Clause 9: Concept

Clause 9: Concept

Definitions

Item: component or set of components that implement a function at the vehicle level

Asset: An object or an item that has cybersecurity properties upon compromising can lead to severe damage to an item’s physical value and its stakeholder

Component: Part of an item that is ideally separated by logically and separable

Function(s): Intended behavior of the item during the lifecycle phase and vehicle functionality that’s defined for an item

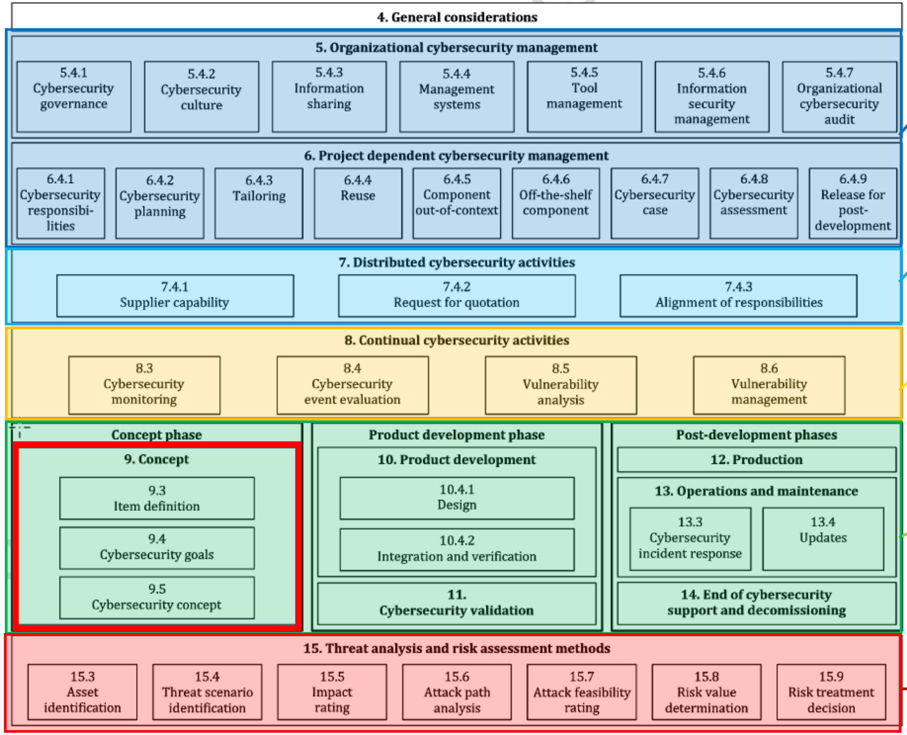
Threat scenario: Statement of potential negative actions that lead to a damage scenario

Damage scenario: Adverse consequence or undesirable result due to the compromise of a cybersecurity property(s) of an asset or a group of assets

Vulnerability: Weakness that can be exploited by a threat scenario

Risk: Effect of uncertainty on-road vehicle cybersecurity (3.1.8) expressed in terms of attack feasibility (3.1.3) and impact

Structure of ISO 21434



4. General considerations

5. Organizational cybersecurity management

- 5.4.1 Cybersecurity governance
- 5.4.2 Cybersecurity culture
- 5.4.3 Information sharing
- 5.4.4 Management systems
- 5.4.5 Tool management
- 5.4.6 Information security management
- 5.4.7 Organizational cybersecurity audit

6. Project dependent cybersecurity management

- 6.4.1 Cybersecurity responsibilities
- 6.4.2 Cybersecurity planning
- 6.4.3 Tailoring
- 6.4.4 Reuse
- 6.4.5 Component out-of-context
- 6.4.6 Off-the-shelf component
- 6.4.7 Cybersecurity case
- 6.4.8 Cybersecurity assessment
- 6.4.9 Release for post-development

7. Distributed cybersecurity activities

- 7.4.1 Supplier capability
- 7.4.2 Request for quotation
- 7.4.3 Alignment of responsibilities

8. Continual cybersecurity activities

- 8.3 Cybersecurity monitoring
- 8.4 Cybersecurity event evaluation
- 8.5 Vulnerability analysis
- 8.6 Vulnerability management

Concept phase

9. Concept

- 9.3 Item definition
- 9.4 Cybersecurity goals
- 9.5 Cybersecurity concept

Product development phase

10. Product development

- 10.4.1 Design
- 10.4.2 Integration and verification

11. Cybersecurity validation

Post-development phases

12. Production

13. Operations and maintenance

- 13.3 Cybersecurity incident response
- 13.4 Updates

14. End of cybersecurity support and decomissioning

15. Threat analysis and risk assessment methods

- 15.3 Asset identification
- 15.4 Threat scenario identification
- 15.5 Impact rating
- 15.6 Attack path analysis
- 15.7 Attack feasibility rating
- 15.8 Risk value determination
- 15.9 Risk treatment decision

Overall & project specific management processes

(similar to ISO 26262) :

- Management Systems
- Policies
- Preparation for assessment

Distributed CS activities

- Define interfaces between customer, supplier, third parties..

Continual CS Activities :

- Requirements for continuous monitoring of CS relevant information
- Framework for analysis and management of vulnerabilities

Concept, Development and Post-Development

- Add-on of CS relevant activities during concept and development :
  - Establishment of CS goals and requirements
  - TARA and vulnerability analysis during development
- Consideration of post-development requirements (during of after production, decommissioning …)
- Definition of post development processes (Production, Incident response, Update)

TARA : Threat Analysis and Risk Assessment

- Describes the steps to perform a robust risk analysis on the system
- Complex process to be performed multiple times and for multiple assets

Clause 9: Concept

DEKRA DIGITAL

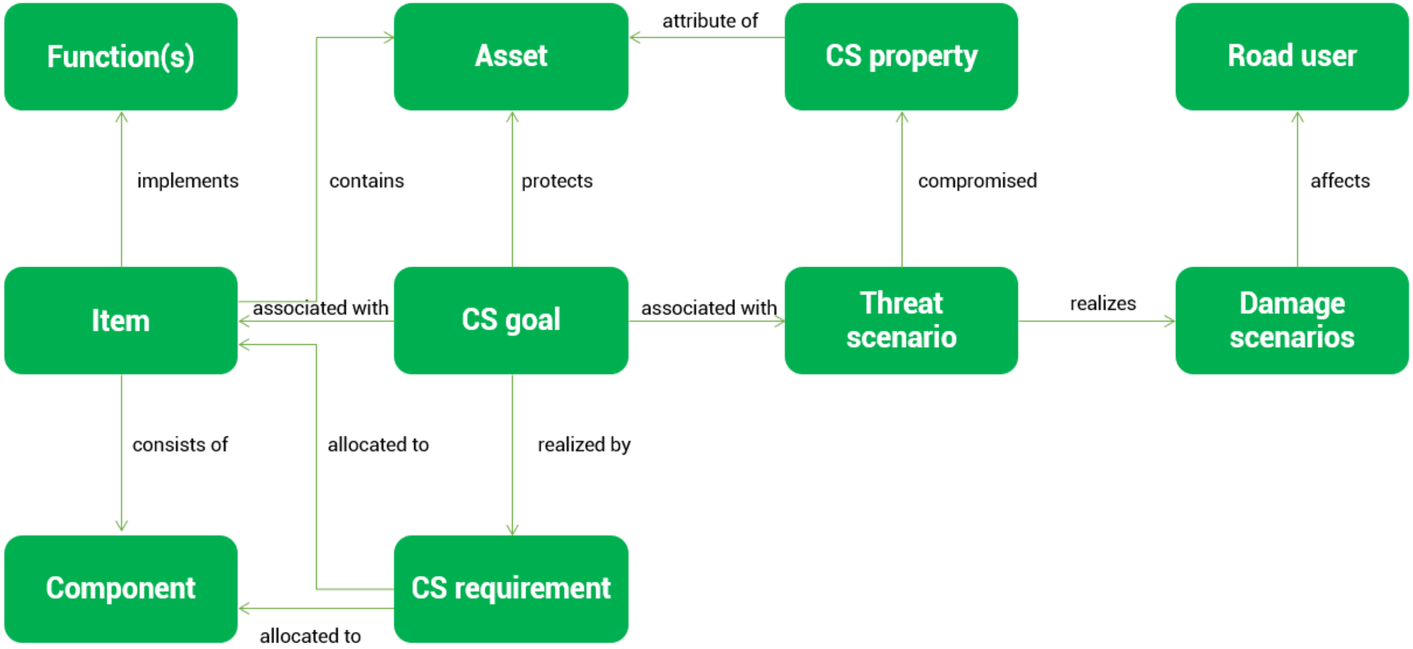


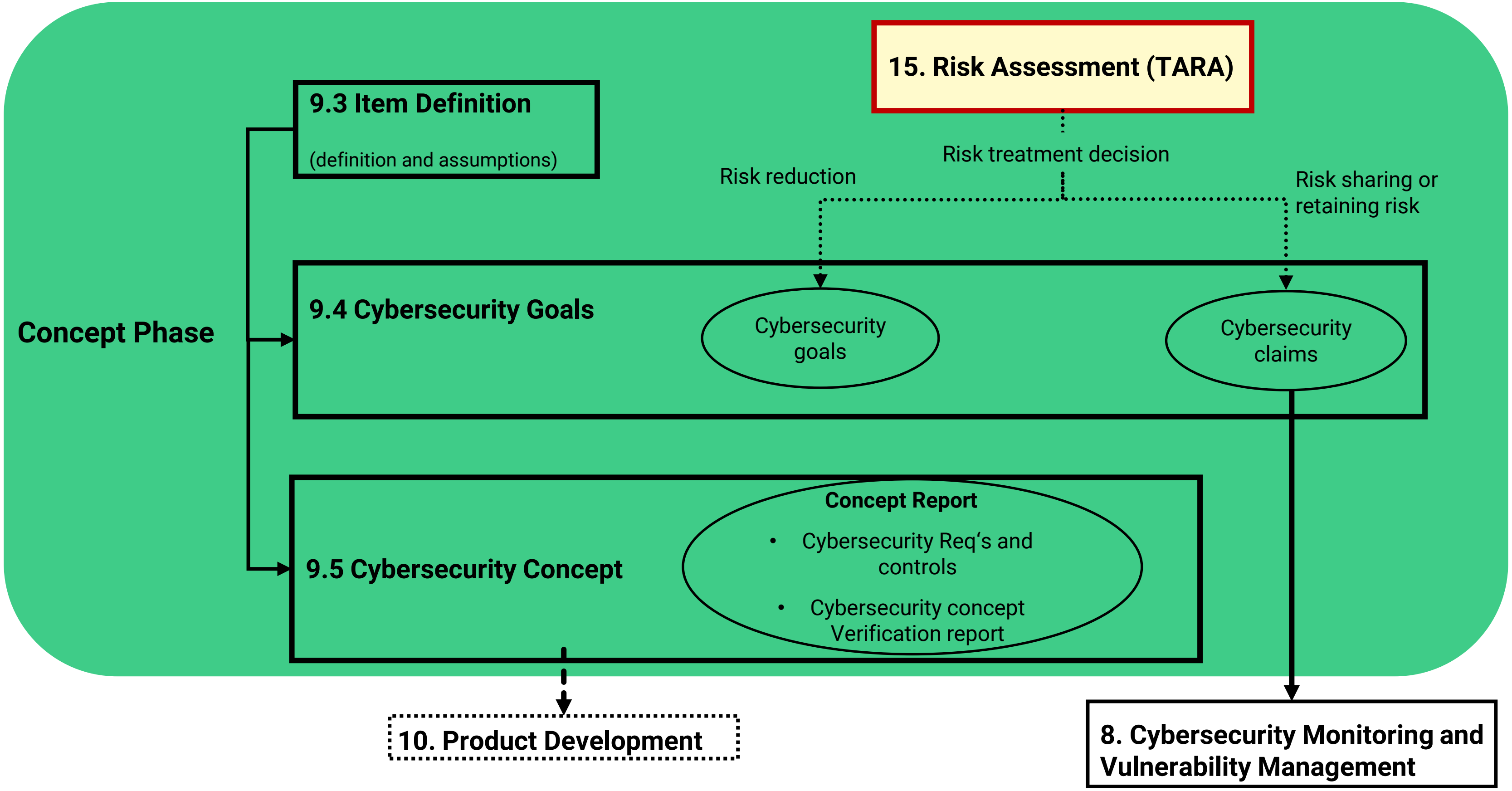
Figure 1 - Relationship between Item, functions and components as given in ISO/SAE 21434:2021

Clause 9: Concept

Why do we need the Cybersecurity concept?

- In general, this clause helps in defining the items and their environment for subsequent activities
- The main goal of this clause is to determine the cybersecurity goals and claims associated with an item and its operational environment
- Risk(s) would be identified in the concept phase, these risks should be documented and managed before the application development and further activities begin
- The cybersecurity concept report is the highest level of requirements document which defines how the cybersecurity goals will be fulfilled while developing an item and its associated components

Clause 9: Concept



15. Risk Assessment (TARA)

Risk treatment decision

Risk reduction

Risk sharing or retaining risk

9.3 Item Definition

(definition and assumptions)

Concept Phase

9.4 Cybersecurity Goals

Cybersecurity goals

Cybersecurity claims

9.5 Cybersecurity Concept

Concept Report

- Cybersecurity Req's and controls
- Cybersecurity concept Verification report

10. Product Development

8. Cybersecurity Monitoring and Vulnerability Management

Clause 9: Concept

Item Definition

- Item is a feature/product or a combination of features to implement a function at the vehicle level
- The operational environment (internal and external) of the item functions and interactions

Key Requirements

1. **Item Boundary**
   - A clear separation of the item and its operational environment
   - Item’s external and internal interfaces to other items or components in the vehicle can be included
2. **Item Functions**
   - Describes expected functionality or behavior at certain lifecycle phases of an item. The vehicle functionality directly depends on the behavior determined by the item
   - Lifecycle phases (ex: product development (testing), production, operations and maintenance, decommissioning)

Clause 9: Concept

3. **Preliminary Architecture**

- An architecture is a blueprint that gives a component level description and its dependencies
- Component interfaces, connections, data traverse, etc. Are taken into consideration

4. **Constraints and compliance**

- Functional or technical constraints, regulations, standards, etc., that need to be complied with. This includes cybersecurity development principles of the organization

Operational Environment

- Describing the operational environment in which the item should work always helps in realizing the underlying threat scenarios and attacks on the system
- The environment considered includes hardware, software, and relevant dependencies the system is expected to work with
- Assumptions are allowed to be made with relevant information
  - e.g., Digital certificates generated while data exchanging between two components are managed as required

Clause 9: Concept

Example: Headlamp System

- Item – Headlamp system
- Item Function – Basic functional overview of the headlamp system is as follows
  - The system turns on/off the headlamp according to the switch based on the user demand
  - Automatic headlamp switch from high beam to low beam upon oncoming vehicle is detected and vice versa when an oncoming vehicle is no longer detected
- Item Boundary and Preliminary architecture are defined in the item’s base architecture, refer figure in the next slide

Clause 9: Concept

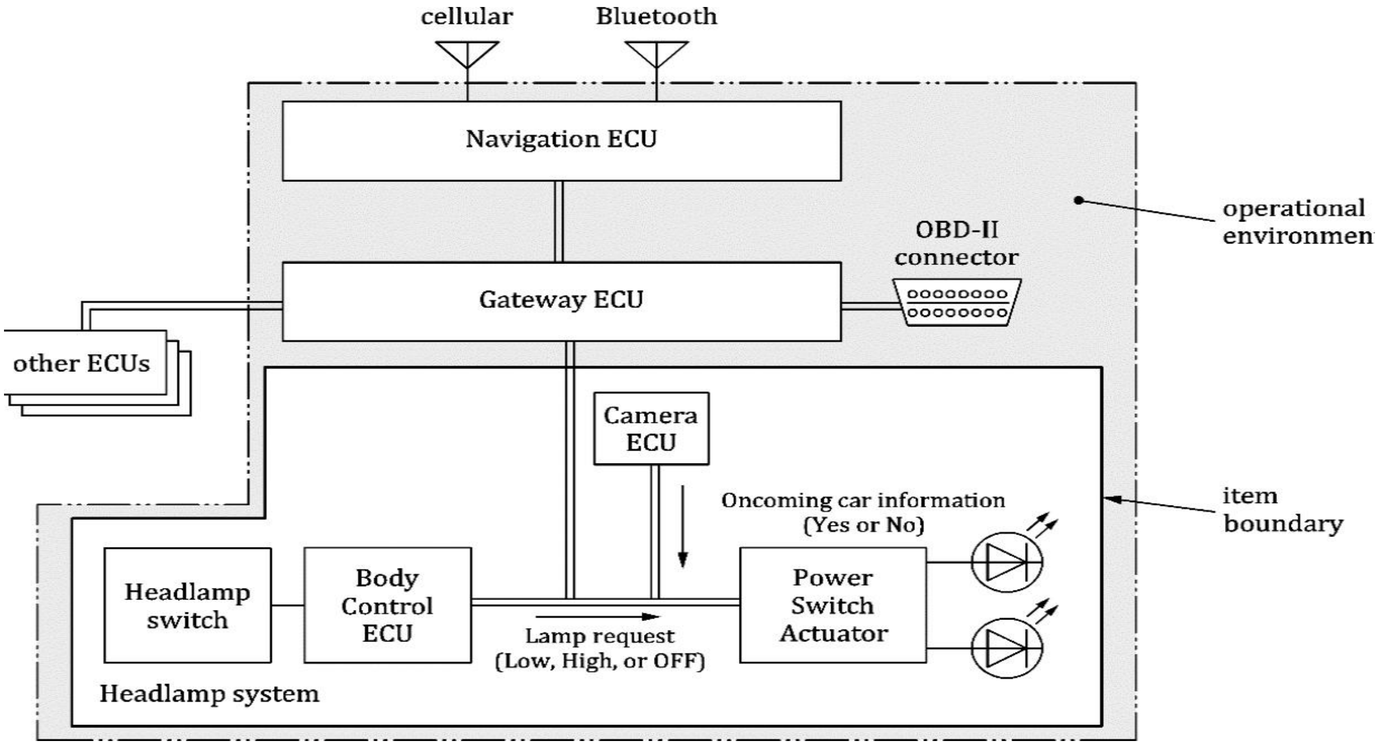


Figure.2 Example of item boundary and preliminary architecture of the headlamp according to ISO 21434

Clause 9: Concept

Table-1:

Example Description for the operational environment as per ISO 21434

Operational Environment for Headlamp System
The item (headlamp system) is connected with the gateway ECU, and the gateway ECU relates to the navigation ECU by data communication.
Navigation ECU has external communication interfaces • Bluetooth • Cellular Assumption: • Navigation ECU has a firewall to prevent invalid data communication from external interfaces.
Gateway ECU has external communication interfaces • OBD-II Assumption: • Gateway ECU has strong security controls including a firewall function (developed as CAL4).
The item is physically protected by anti-tamper enclosures, which is an assumption on the operational environment.

Clause 9: Concept

Cybersecurity Goals

- Cybersecurity goal is a concept level requirement to protect assets against one or more threat scenarios
- Cybersecurity goals are set for each, and every individual item based on their definition and initial TARA
- Cybersecurity requirements and employed security controls aim to attain the security goal This will establish a connection between security goal and security requirements

Key Requirements

1. Initial risk assessment for an item is performed based on the following steps
   - asset identification
   - threat scenario identification
   - impact rating
   - attack path analysis
   - attack feasibility rating
   - risk value determination

Clause 9: Concept

2. For all the cybersecurity risks that are to be reduced/treated cybersecurity goals should be assigned

3. Risk treatment decision for a threat scenario

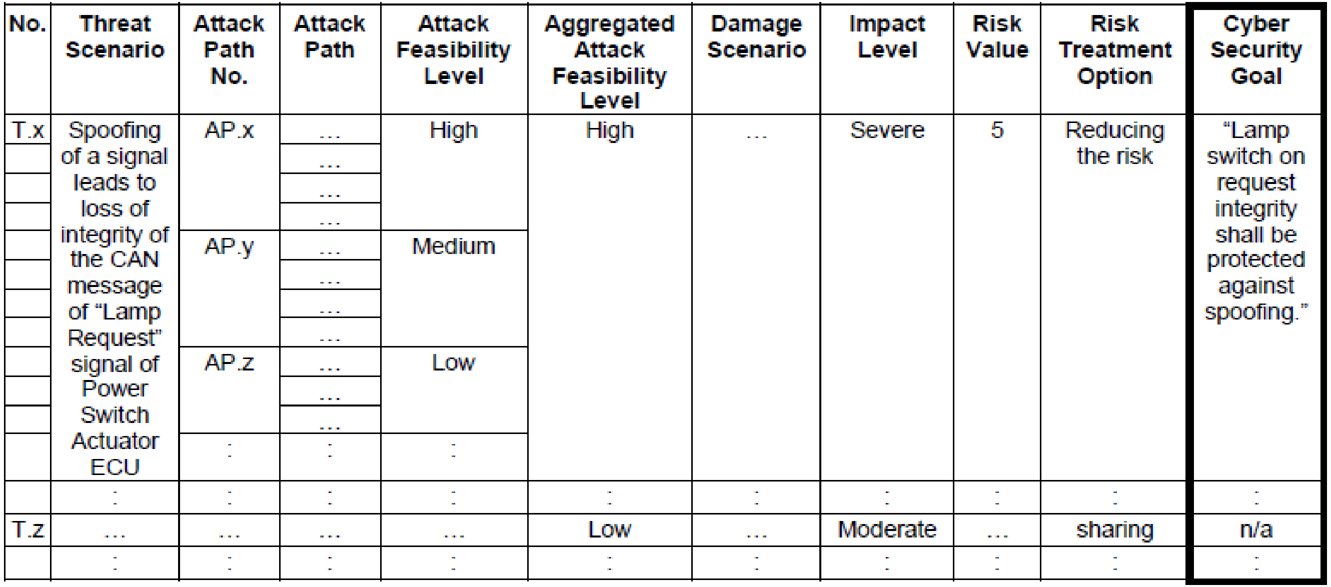
- cybersecurity assurance level (CAL) level can be determined for corresponding goals
- goals can be specified at any point of the Item's lifecycle phase
- sharing, transferring, or retaining of the risks based on the assumptions will be done by mentioning corresponding cybersecurity claims as part of the goals

4. Verification report for cybersecurity goals

- correctness and completeness of the item definition analysis
- completeness, correctness, and consistency of the
  - Risk treatment decision made based on the analysis
  - Cybersecurity goals and claims for the risk treatment decisions

Clause 9: Concept

Example: Cybersecurity Goal(s) for Headlamp system



No.	Threat Scenario	Attack Path No.	Attack Path	Attack Feasibility Level	Aggregated Attack Feasibility Level	Damage Scenario	Impact Level	Risk Value	Risk Treatment Option	Cyber Security Goal
T.x	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU	AP.x	...	High	High	...	Severe	5	Reducing the risk	"Lamp switch on request integrity shall be protected against spoofing."
			...							
			...							
			...							
		AP.y	...	Medium						
			...							
			...							
			...							
		AP.z	...	Low						
			...							
			...							
		:	:	:						
	:	:	:	:	:	:	:	:	:	:
T.z	...	...	...	...	Low	...	Moderate	...	sharing	n/a
	:	:	:	:	:	:	:	:	:	:

Note: A complete TARA is performed initially while deriving goals and explained in detail under the clause 15

Figure 3: Example cybersecurity goals derived for Headlamp system as given in ISO 21434 DIS version

Clause 9: Concept

Example: Cybersecurity Goal(s) for Headlamp system

Related Threat Scenario or Related Assumption	Cybersecurity Claim
T.z from figure 3 Treatment option: sharing	Risk of T.z is transferred to insurance. It is adequate because its impact level is low, and its aggregated attack feasibility is moderate. If the insurance does not match to the risk, its risk treatment is re-considered
Assumption on the operational environment - The item is physically protected by anti-tamper enclosures	Assumption A.1 (see Table G.1) is satisfied. If the assumption is failed to be satisfied, risks related to the assumption are (identified and) managed.
…	…

Note: A complete TARA is performed initially to derive CS goals and explained in detail under the clause 15

Table 2- Example cybersecurity claims derived for Headlamp system as given in ISO 21434 DIS version

Clause 9: Concept

DEKRA DIGITAL

Cybersecurity assurance levels (CAL)

- CALs are a classification system that is used to specify assurance requirements categorically in order to protect the assets of an item or component that are being developed in all phases of the product life cycle
- CAL is usually determined by the organization responsible for product development and it helps to address risk mitigation for threat scenarios in product development phases precisely

Determining CAL

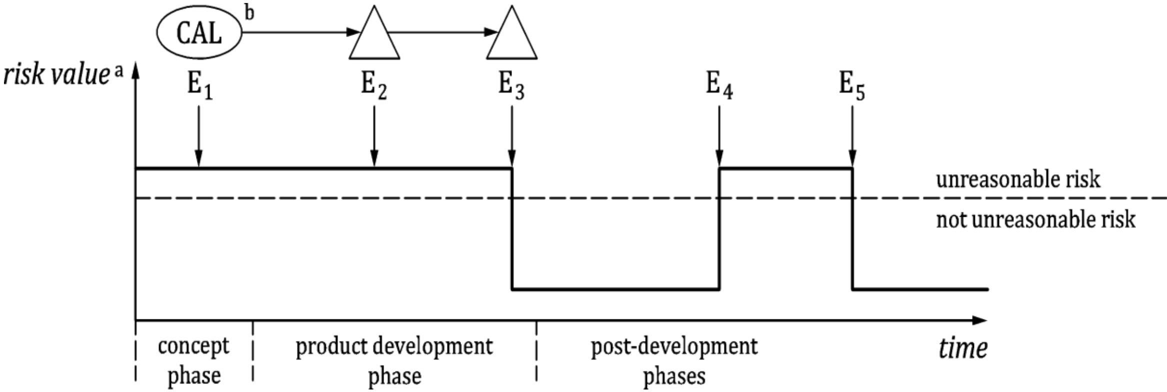
- CAL cannot be determined directly by risk value, as the risk value is dynamic and changes over the time as design, implementation, and operational environment of the product
- CAL is determined usually at the start of development during the concept phase by considering parameters like impact and attack vectors which are likely to remain constant

Clause 9: Concept

Determining CAL

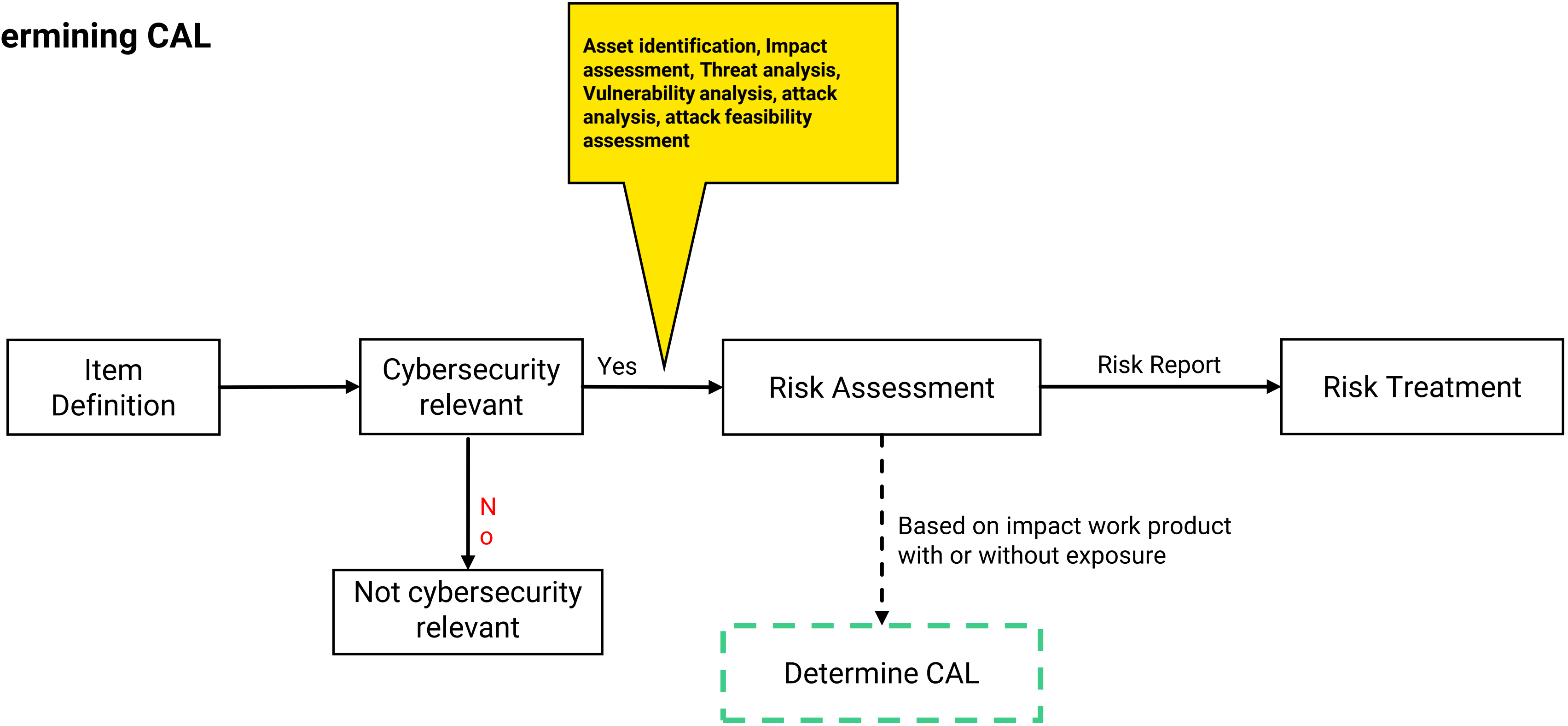
Relation between Risk and CAL

- Event 1(E1): Cybersecurity requirement is specified
- Event 2(E2): Cybersecurity control is implemented
- Event 3(E3): Test shows cybersecurity control is effective
- Event 4(E4): Vulnerability is discovered in the field
- Event 5(E5): Vulnerability is fixed
- CAL is determined at E1, concept phase and applied(△) in the following phases



Clause 9: Concept

Determining CAL



Asset identification, Impact assessment, Threat analysis, Vulnerability analysis, attack analysis, attack feasibility assessment

Based on impact work product with or without exposure

Clause 9: Concept

Determining CAL

- There are 4 CAL levels (CAL 1,2,3,4) that are available to assign for an impact based on the threat scenario identified
- Each CAL helps in knowing the level of rigor with which cybersecurity activities are performed

		Attack vector			
		Physical	Local	Adjacent	Network
Impact	Severe	CAL2	CAL3	CAL4	CAL4
	Major	CAL1	CAL2	CAL3	CAL4
	Moderate	CAL1	CAL1	CAL2	CAL3
	Negligible	-	-	-	-

Clause 9: Concept

Using CAL

- The table explains CAL levels and their corresponding description
- These CAL levels can be applied to each cybersecurity goal and any of the cybersecurity activities
- CAL does not provide any technical requirements

CAL	Description
CAL 1	Low to moderate cybersecurity assurance is required
CAL 2	Moderate cybersecurity assurance is required
CAL 3	Moderate to high cybersecurity assurance is required
CAL 4	High cybersecurity assurance is required

Clause 9: Concept

Using CAL

- Definition of the level of rigor required in the different CAL levels

CAL	Description
CAL 1	Functionally and structurally tested. Perform testing activities and vulnerability analysis. Confident in correct operation is required, but the threats to security are not viewed as serious
CAL 2	Methodically tested and checked. Ensures moderate confident that the item will not be tampered with during development
CAL 3	Methodically designed, tested and checked. Requires more design description, implementation representation for security functions and improved procedures to provide high confident that the item will not be tampered with during development
CAL 4	Advanced methodically designed, tested and reviewed. Perform independent vulnerability analysis to gain maximun confident

Clause 9: Concept

Example

- **Item**: Headlamp system
- **Asset**: Lamp switch off request

Threat Scenario	Attack path	Impact Level	Cybersecurity Goal	Attack Vector	CAL
Spoofing of a signal leads to loss of integrity of the CAN message of “Lamp Request” signal of Power Switch Actuator ECU	Attacker delivers the malicious code through cellular interface compromising the gateway ECU and injects spoofed lamp switch off signals	Severe (safety impact due to loss of integrity)	Lamp switch off request integrity shall be protected against spoofing	Network	CAL4

Clause 9: Concept

Cybersecurity Concept

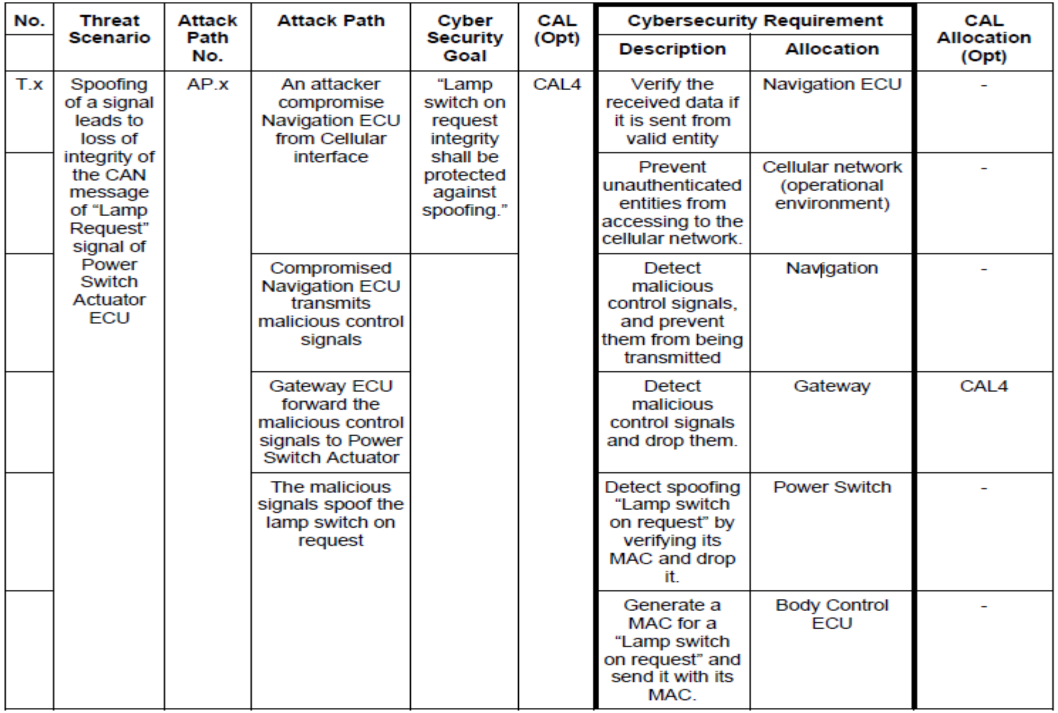
- A cybersecurity concept for an item is a complete set of cybersecurity requirements allotted to components, the operational environment, etc., with associated information on cybersecurity controls to achieve the cybersecurity goals
- Item definition, cybersecurity goals, and claims are the main criteria to accomplish a cybersecurity concept

Key Requirements

1. Technical and operational cybersecurity requirements to be defined for the item and its dependencies (functions, components, etc.)
2. The cybersecurity concept report, which is a final work product to be verified for the fulfillment of the objectives and its requirements
3. The cybersecurity concept report should be in a condition to act as a prerequisite in the next stages of an item or a feature development

Clause 9: Concept

Example: Cybersecurity Concept Report for Headlamp system



No.	Threat Scenario	Attack Path No.	Attack Path	Cyber Security Goal	CAL (Opt)	Cybersecurity Requirement		CAL Allocation (Opt)
						Description	Allocation	
T.x	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU	AP.x	An attacker compromise Navigation ECU from Cellular interface	"Lamp switch on request integrity shall be protected against spoofing."	CAL4	Verify the received data if it is sent from valid entity	Navigation ECU	-
						Prevent unauthenticated entities from accessing to the cellular network.	Cellular network (operational environment)	-
			Compromised Navigation ECU transmits malicious control signals			Detect malicious control signals, and prevent them from being transmitted	Navigation	-
			Gateway ECU forward the malicious control signals to Power Switch Actuator			Detect malicious control signals and drop them.	Gateway	CAL4
			The malicious signals spoof the lamp switch on request			Detect spoofing "Lamp switch on request" by verifying its MAC and drop it.	Power Switch	-
						Generate a MAC for a "Lamp switch on request" and send it with its MAC.	Body Control ECU	-

Figure 4: Example cybersecurity report for Headlamp system as given in ISO 21434 DIS version

Clause 9: Concept

DEKRA DIGITAL

Summary of work products

- [WP-09-01] Item definition
- [WP-09-02] TARA
- [WP-09-03] Cybersecurity goals
- [WP-09-04] Cybersecurity claims
- [WP-09-05] Verification report for cybersecurity goals
- [WP-09-06] Cybersecurity concept
- [WP-09-07] Verification report for the cybersecurity concept

Example (Case study)

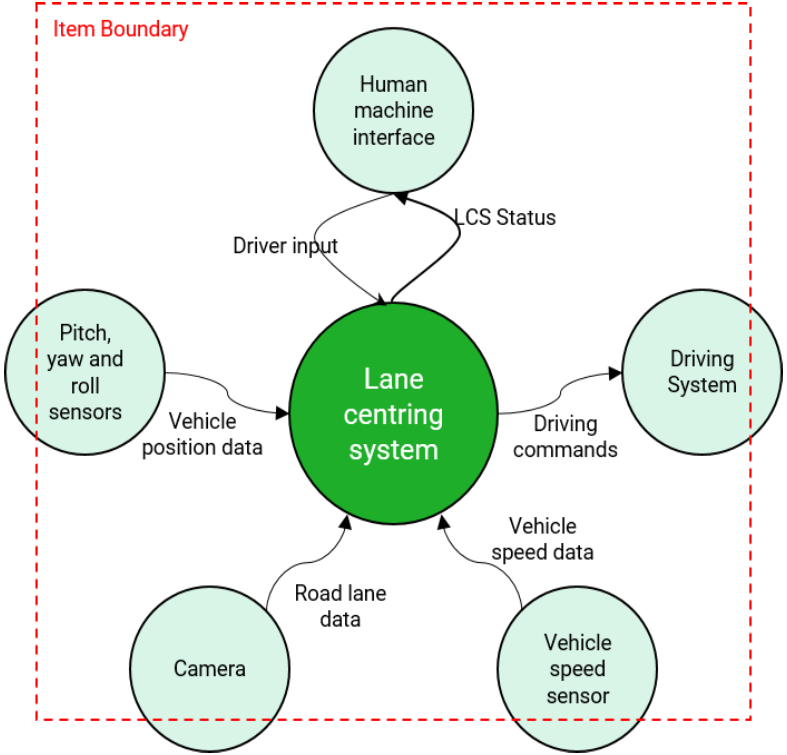
Clause 9: Concept

DEKRA DIGITAL

Use Case Scenario

Automatic lane-centering system:

- Consider the scenario where an automatic lane-centering system is developed. The functions, constraints, and assumptions were mentioned during previous sessions.
- We have identified the assets, and threats and rated the risks.
- Now, we will assign cybersecurity goals and establish the cybersecurity concept.
- Cybersecurity claims will be identified



Clause 9: Concept

Risk Treatment Decision

Threat scenario	Aggregated attack feasibility	Impact severity				Risk				Risk treatment option
		S	F	O	P	S	F	O	P	
The attacker is able to attach a hardware device to the vehicle network. This allows the attacker to read the camera data	Low	Negligible	Negligible	Negligible	Moderate	1	1	1	2	Sharing
The camera input is spoofed by the attacker and the camera sends wrong data	High	Severe	Moderate	Major	Negligible	5	3	4	1	Reduction
The camera is tampered by the attacker and the camera sends wrong data	High	Severe	Moderate	Major	Negligible	5	3	4	1	Reduction
The communication of camera data is severed by the attacker such that the road lane data is not usable	High High	Severe Severe	Moderate Moderate	Major Major	Negligible Negligible	5 5	3 3	4 4	1 1	Reduction
The speed sensor data is tampered which in turn sends incorrect speed data	Medium	Severe	Moderate	Major	Negligible	4	2	3	1	Reduction
The communication of vehicle speed data is severed by the attacker such that the speed data is not usable	High High	Severe Severe	Moderate Moderate	Major Major	Negligible Negligible	5 5	3 3	4 4	1 1	Reduction
The lane centering system is corrupted via malicious codes which sends incorrect driving commands	Low	Severe	Moderate	Major	Negligible	3	2	2	1	Reduction
The driving commands are made useless due to loss of communication.	Low	Severe	Moderate	Major	Negligible	3	2	2	1	Reduction
The pitch and yaw sensors are tampered by an attacker and the sensors send incorrect signals	High	Severe	Moderate	Major	Negligible	5	3	4	1	Reduction
The communication of pitch and yaw sensors are tampered	High	Severe	Moderate	Major	Negligible	5	3	4	1	Reduction
The driver inputs and notifications are tampered using some malicious program	Low	Severe	Moderate	Major	Negligible	3	2	2	1	Reduction
The turn on or off signals is disrupted using malicious software	Low	Negligible	Negligible	Major	Negligible	1	1	2	1	Retention
The lane centering system is corrupted via malicious codes hence the notifications are blocked	Low	Moderate	Moderate	Moderate	Negligible	2	2	2	1	Reduction

Clause 9: Concept

Cybersecurity goals

- Assigned to all threat scenarios with risk treatment option “risk reduction”
- It can refer to an asset, attack path, or damage scenario associated with the threat scenario
- Different cybersecurity requirements are defined to achieve the cybersecurity goals

Example:

Asset: Lamp switch off request

Threat scenario: Spoofing lamp switch off request signals (Spoofing)

Attack path: Attacker delivers the malicious code through the cellular interface, compromising the gateway ECU, and injects spoofed lamp switch off signals

Impact: Severe **Attack feasibility:** Medium **Risk:** 4 **Risk treatment option:** Reduction

Cybersecurity goal:

“Lamp switch off request integrity shall be protected against spoofing.”

Clause 9: Concept

Cybersecurity Goals

Threat scenario: The driving commands are not available due to communication loss

Attack path: The attacker injects a malicious code that corrupts the communication channel. Hence the data is unreadable by the system

Impact: : safety: **severe**, financial: **moderate**, operational: **major**, Privacy: **negligible**

Attack feasibility: Low **Risk:** 3

Risk treatment option: Reduction (safety risk)

Cybersecurity goal:

“The driving commands generated by the lane centering system shall always be available and protected against denial of service”

Clause 9: Concept

Cybersecurity Goals

Threat scenario	Risk				Risk treatment option	Cybersecurity goal
	S	F	O	P		
The attacker is able to attach a hardware device to the vehicle network. This allows the attacker to read the camera data	1	1	1	2	Sharing	n/a
The camera input is spoofed by the attacker and the camera sends wrong data	5	3	4	1	Reduction	The camera data shall be protected against spoofing
The camera is tampered by the attacker and the camera sends wrong data	5	3	4	1	Reduction	The camera data shall be protected against tampering
The communication of camera data is severed by the attacker such that the road lane data is not usable	5 5	3 3	4 4	1 1	Reduction	The camera data shall always be available and protected against denial of service.
The speed sensor data is tampered which in turn sends incorrect speed data	4	2	3	1	Reduction	The speed sensor data shall be protected against tampering
The communication of vehicle speed data is severed by the attacker such that the speed data is not usable	5 5	3 3	4 4	1 1	Reduction	The speed sensor shall always be available and protected against denial of service.
The lane centering system is corrupted via malicious codes which sends incorrect driving commands	3	2	2	1	Reduction	The driving commands generated by the lane centering system shall be protected against tampering
The driving commands are made useless due to loss of communication.	3	2	2	1	Reduction	Thedriving commands generated by the lane centering system shall always be available and protected against denial of service.
The pitch and yaw sensors are tampered by an attacker and the sensors send incorrect signals	5	3	4	1	Reduction	The vehicle position data shall be protected against tampering.
The communication of pitch and yaw sensors are tampered	5	3	4	1	Reduction	The vehicle position data shall always be available and protected against denial of service.
The driver inputs and notifications are tampered using some malicious program	3	2	2	1	Reduction	The driver input and notification signals shall be protected against tampering.
The turn on or off signals is disrupted using malicious software	1	1	2	1	Retention	n/a
The lane centering system is corrupted via malicious codes hence the notifications are blocked	2	2	2	1	Reduction	The driver input and notification signals shall always be available and protected against denial of service.

DEKRA

DEKRA DIGITAL

Thank you for your attention