Attack feasibility ratings	[WP-15-06]	C		S		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1 (S): Component TARA performed on delivered component/SW/HW only to verify customer Security Goals/Requirements
	Attack feasibility ratings	[WP-15-07]	C		S		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1 (S): Component TARA performed on delivered component/SW/HW only to verify customer Security Goals/Requirements
	Risk treatment decisions	[WP-15-08]	C		S		short as deliverable and full at location	OEM: TARA under responsibility of the OEM TIER1: component TARA under responsibility of the TIER1

C = Customer
S = Supplier

R is responsible for conducting the activities resulting in the work product
A approves the work product provided by the other party
S supports the other party for the activities resulting in the work product
I (informed): the organization that is informed of the progress of the activity and any decisions being made

Contact Persons

Dr. Marcus Bollig
Executive board
marcus.bollig@vda.de

Martin Lorenz
Head of the Coordination Unit for Security & Data
martin.lorenz@vda.de

Stephan Krähnert
Department of Standardization
stephan.kraehnert@vda.de

Publisher

German Association of the Automotive Industry
Behrenstraße 35, 10117 Berlin
www.vda.de/en

Registered representative R001243
EU Transparency No. 95574664768-90

Version

Version 1.0, July 2022