Cybersecurity engineering

ISO/SAE 21434 Road Vehicles: Cybersecurity Engineering (2021)

ISO: International Standard Organization

SAE: Society of Automotive Engineering

The main objective of the standard is making automotive companies (vehicle manufactures, component supplies, …) aware of the importance of the cybersecurity in the product development process.

Cybersecurity management

- The standard specifies requirements for cybersecurity risk management regarding the c**oncept**, **product development**, **production operation**, **maintenance** and **decommissioning** of electric and electronic (E/E) systems in road vehicles.

- The document provides vocabulary, objectives, requirements and guidelines related to cybersecurity engineering as a foundation for common understanding throughout the supply chain. This enables organizations to:
    — define cybersecurity policies and processes;
    — manage cybersecurity risk; and
    — foster a cybersecurity culture

Cybersecurity management

Cybersecurity requirements

- Organization level

- Project level: requirements of an item in the product lifecycle
  - Concept phase
  - Development phase
  - Production phase

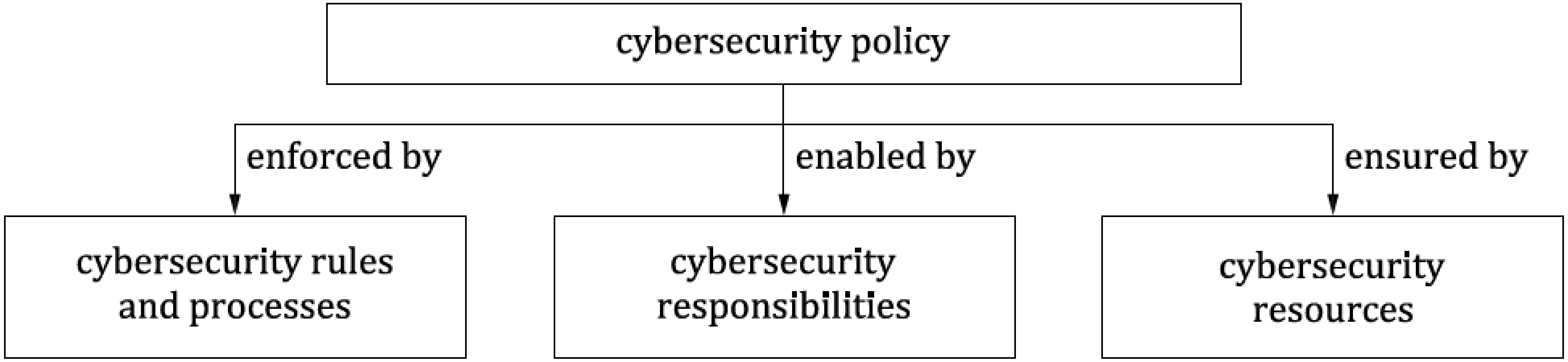
Security
by design

- Continual cybersecurity activities

- Post-production phase

Cybersecurity management

Governance of cybersecurity by an organization



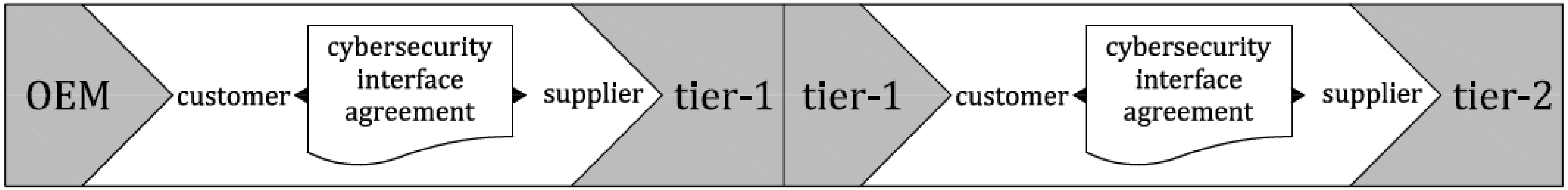
Cybersecurity management

Distributed activities

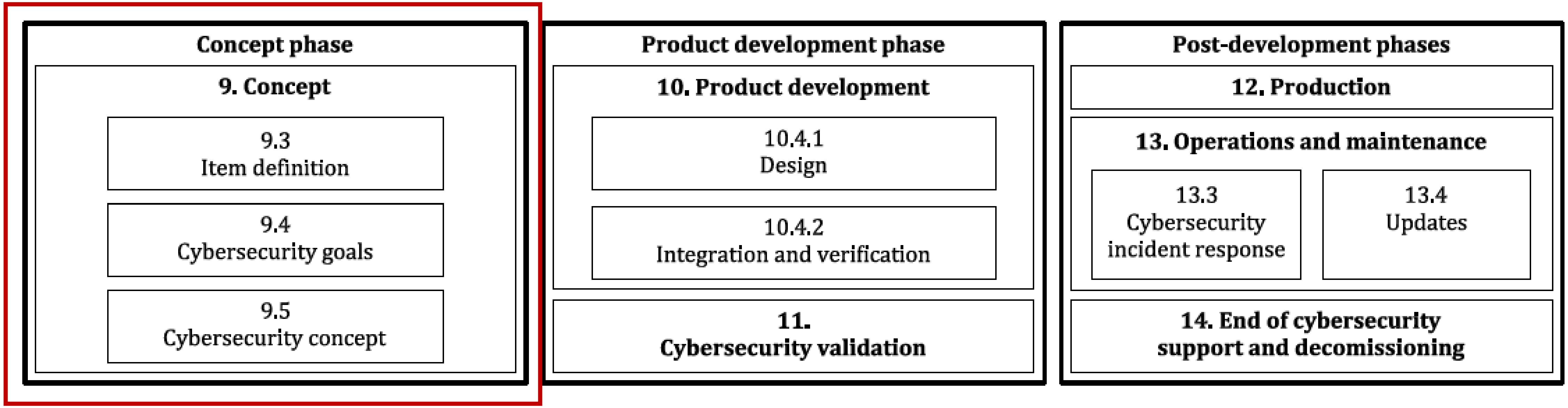
Customer/supplier relationship in the supply chain

Supplier : evidence of the organization capability concerning cybersecurity

original equipment manufacturer (**OEM**) is generally perceived as a company that produces parts and equipment that may be marketed by another manufacturer



ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering



ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

The standard considers the perspective of an **item** and its components and interfaces.

item: - component or set of components that *implements a function at vehicle level* (a system is an item if it implements a function at vehicle level; otherwise it is a component)

- all electronic equipment and software in a vehicle involved in the realization of a specific functionality at vehicle level, e.g., braking

- an item or a component interacts with its operational environment

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

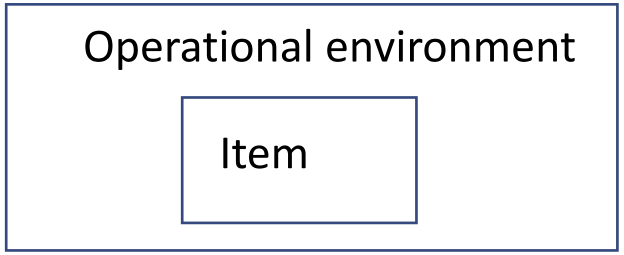
Concept phase

consideration of vehicle level functionality, as implemented in items

The basis of all the activities is the “item definition”

“item definition”: the item and its operational environment

item definition



- *existing information* (in-vehicle E/E system architecture, including in-vehicle network, networks external to the vehicle, etc)
- *item boundary*

  includes the description of the interfaces with the other items internal or external to the vehicle and E/E systems external to the vehicle
- *item functions*

  vehicle functionality realized by the item (behaviour in the lifecycle)
- *preliminary architecture*

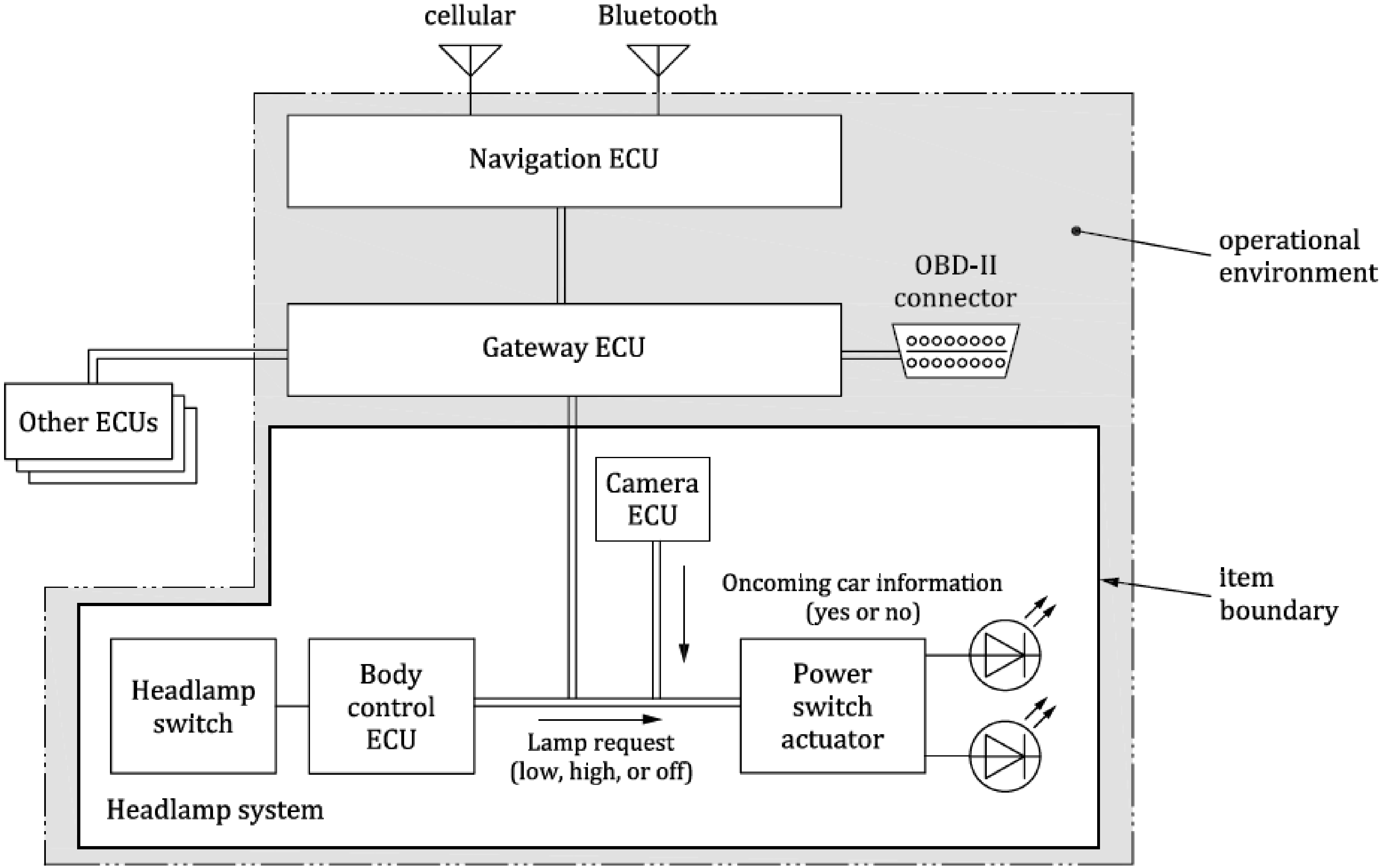
  includes identification of components of the item and their connections, and eternal interfaces

- *information about operational environment of the item revelant to cybersecurity*

Headlamp system

item: headlamp system

function: the headlamp system turns on/off the headlamp in accordance
with the switch by demand of the driver. If the headlamp is in high-beam mode, the headlamp system switches the headlamp automatically to the low-beam mode when an oncoming vehicle is detected. It also returns the headlamp automatically to the high-beam mode if the oncoming vehicle is no longer detected.

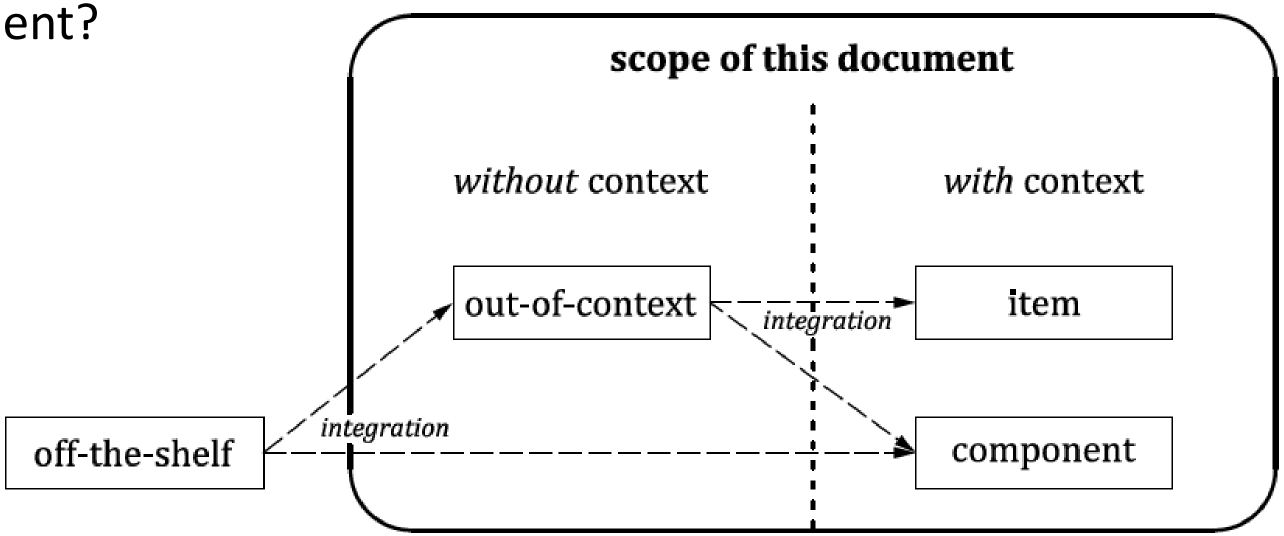


Example description of the operational environment

The item (headlamp system) is connected with the gateway ECU, and the gateway ECU is connected with 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).

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

Is the item (component) security relevant?
Is the item (component) a new development or a reuse?
Reuse in the same environment?
Reuse with modification?
Off-the-shelf component?



Specify the actions required for cybersecurity during the concept and development phase
-> Cybersecurity plan (updated when activities change or during development)

Concept phase

Identification of cybersecurity goals

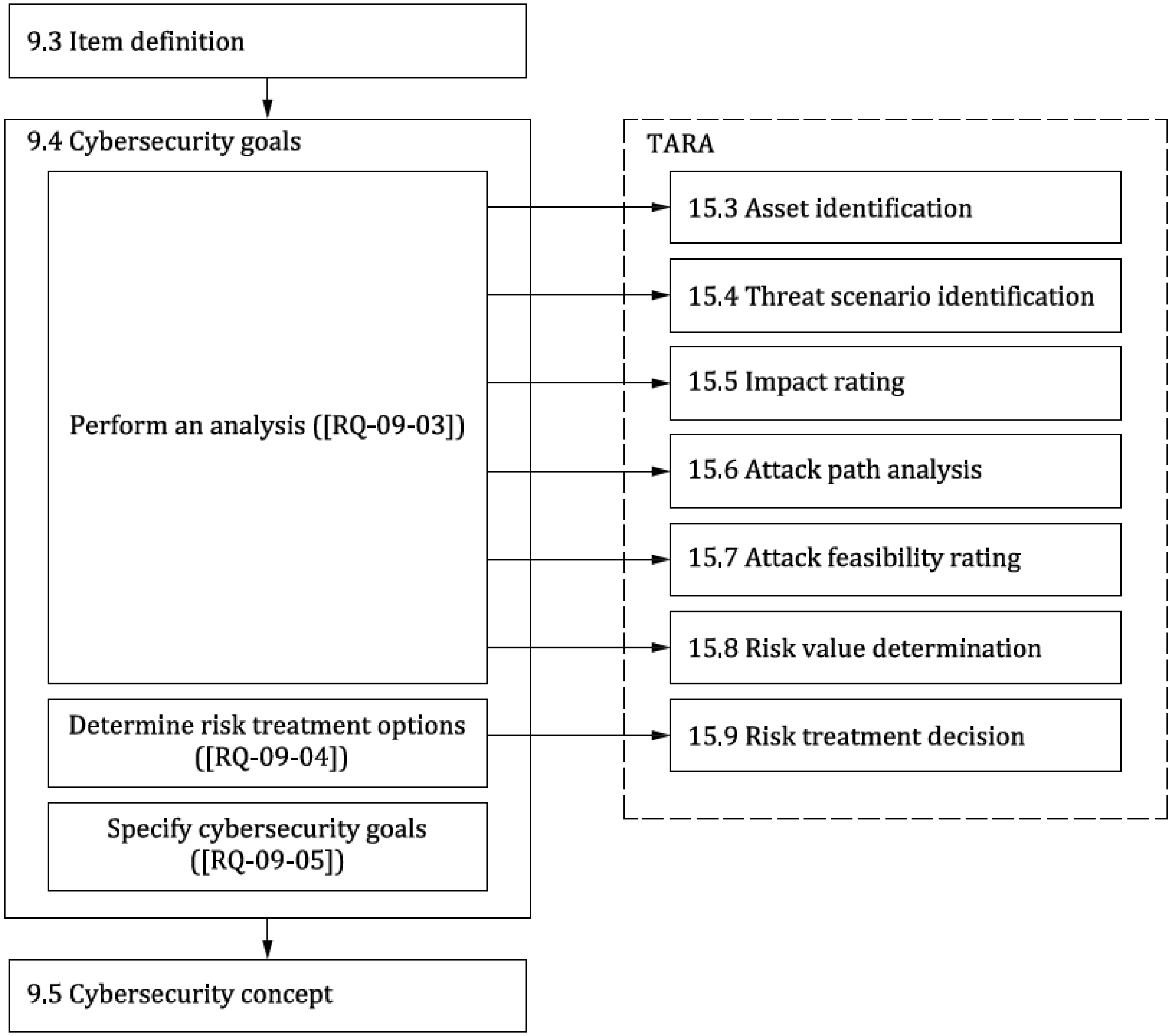
Performed from the viewpoint of affected road users

Analysis of the item
Threats identification
Vulnerability of the product
Manage the impact of threats
Possible harm associated to the threat

Activities: TARA
(Threat Analysis and Risk Assessment)

Activities that can be executed many times
in different phase of the development lifecycle

CAL: Cybersecurity Assurance Level



ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

Asset: object that has value, or contributes to value
e.g., sensor, actuators, components of an ECU, function
an asset has one or more cybersecurity properties whose compromise can lead to damage scenarios

Asset properties of cybersecurity: confidentiality, integrity, availability

Identification of the consequences (damage scenarios) of cybersecurity properties violation

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

Threat analysis and risk assessment methods - TARA

- **Asset identification**
  - identify assets, their security properties and their damage scenarios
- **Threat scenarios**
  - identify threat scenarios
- **Impact rating**
  - determine the impact rating of damage scenarios
- **Attack path analysis**
  - identify the attack path that realizes threat scenarios
- **Attack feasibility rating**
  - determine the ease with which attack paths can be exploited
- **Risk value determination**
  - determine the risk values of threat scenarios
- **Risk treatment decision**
  - select appropriate risk treatment options for threat scenarios

Viewpoint of affected road users

Modules tha can be invoked at any point in the lifecycle of an item or component

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

Asset identification

Input: item definition

Output: *identification of damage scenarios*
identification of assets with cybersecurity properties whose compromise leads to damage scenarios

----

Asset= customer personal information stored in infotainment,
Security property: confidentiality
Damage: disclosure of information

Asset: data communication of the braking function
Security property: integrity
Damage: collision with following vehicle caused by unintended full braking in case of high speed

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

Headlamp system: example list of assets and damage scenarios

Asset	Cybersecurity property			Damage scenario
	C	I	A	
Data communication (lamp request)	—	X	X	Vehicle cannot be driven at night, because (the driver perceives) the headlamp function was inhibited while parked.
	—	X	—	Front collision with a narrow stationary object (e.g. a tree) caused by unintended turning-off of headlamp during night driving at medium speed.
Data communication (oncoming car information)	—	X	—	Drivers of oncoming vehicles are blinded, it is caused by not being able to change to low beam during night driving.
	—	—	X	Malfunctioning automatic high beam caused by headlamp always remaining at low beam during night driving.
Firmware of body control ECU	X	X	—	...

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

Threat scenario identification

Input: item definition ; damage scenarios; assets with cybersecurity properties

Output: *identification of threat scenarios*

target asset, compromised security property, cause of compromise

Threat modelling approaches: EVITA, STRIDE, PASTA, …..

Spoofing of CAN messages for braking ECU leads to loss of integrity of the message and of integrity of the braking function

One damage scenario can correspond to many threat scenarios

One threat scenario can correspond to many damage scenarios

Headlamp system

Damage scenario	Threat scenario
Front collision with a narrow stationary object (e.g. a tree) caused by unintended turning-off of headlamp during night driving at medium speed	Spoofing of a signal leads to loss of integrity of the data communication of the "Lamp Request" signal to the power switch actuator ECU, potentially causing the headlamp to turn off unintentionally.
	Tampering with a signal sent by body control ECU leads to loss of integrity of the data communication of the "Lamp Request" signal to the power switch actuator ECU, potentially causing the headlamp to turn off unintentionally.
Malfunctioning automatic high beam caused by headlamp always remaining at low beam during night driving	Asset: oncoming car information Cybersecurity property: availability Associated cause: denial of service of oncoming car information

Impact rating

Input: damage scenarios; item definition; assets with cybersecurity properties

Output: *damage scenario assessed against adverse consequences for road users in the following impact categories (SFOP)*

- *safety*
- *financial*
- *operational*
- *privacy*

Impact rating:

- *severe*
- *major*
- *moderate*
- *negligible*

Damage scenario	Impact category	Impact rating
Vehicle cannot be driven at night, because (the driver perceives) the headlamp function was inhibited while parked.	O	Major
Front collision with a narrow stationary object (e.g. a tree) caused by unintended turning-off of headlamp during night driving at medium speed.	S	Severe (S3)
Malfunctioning automatic high beam caused by headlamp always remaining at low beam during night driving.	O	Moderate

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

Attack path analysis

Input: item definition; threat scenarios, weaknesses found during development; architectural design, previous attack paths, vulnerability analysis

Output: *threats scenarios are analysed to identify attack paths*

top-down approaches: deduce attack paths by analysing the ways in which a threat scenario could be realized: attack trees; attack graphs

bottom-up approaches: build attack path from identified vulnerability

Attack paths are associated with the threat scenarios that can be realized

Threat scenario: spoofing CAN for braking ECU -> loss of integrity of /braking function

Example of Attack path:
telematics ECU compromised by cellular interface ;
gateway ECU compromised via CAN communications from telematics ECU ;
gateway ECU forwards malicious braking request signals

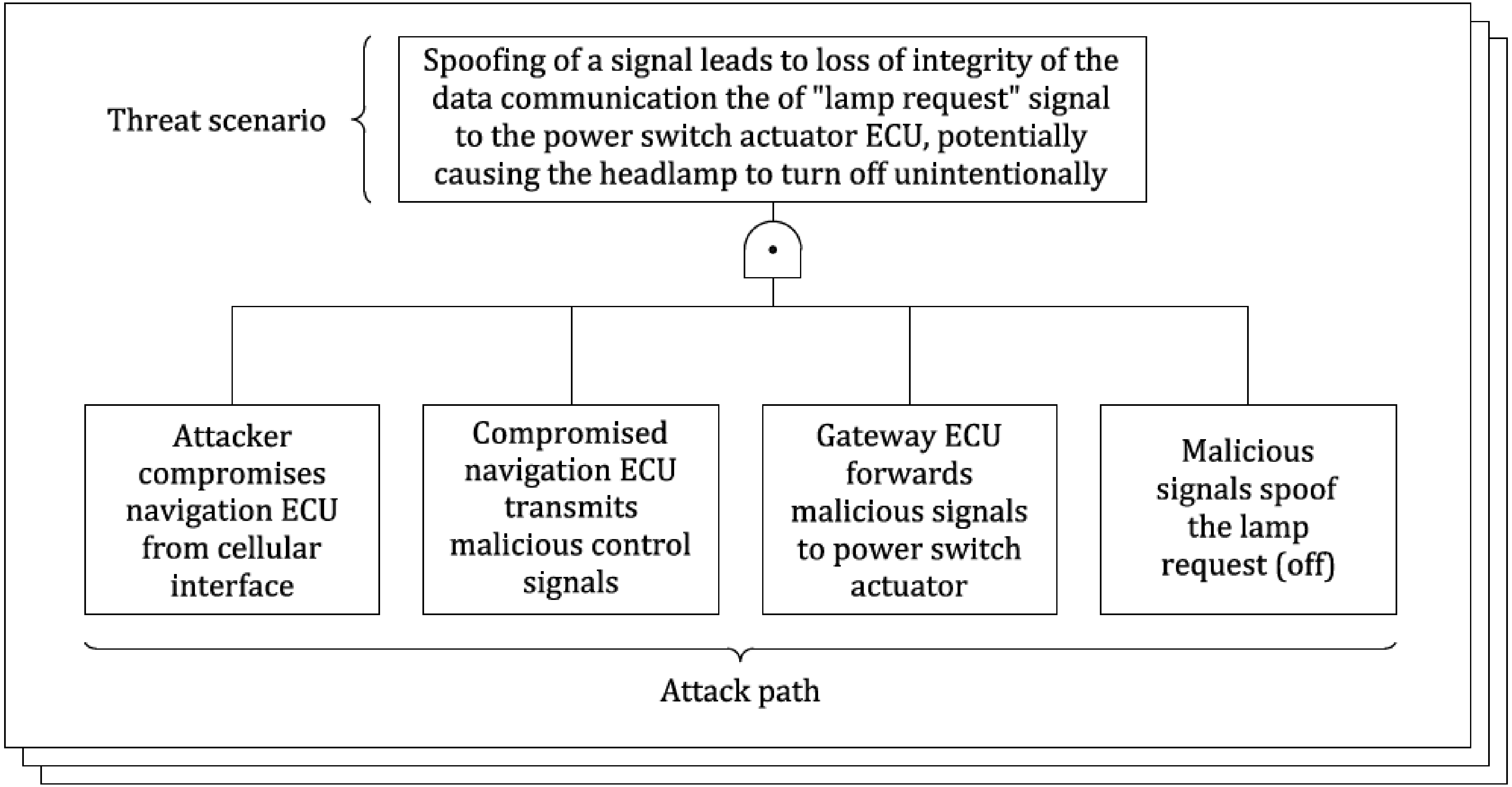
Headlamp system

An example

Threat scenario	Attack path
Spoofing of a signal leads to loss of integrity of the data communication of the “Lamp Request” signal to the power switch actuator ECU, potentially causing the headlamp to turn off unintentionally	i. Attacker compromises navigation ECU from cellular interface. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (OFF).
	i. Attacker compromises navigation ECU from Bluetooth interface. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (OFF).
	i. Attacker gets local (see Table G.9) access to OBD connector. ii. Attacker sends malicious control signals from OBD connector. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (OFF).

Headlamp system

Example of an attack path derived by attack tree analysis



ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

Is the attack feasible?

Attack feasibility rating

Input: attack paths; architectural design; vulnerability analysis

Output: for each attack path, attack feasibility rating determined

Attack feasibility rating	Description
High	The attack path can be accomplished utilizing low effort.
Medium	The attack path can be accomplished utilizing medium effort.
Low	The attack path can be accomplished utilizing high effort.
Very low	The attack path can be accomplished utilizing very high effort.

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

Attack feasibility rating

possible methods

- <u>Attack potential based approach</u> (effort to attack an item/component)
  - elapsed time
  - specialist expertise
  - knowledge of the item or component
  - window of opportunity
  - equipment
- <u>CVSS-based approach</u> (Common Vulnerability Scoring System)

  feasibility rating should be determined based on exploitability metrics of the base metric group
  - attack vector (physical access/local area network access/ ….)
  - attack complexity
  - privileges required
  - user interaction

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

Attack feasibility rating

possible approaches

- <u>Attack-vector based approach (concept phase, few information on the item)</u>
  - evaluation of the predominant attack vector (e.g., CVSS) of the attack path

Headlamp system

Examples of attack feasibility rating with the attack vector-based approach

Attack path	Attack feasibility rating
i. Attacker compromises navigation ECU **from cellular interface.** ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (ON).	High
i. Attacker compromises navigation ECU **from Bluetooth interface.** ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (ON).	Medium
i. Attacker sends malicious control signals **from OBD2 connector.** ii. Gateway ECU forwards the malicious signals to power switch actuator. iii. Malicious signals spoof the lamp request (ON).	Low

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

Risk value determination

Input: threats scenarios, impact ratings of the damage scenarios, attack feasibility rating

Output: for each threat scenario, the risk determined from the impact of the damage scenarios and the attack feasibility of the associated attack paths

Threat scenario corresponds to more than one attack path, the attack feasibility ratings can be aggregated (e.g., maximum of attack feasibility ratings of the corresponding attack paths)

Risk value of the threat scenario = value between (and including) 1 and 5, where 1 represents the minimum risk

Methods: risk matrices or risk formulas (impact rating * attack feasibility rating)

Headlamp system

Risk matrix example

		Attack feasibility rating			
		Very Low	Low	Medium	High
Impact rating	Severe	**2**	**3**	**4**	**5**
	Major	**1**	**2**	**3**	**4**
	Moderate	**1**	**2**	**2**	**3**
	Negligible	**1**	**1**	**1**	**1**

Headlamp system examples of determined risk values

Threat scenario	Aggregated attack feasibility rating	Impact rating	Risk value
Spoofing of a signal leads to loss of integrity of the data communication of "Lamp Request" signal for power switch actuator ECU	**High**	**Severe**	**S: 5**
Denial of service of oncoming car information	Low	Moderate	O: 2

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

Risk treatment decision

Input: item definition, threats scenarios, risk values, cybersecurity specifications, previous treatment decisions of the item or similar items, impact rating with associated impact categories, attack paths, attack feasibility ratings,

Output: for each threat scenario, considering its risk value, one or more of the following risk treatment options is determined:

- avoiding the risk (removing risk sources, not start or continue with the activity that gives rise to the risk)
- reducing the risk
- sharing the risk (through contracts or transferring risk by buying insurance)
- retaining the risk

Rationales for sharing/retaining the risk recorded as security claims subject to cybersecurity monitoring and vulnerability management

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

Risk treatment decision

Input: item definition, threats scenarios, risk values, cybersecurity specifications, previous treatment decisions of the item or similar items, impact rating with associated impact categories, attack paths, attack feasibility ratings,

Output: for each threat scenario, considering its risk value, one or more of the following risk treatment options is determined:

- avoiding the risk (removing risk sources, not start or continue with the activity that gives rise to the risk)
- reducing the risk
- sharing the risk (through contracts or transferring risk by buying insurance)
- retaining the risk

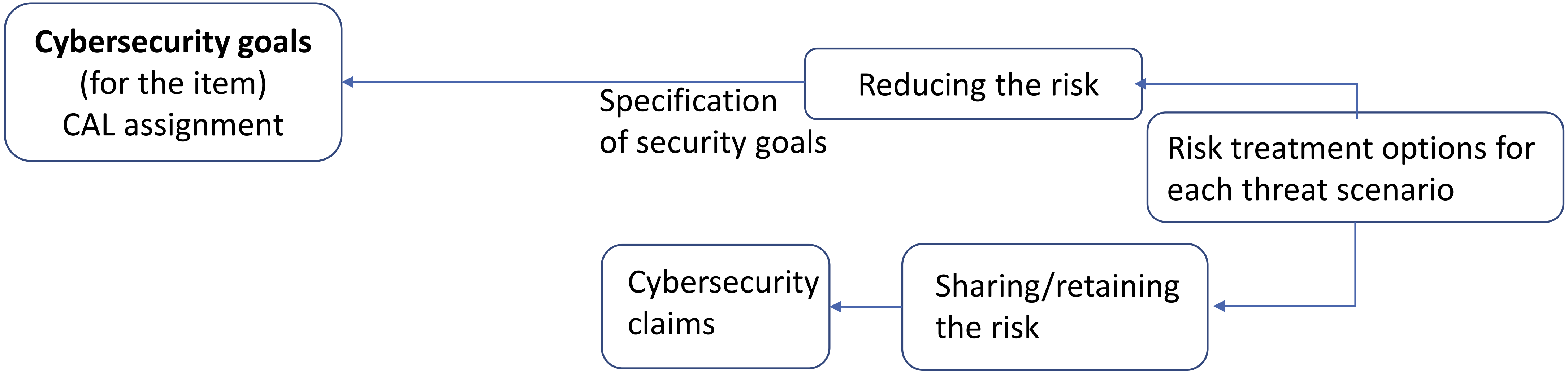
Rationales for sharing/retaining the risk recorded as security claims subject to cybersecurity monitoring and vulnerability management

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

Identification of the Cybersecurity goals

-> Concept level cybersecurity requirements associtated with one or more threat scenario
how to protect the item to avoid the threat scenario

Example: Spoofing of a signal - headlamp system
Lamp switch on request integrity shall be protected against spoofing



Cybersecurity claim: justification of retaining the risk
Example: risk transferred to insurance

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

CAL, level of cybersecurity requested, not related to risk value, determined at the start of the develpment

Expected rigour in cybersecurity assurance measures

<table>
<tr><th>CAL</th><th>Description</th><th>a) Methods to provide confidence that cybersecurity activities are performed with appropriate rigour</th><th>b) Methods to provide confidence that unmanaged vulnerabilities do not remain</th><th>c) Independence scheme to provide confidence that the cybersecurity activities performed are appropriate</th></tr>
<tr><td>CAL1</td><td>Low to moderate cybersecurity assurance is required</td><td rowspan="2">Requirement based testing</td><td rowspan="2">Activities such as analysis and/or testing to search for vulnerabilities based on known information</td><td>Not needed</td></tr>
<tr><td>CAL2</td><td>Moderate cybersecurity assurance is required</td><td>Cybersecurity assessments are carried out by a different person than the originator</td></tr>
<tr><td>CAL3</td><td>Moderate to high cybersecurity assurance is required</td><td>All interactions between components are tested</td><td rowspan="2">Activities such as analysis and/or testing to search for vulnerabilities by exploratory methods</td><td>Cybersecurity assessments are carried out by a person in a different team than the originator</td></tr>
<tr><td>CAL4</td><td>High cybersecurity assurance is required</td><td>All combinations of interactions between components are tested</td><td>Cybersecurity assessments are carried out by a person who is independent regarding management, resources and release authority from the originating department</td></tr>
</table>

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

TARA results with respect to item definition

- Correctness
- Completeness

Risk treatment decision with respect to TARA results

- Correctness
- Completeness
- Consistency

Cybersecurity goals and claims with respect to item definition and risk treatment decision

- Correctness
- Completeness
- Consistency

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

Cybersecurity goals
(for the item)
CAL assignment

Cybersecurity claims

Cybersecurity concept

Cybersecurity concept
Cybersecurity requirements for the item and for the operating environment , and the measures that must be implemented to modify the risk

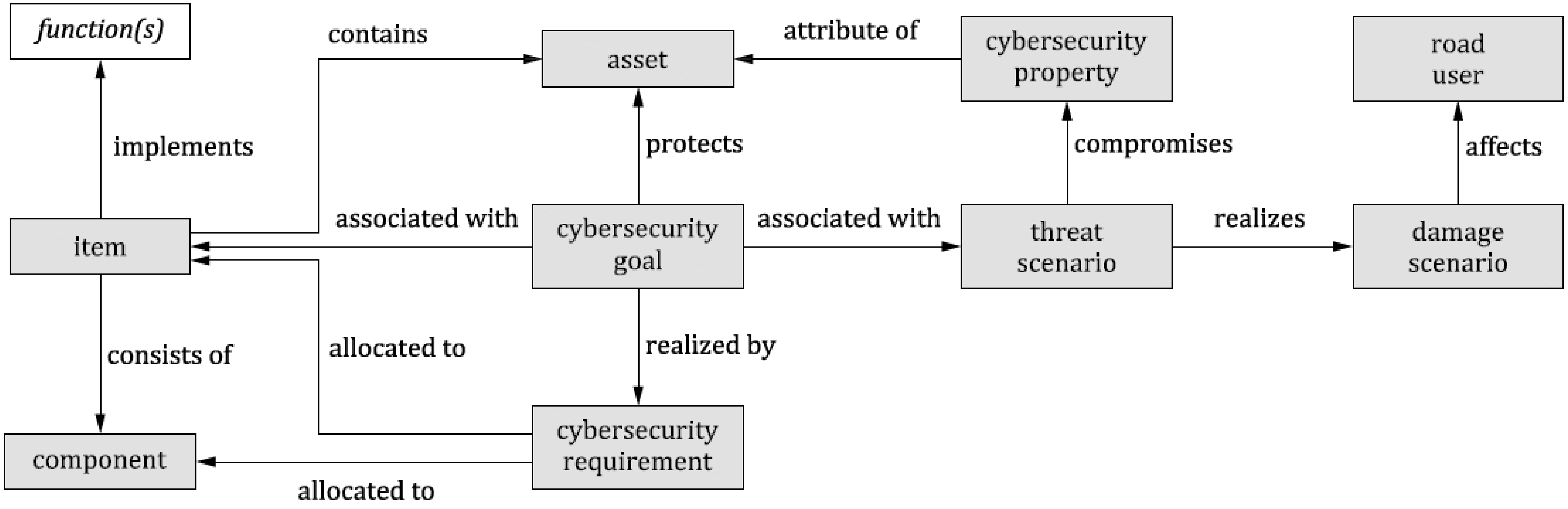
Allocation of requirements on the architecture of the item
Identificaton of who is the responsable to protect the property of the asset
Describe the technical and operational cybersecurity controls and their interactions to achieve the cybersecurity goals

Example: Spoofing of signal – headlamp system
Cybersecurity goal: Lamp switch on request integrity shall be protected by spoofing
Cybersecurity requirement: verify if the received value is sent by a valid entity
Allocation: navigation ECU

ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering

Concept phase

BS ISO/SAE 21434:2021
ISO/SAE 21434:2021(E)



Relationship between item, function, component and related terms