SESIP Mapping to ISO/SAE 21434:2021

March 2024

GLOBALPLATFORM®

THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Background

- The need for Automotive Cybersecurity increased in parallel to the development of the connected cars, vehicles are being connected to everything (V2X) – traffic lights, parking meters, other vehicles, and much more
- As the **automotive** ecosystem becomes **increasingly connected**, attack points multiply, exposing **new vulnerabilities** that hackers can exploit to threaten vehicle safety, users´ privacy, and car data integrity
- The automotive industry realized that this threats should be handled by regulation:
  - **ISO/SAE 21434** - Baseline for vehicle manufacturers and suppliers to ensure that cybersecurity risks are managed efficiently and effectively
  - **UNECE WP.29 (No.155)** - The objective of the WP.29 is to initiate and pursue actions aimed at the worldwide harmonization or development of technical regulations for vehicles
  - **Automotive Cybersecurity Management System (CSMS)** assessment was defined for auditing vehicle manufacturer or OEM's cybersecurity framework. The assessment identifies if the organisation’s processes provide a suitable cybersecurity framework across the product lifecycle and that the CSMS requirements of both the UNECE Cybersecurity Vehicle Regulation and ISO/SAE 21434 are fulfilled.

SESIP compliance to ISO/SAE DIS 21434

- ISO 21434, among the rest, is based on ISO/IEC 15408 (all parts), *Information technology - Security techniques - Evaluation criteria for IT security*

- SESIP methodology is based on ISO/IEC 15408 and more regulations which supports the requirements of ISO 21434 in the functional and environment security requirements

SESIP compliance to ISO/SAE DIS 21434

		SESIP	Notes
Sec 5	OVERALL CYBERSECURITY MANAGEMENT	✓	Covered by ALC_DVS assurance family
Sec 6	PROJECT DEPENDENT CYBERSECURITY MANAGEMENT	✓	Covered by ALC_DVS assurance family
Sec 7	CONTINUOUS CYBERSECURITY ACTIVITIES	✓	Covered by ALC_DVS, ALC_FLR & AVA_VAN assurance families
Sec 8	RISK ASSESSMENT METHODS	✓	SESIP methodology includes risk analysis for the architecture design and vulnerability. The analysis should be reflected at the Security target by Assets, Threats, Objectives and Security functional requirements description.
Sec 9	CONCEPT PHASE	✓	Covered by SESIP assurance families: ADV_FSP – functional specifications which identify the security function interfaces and environment. ADV_ARC – security architecture AGD_OPR – Operational environment security guidance

W77Q compliance to ISO/SAE DIS 21434

		SESIP	Notes
Sec 10	PRODUCT DEVELOPMENT	✓	Covered by SESIP assurance classes and families: ADV: Development ATE: Tests ALC_CMC
Sec 11	CYBERSECURITY VALIDATION	✓	Covered by SESIP assurance classes and families: AVA_VAN AGD_OPR ATE
Sec 12	PRODUCTION	✓	Covered by ALC_DVS assurance family
Sec 13	OPERATIONS AND MAINTENANCE	✓	Covered by ALC assurance classes and families: ALC_DVS ALC_FLR
Sec 14	DECOMMISSIONING	N/A	Out of scope of ISO 21434
Sec 15	DISTRIBUTED CYBERSECURITY ACTIVITIES	✓	Covered by ALC_DVS assurance families - ALC_DVS, ALC_DEL

SESIP Group expectation from GP Board

- Approving SESIP subgroup task – Mapping and methodology adjustment for the automotive security industry, while ISO21434 is the first standard to be handled.

- Identify the relevant groups for a liaison regarding ISO21434 recognition in SESIP methodology for evaluation

Thank You

Rachel Menda-Shabat

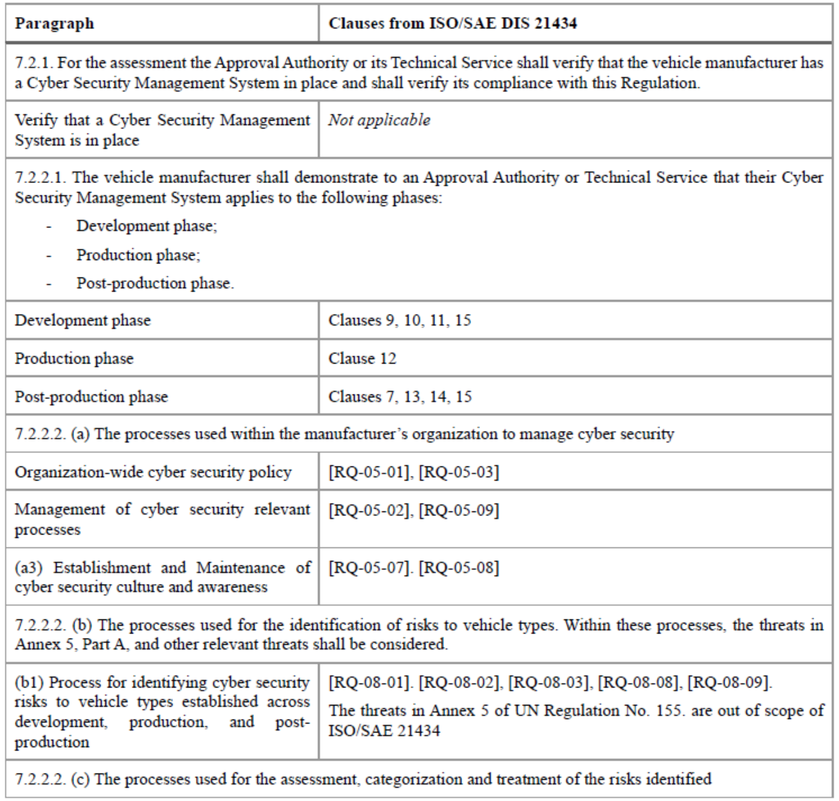
Director of Security Solution Certification Division, Winbond

Nov 16, 2021

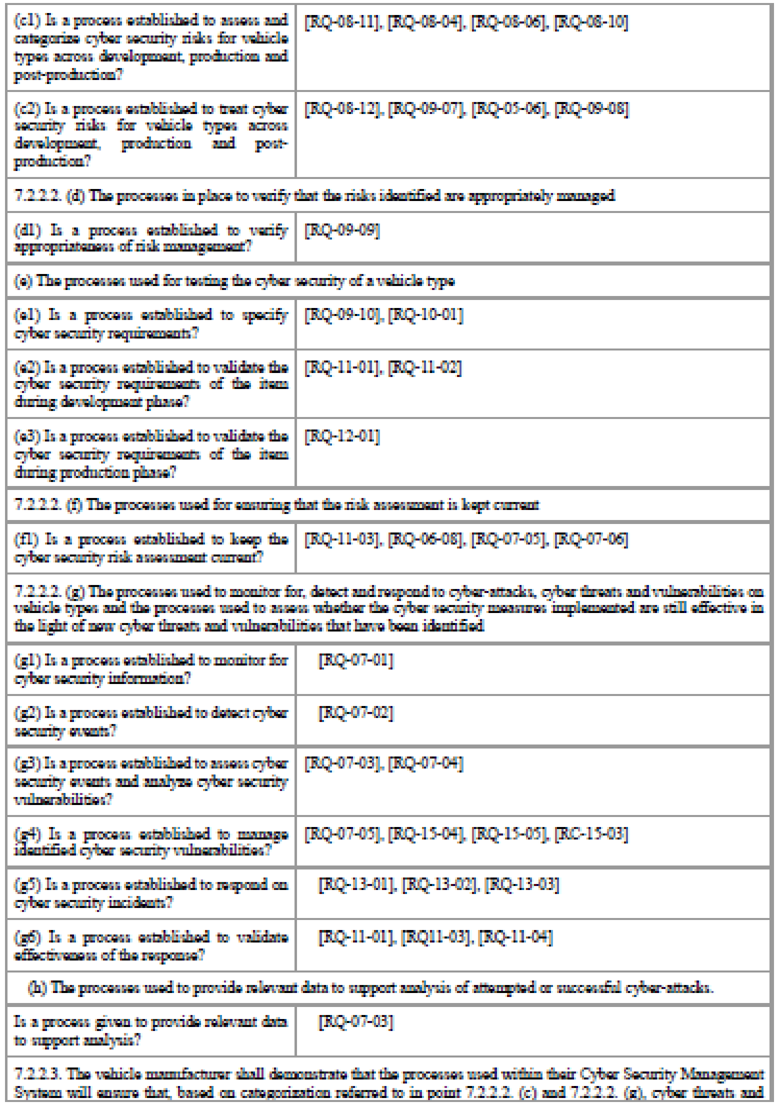
GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Backup

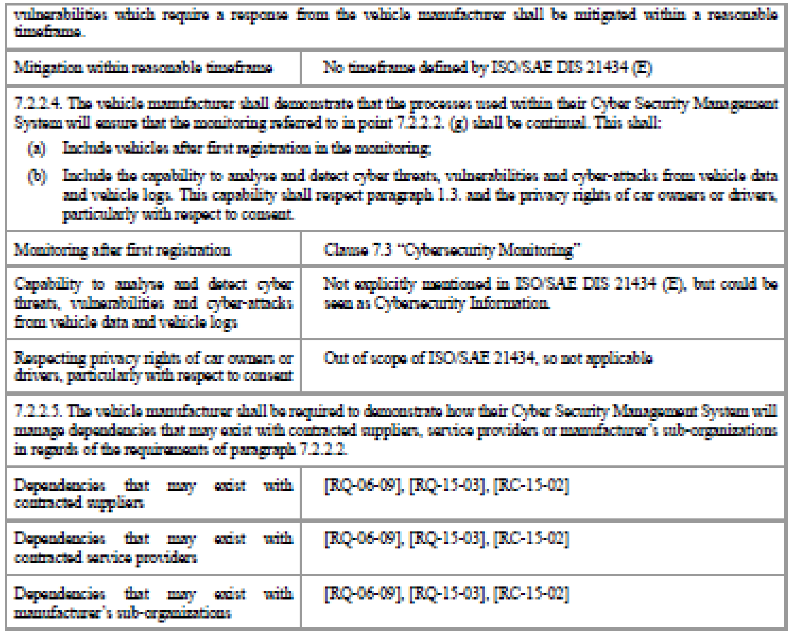
Link between WP.29 and ISO/SAE DIS 21434



Paragraph	Clauses from ISO/SAE DIS 21434
7.2.1. For the assessment the Approval Authority or its Technical Service shall verify that the vehicle manufacturer has a Cyber Security Management System in place and shall verify its compliance with this Regulation.	
Verify that a Cyber Security Management System is in place	*Not applicable*
7.2.2.1. The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System applies to the following phases: - Development phase; - Production phase; - Post-production phase.	
Development phase	Clauses 9, 10, 11, 15
Production phase	Clause 12
Post-production phase	Clauses 7, 13, 14, 15
7.2.2.2. (a) The processes used within the manufacturer's organization to manage cyber security	
Organization-wide cyber security policy	[RQ-05-01], [RQ-05-03]
Management of cyber security relevant processes	[RQ-05-02], [RQ-05-09]
(a3) Establishment and Maintenance of cyber security culture and awareness	[RQ-05-07]. [RQ-05-08]
7.2.2.2. (b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats shall be considered.	
(b1) Process for identifying cyber security risks to vehicle types established across development, production, and post-production	[RQ-08-01]. [RQ-08-02], [RQ-08-03], [RQ-08-08], [RQ-08-09]. The threats in Annex 5 of UN Regulation No. 155. are out of scope of ISO/SAE 21434
7.2.2.2. (c) The processes used for the assessment, categorization and treatment of the risks identified	

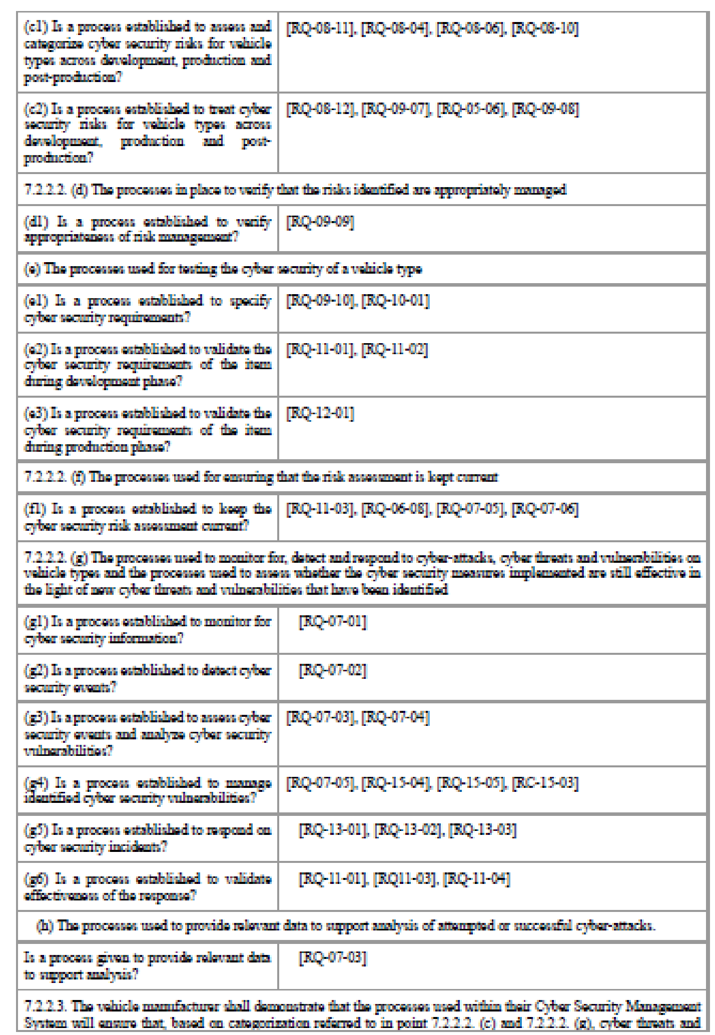


(c1) Is a process established to assess and categorize cyber security risks for vehicle types across development, production and post-production?	[RQ-08-11], [RQ-08-04], [RQ-08-06], [RQ-08-10]
(c2) Is a process established to treat cyber security risks for vehicle types across development, production and post-production?	[RQ-08-12], [RQ-09-07], [RQ-05-06], [RQ-09-08]
7.2.2.2. (d) The processes in place to verify that the risks identified are appropriately managed	
(d1) Is a process established to verify appropriateness of risk management?	[RQ-09-09]
(e) The processes used for testing the cyber security of a vehicle type	
(e1) Is a process established to specify cyber security requirements?	[RQ-09-10], [RQ-10-01]
(e2) Is a process established to validate the cyber security requirements of the item during development phase?	[RQ-11-01], [RQ-11-02]
(e3) Is a process established to validate the cyber security requirements of the item during production phase?	[RQ-12-01]
7.2.2.2. (f) The processes used for ensuring that the risk assessment is kept current	
(f1) Is a process established to keep the cyber security risk assessment current?	[RQ-11-03], [RQ-06-08], [RQ-07-05], [RQ-07-06]
7.2.2.2. (g) The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified	
(g1) Is a process established to monitor for cyber security information?	[RQ-07-01]
(g2) Is a process established to detect cyber security events?	[RQ-07-02]
(g3) Is a process established to assess cyber security events and analyze cyber security vulnerabilities?	[RQ-07-03], [RQ-07-04]
(g4) Is a process established to manage identified cyber security vulnerabilities?	[RQ-07-05], [RQ-15-04], [RQ-15-05], [RC-15-03]
(g5) Is a process established to respond on cyber security incidents?	[RQ-13-01], [RQ-13-02], [RQ-13-03]
(g6) Is a process established to validate effectiveness of the response?	[RQ-11-01], [RQ11-03], [RQ-11-04]
(h) The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.	
Is a process given to provide relevant data to support analysis?	[RQ-07-03]
7.2.2.3. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that, based on categorization referred to in point 7.2.2.2. (c) and 7.2.2.2. (g), cyber threats and	

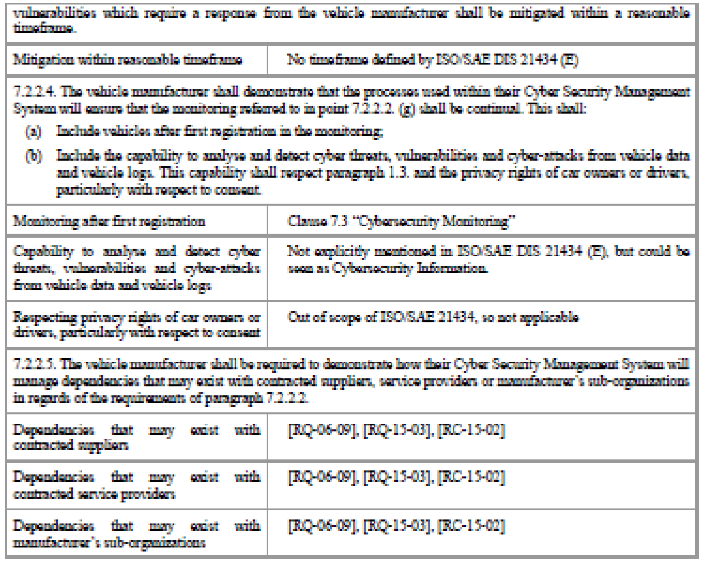


vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe.	
Mitigation within reasonable timeframe	No timeframe defined by ISO/SAE DIS 21434 (E)
7.2.2.4. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that the monitoring referred to in point 7.2.2.2. (g) shall be continual. This shall: (a) Include vehicles after first registration in the monitoring; (b) Include the capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect paragraph 1.3. and the privacy rights of car owners or drivers, particularly with respect to consent.	
Monitoring after first registration	Clause 7.3 "Cybersecurity Monitoring"
Capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs	Not explicitly mentioned in ISO/SAE DIS 21434 (E), but could be seen as Cybersecurity Information.
Respecting privacy rights of car owners or drivers, particularly with respect to consent	Out of scope of ISO/SAE 21434, so not applicable
7.2.2.5. The vehicle manufacturer shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations in regards of the requirements of paragraph 7.2.2.2.	
Dependancies that may exist with contracted suppliers	[RQ-06-09], [RQ-15-03], [RC-15-02]
Dependancies that may exist with contracted service providers	[RQ-06-09], [RQ-15-03], [RC-15-02]
Dependancies that may exist with manufacturer's sub-organizations	[RQ-06-09], [RQ-15-03], [RC-15-02]

Link between WP.29 and ISO/SAE DIS 21434



(c1) Is a process established to assess and categorize cyber security risks for vehicle types across development, production and post-production?	[RQ-08-11], [RQ-08-04], [RQ-08-06], [RQ-08-10]
(c2) Is a process established to treat cyber security risks for vehicle types across development, production and post-production?	[RQ-08-12], [RQ-09-07], [RQ-05-06], [RQ-09-08]
7.2.2.2. (d) The processes in place to verify that the risks identified are appropriately managed	
(d1) Is a process established to verify appropriateness of risk management?	[RQ-09-09]
(e) The processes used for testing the cyber security of a vehicle type	
(e1) Is a process established to specify cyber security requirements?	[RQ-09-10], [RQ-10-01]
(e2) Is a process established to validate the cyber security requirements of the item during development phase?	[RQ-11-01], [RQ-11-02]
(e3) Is a process established to validate the cyber security requirements of the item during production phase?	[RQ-12-01]
7.2.2.2. (f) The processes used for ensuring that the risk assessment is kept current	
(f1) Is a process established to keep the cyber security risk assessment current?	[RQ-11-03], [RQ-06-08], [RQ-07-05], [RQ-07-06]
7.2.2.2. (g) The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified	
(g1) Is a process established to monitor for cyber security information?	[RQ-07-01]
(g2) Is a process established to detect cyber security events?	[RQ-07-02]
(g3) Is a process established to assess cyber security events and analyze cyber security vulnerabilities?	[RQ-07-03], [RQ-07-04]
(g4) Is a process established to manage identified cyber security vulnerabilities?	[RQ-07-05], [RQ-15-04], [RQ-15-05], [RC-15-03]
(g5) Is a process established to respond on cyber security incidents?	[RQ-13-01], [RQ-13-02], [RQ-13-03]
(g6) Is a process established to validate effectiveness of the response?	[RQ-11-01], [RQ11-03], [RQ-11-04]
(h) The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.	
Is a process given to provide relevant data to support analysis?	[RQ-07-03]
7.2.2.3. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that, based on categorization referred to in point 7.2.2.2. (c) and 7.2.2.2. (g), cyber threats and	



vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe.	
Mitigation within reasonable timeframe	No timeframe defined by ISO/SAE DIS 21434 (E)
7.2.2.4. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that the monitoring referred to in point 7.2.2.2. (g) shall be continual. This shall: (a) Include vehicles after first registration in the monitoring; (b) Include the capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect paragraph 1.3. and the privacy rights of car owners or drivers, particularly with respect to consent.	
Monitoring after first registration	Clause 7.3 "Cybersecurity Monitoring"
Capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs	Not explicitly mentioned in ISO/SAE DIS 21434 (E), but could be seen as Cybersecurity Information.
Respecting privacy rights of car owners or drivers, particularly with respect to consent	Out of scope of ISO/SAE 21434, so not applicable
7.2.2.5. The vehicle manufacturer shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations in regards of the requirements of paragraph 7.2.2.2.	
Dependencies that may exist with contracted suppliers	[RQ-06-09], [RQ-15-03], [RC-15-02]
Dependencies that may exist with contracted service providers	[RQ-06-09], [RQ-15-03], [RC-15-02]
Dependencies that may exist with manufacturer's sub-organizations	[RQ-06-09], [RQ-15-03], [RC-15-02]

ISO/SAE DIS 21434 ACTIVITIES AND WORK PRODUCTS VS. SESIP methodology expected Deliveries

Activities		Raw material exist at SESIP	Work Products	
Organization Culture				
Cybersecurity Management	5. Overall Cybersecurity Management	YES	[WP-05-01] [WP-05-02] [WP-05-03] [WP-05-04] [WP-05-05]	**Cybersecurity policy, rules and processes** **Evidence of competence management, awareness management and continuous improvement** **Organizational cybersecurity audit report** **Evidence of the organization's management systems** **Evidence of tool management**
	6. Project Dependent Cybersecurity Management	YES	[WP-06-01] [WP-06-02] [WP-06-03] [WP-06-04]	**Cybersecurity plan** **Cybersecurity case** **Cybersecurity assessment report** **Release for post-development report**
Continuous Cybersecurity Activities				
Continuous Cybersecurity Activities	7.3 Cybersecurity Monitoring	YES	[WP-07-01] [WP-07-02]	**List of sources for cybersecurity monitoring** **Results from the triage of cybersecurity information**
	7.4 Cybersecurity Event Assessment	YES	[WP-07-03]	**Cybersecurity event assessment**
	7.5 Vulnerability Analysis	YES	[WP-07-04]	**Vulnerability analysis**
	7.6 Vulnerability Management	YES	[WP-07-05]	**Rationale for the managed vulnerability**
Concept and Product Development Phases				
Risk Assessment Methods	8.3 Asset Identification	YES	[WP-08-01] [WP-08-02]	**Damage scenarios** **Identified assets and cybersecurity properties**
	8.4 Threat Scenario Identification	YES	[WP-08-03]	**Threat scenarios**
	8.5 Impact Rating	YES	[WP-08-04]	**Impact rating, including the associated impact categories of the damage scenarios**
	8.6 Attack Path Analysis	YES	[WP-08-05]	**Identified attack paths**
	8.7 Attack Feasibility Rating	YES	[WP-08-06]	**Attack feasibility rating**
	8.8 Risk Determination	YES	[WP-08-07]	**Risk value**
	8.9 Risk Treatment Decision	YES	[WP-08-08]	**Risk treatment decision per threat scenario**
Concept Phase	9.3 Item Definition	YES	[WP-09-01]	**Item definition**
	9.4 Cybersecurity Goals	YES	[WP-09-02] [WP-09-03] [WP-09-04] [WP-09-05] [WP-09-06]	**Threat analysis and risk assessment** **Risk treatment decisions** **Cybersecurity goals** **Cybersecurity claims** **Verification report**
	9.5 Cybersecurity Concept	YES	[WP-09-07] [WP-09-08]	**Cybersecurity concept** **Verification report of cybersecurity concept**

ISO/SAE DIS 21434 ACTIVITIES AND WORK PRODUCTS VS. SESIP methodology expected Deliveries (Cont.)

Activities		Raw material exist in SESIP	Work Products
Product Development Phases	10.4.1 Refinement of Cybersecurity Requirements and Architectural Design	YES	[WP-10-01] Refined cybersecurity specification
		YES	[WP-10-02] Cybersecurity requirements for post-development
		YES	[WP-10-03] Verification report for the refined cybersecurity specification
	10.4.2 Integration and Verification 10.4.3 Specific Requirements for Software Development	YES	[WP-10-04] Vulnerability analysis report
		YES	[WP-10-05] Integration and verification specification
		YES	[WP-10-06] Integration and verification reports
		YES	[WP-10-07] Documentation of the modelling, design, or programming languages and coding guidelines
		YES	[WP-10-08] Software unit design and software unit implementation
	11. Cybersecurity Validation of the Item at Vehicle Level	YES	[WP-11-01] Validation specification [WP-11-02] Validation report
Post-Development phases			
	12. Production	YES	[WP-12-01] Production control plan
	13.3 Cybersecurity Incident Response	YES	[WP-13-01] Cybersecurity incident response plan [WP-13-02] Cybersecurity incident response information
	13.4 Updates	YES	[WP-13-03] Procedures to communicate end of cybersecurity support
	14. Decommissioning	None	
Supporting Processes			
	15. Distributed Cybersecurity Activities	YES	[WP-15-01] Cybersecurity interface agreement