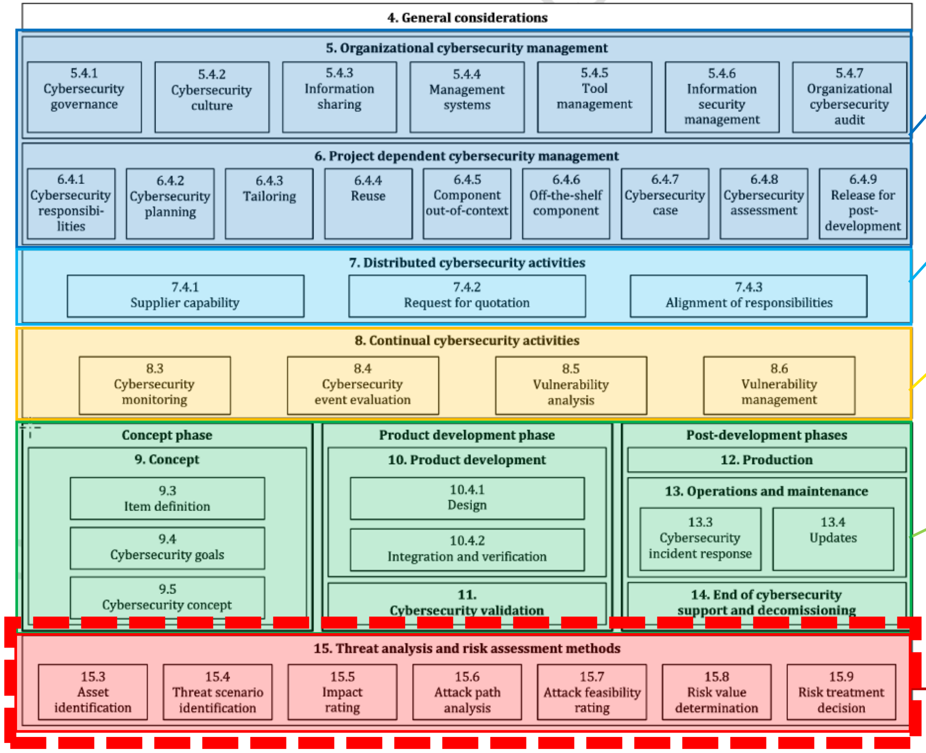
DEKRA

DEKRA DIGITAL

ISO/SAE 21434 – Expert Training

15.
TARA

Structure of ISO 21434



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..

Continuous 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 15: TARA

DEKRA DIGITAL

Introduction

TARA Threat Analysis and Risk Assessment

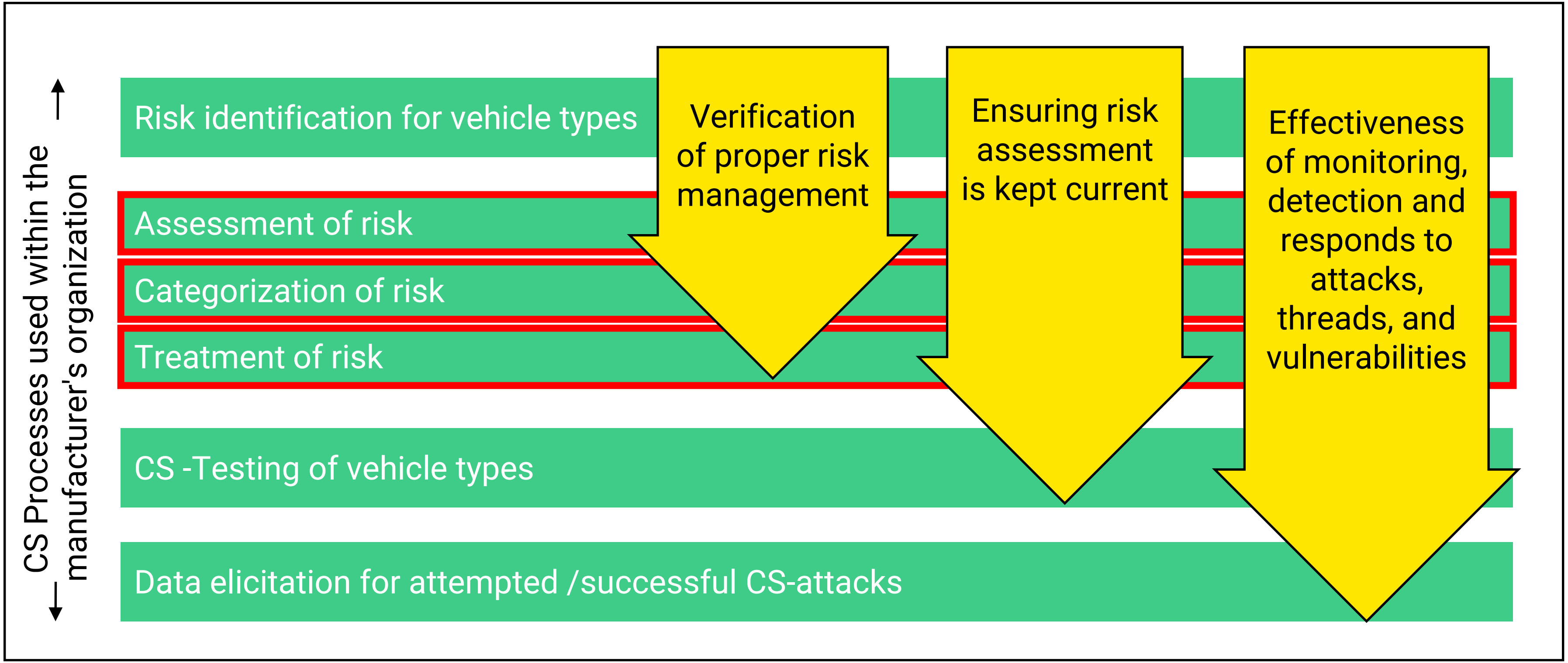
What is Threat Analysis and Risk Assessment?

A process used to analyze threats, examine vulnerabilities and the potential impacts due to threats, and evaluate the resulting security threat

- Key activity defined by ISO/SAE 21434
- Recommended to use through the product lifecycle
- Ensures secure-by-design from the start

Clause 15: TARA

Why is it important to perform TARA as in ISO 21434?



Clause 15: TARA

DEKRA DIGITAL

Objectives

- Identify assets, associated CS properties and damages scenarios
- Identify threat scenarios
- Determine impact rating of damages scenarios
- Identify attack paths for detected threat scenarios
- Determine the ease with which attacks can be performed
- Determine the risk values of threat scenarios
- Select appropriate risk treatment

Clause 15: TARA

Definition and considerations

- Provides risk evaluation, assessment, and treatment of identified risk
- Assess the impact caused by threat scenarios to the road users.
- Road user is considered as the primary stakeholder
- Performed during the entire lifecycle of an item or component
- Work products generated in this clause should be documented
- The organization should define its own rating scales (e.g., scales for impact rating, attack feasibility rating, etc.). In addition, a reason for using these scales should be provided

Clause 15: TARA

DEKRA DIGITAL

9.3 Item Definition

9.4 CS Goals

Perform an analysis
RQ-09-03

Determine risk treatment options
RQ-09-04

Specify CS goals
RQ-09-05

...

9.5 CS Concept

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

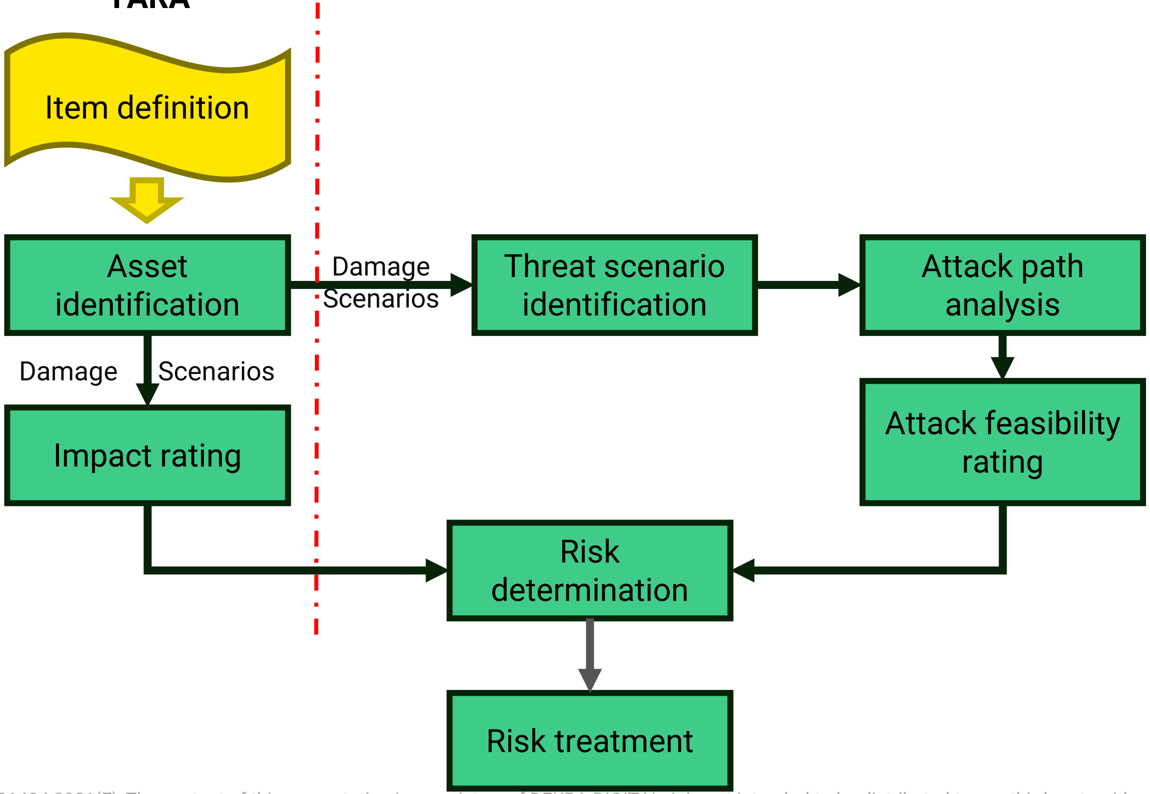
TARA Methods

Item definition

Clause 15: TARA

Performed during the first TARA

Updated during development lifecycle



Clause 15: TARA

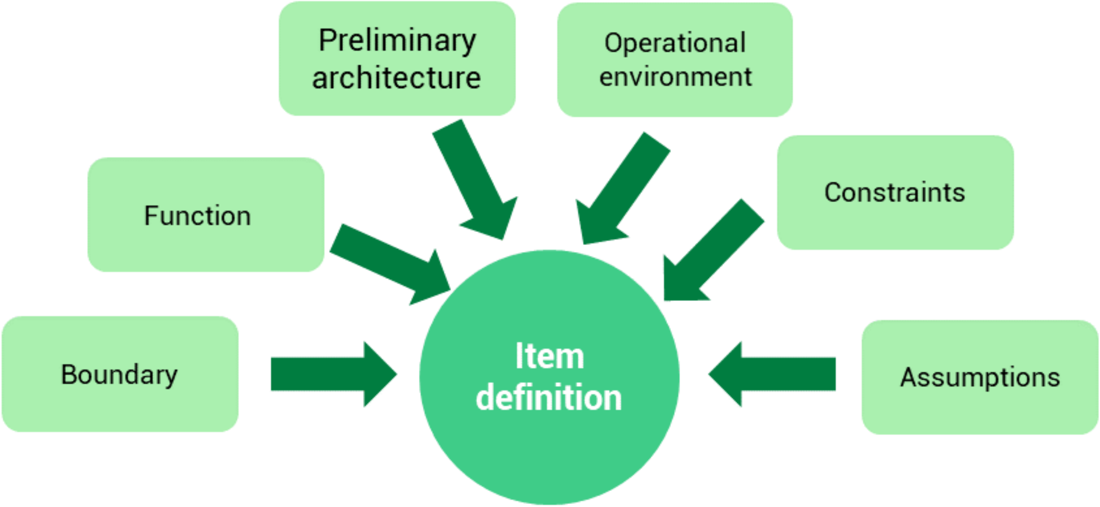
DEKRA DIGITAL

Item definition

- **What is an item?**

"Component or set of components that implements a function at the vehicle level" – ISO 21434

- The definition of item modified from ISO 26262:2018
- The scope of item definition and item boundary can differ from the functional safety process according to ISO 26262

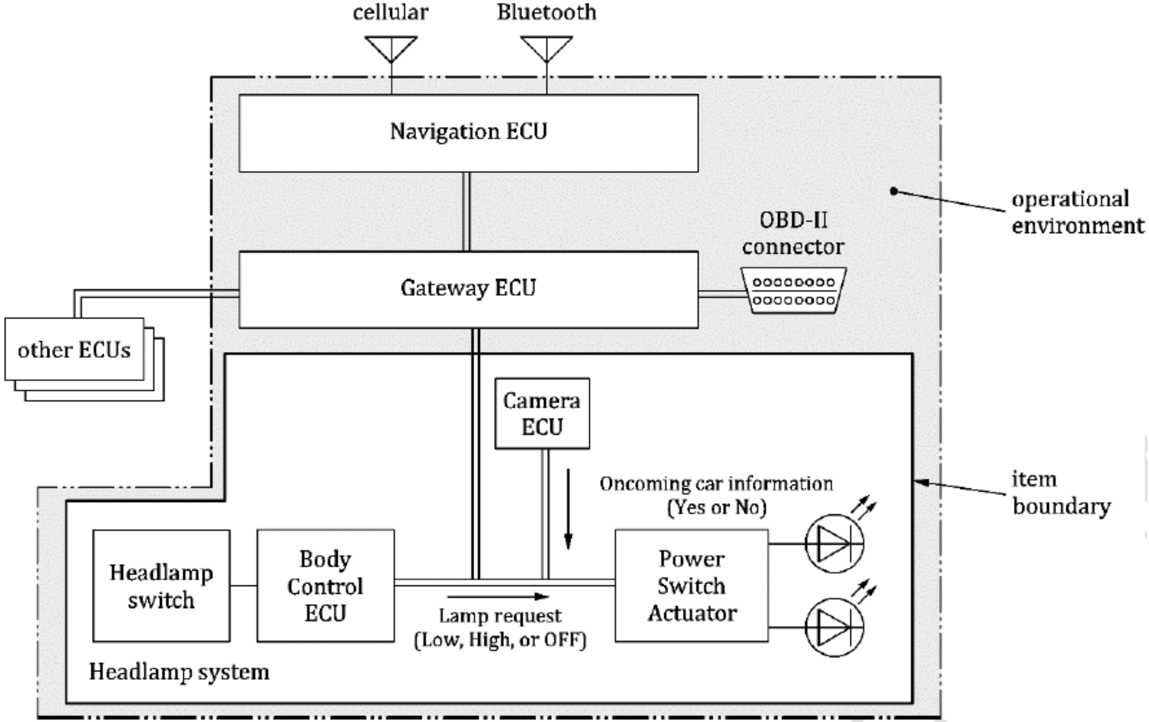


Clause 15: TARA

Item definition: Example

Considering the example of a headlamp system development included in the ISO 21434:

- Item **boundary**
- Item **functions**: functional overview of the item
- Preliminary **architecture**
- **Operational environment** of the item
    - Connections, interfaces
    - Assumptions



Example (Case study)

Clause 15: TARA

Use Case Scenario

To design a simple lane centering system that is capable of maintaining the vehicle in the driving lane.

The lane-centering system is also called auto steer is designed to keep the vehicle centered in a lane. It comes with a steering assist that allows the vehicle to take gentle steering or braking actions to maintain the vehicle in a lane. Along with Adaptive Cruise Control (ACC), lane-centering system can make a car semi-autonomous.

The lane centering system is a fully proactive system. Most of the lane-centering systems are not meant for low-speed driving. It operates only at a certain speed level. It can also maintain the lane while taking curves as long as the curve is too steep. Usually, a camera mounted behind the rear-view mirror is used to determine the lane markings. Different warning methods such as audible warnings, vibrating steering, visual indicators etc. are used to warn the driver. The driver can overcome the automatic steering by turning the wheel harder.

Clause 15: TARA

Description of the system

- The lane-centering system should be operable in various environments (straight roads, curves, highway exits etc.)
- The LCS works only on marked lanes
- The system can provide driving commands such as steering, braking, and acceleration to maintain the lane
- The system is operable only at a certain speed range
- The driver receives notifications about the status of the system
- The driver can turn on/off the system
- The road lane data is obtained by a camera

Clause 15: TARA

- Speed sensors are used to identify the vehicle speed
- The lateral position of the vehicle is determined by vehicle pitch, yaw and roll

The output of the LCS is,

$$\boldsymbol{f}_{\boldsymbol{LCS}} = (\boldsymbol{f}_{\boldsymbol{c}}+\boldsymbol{f}_{\boldsymbol{p}} + \boldsymbol{f}_{\boldsymbol{s}})$$

While,

f_{LCS} is the drive commands from the lane centering system

f_c is the road lane data from the camera

f_p is the vehicle lateral position

f_s is the vehicle speed data

Clause 15: TARA

Assumptions

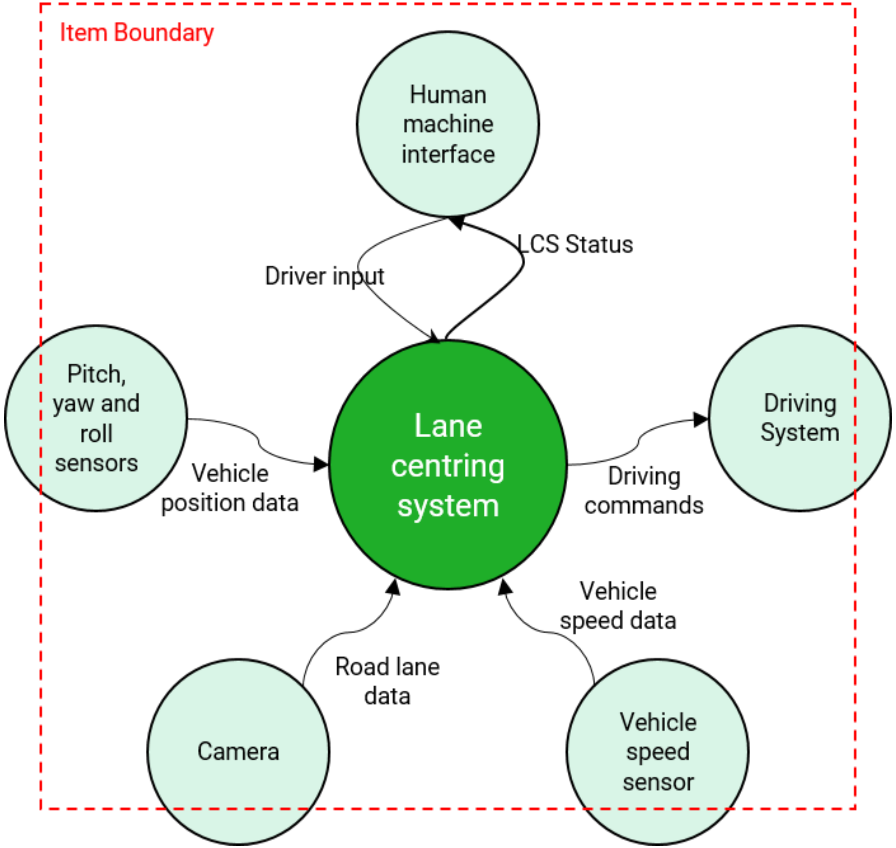
The following are some of the assumptions regarding the item

- A camera-based system is used to identify road lanes
- Whenever the lane centering system is not available, the driver is notified, and the driver takes over
- The lane centering system can be reached via physical diagnostic ports (Such as OBDII)
- The system is isolated from any wireless communication channels (e.g., Bluetooth, Internet)

Clause 15: TARA

DEKRA DIGITAL

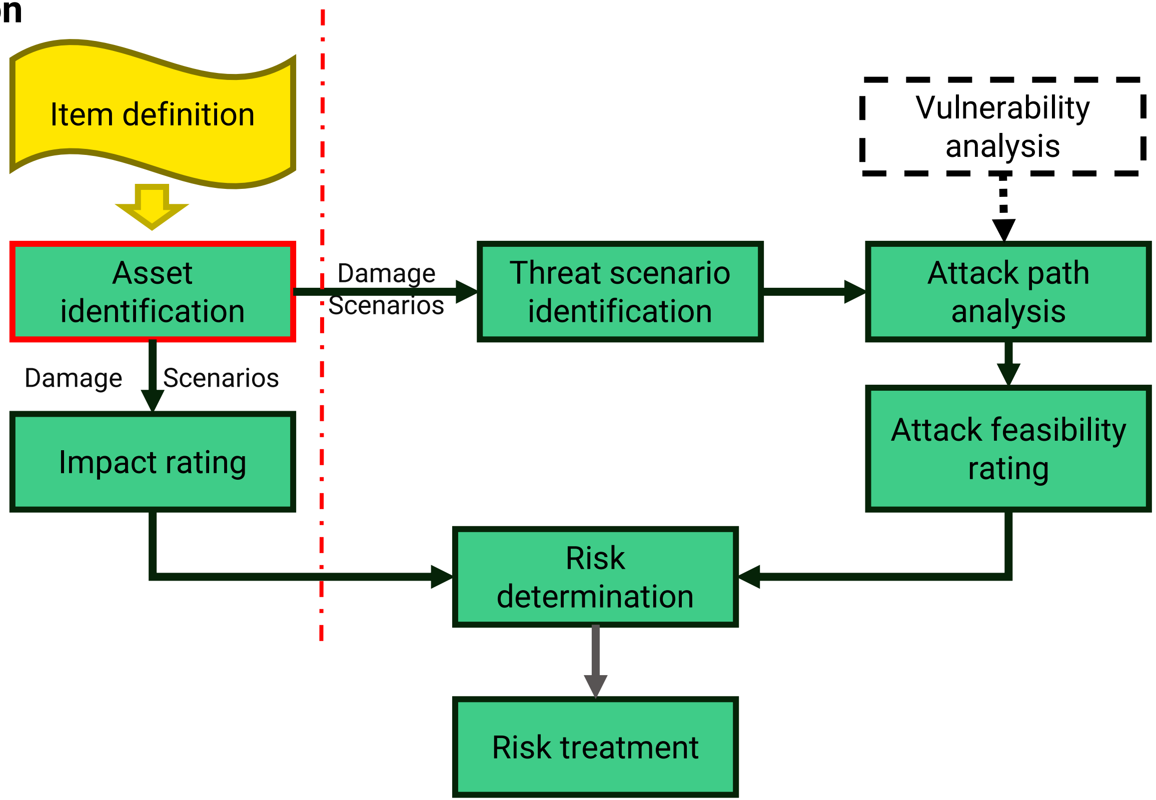
Generic design



Asset identification

Clause 15: TARA

Asset identification

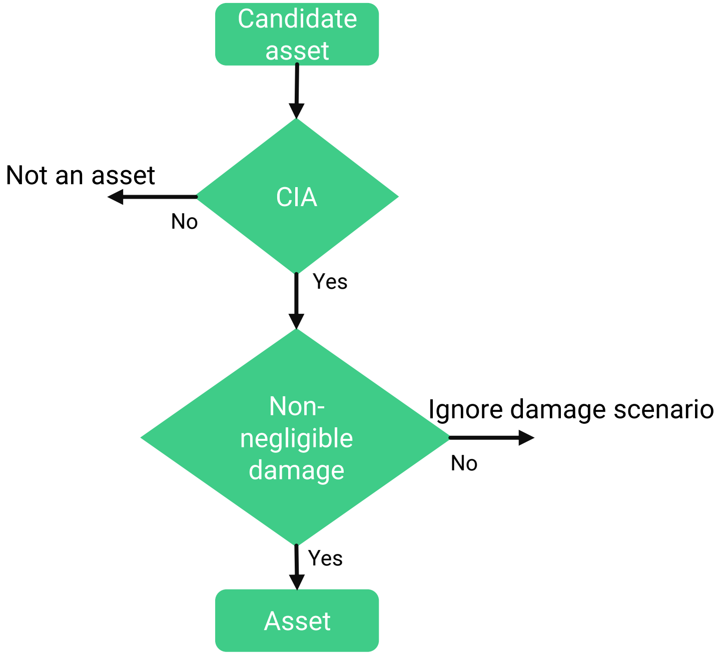


Clause 15: TARA

Asset identification: Key Requirements

"An asset is an object that has value, or contributes to value"- ISO21434

- An asset has one or more CS properties whose compromise can lead to one or more damage scenarios
- **CS properties**: Confidentiality, Integrity and Availability (CIA)
- Identify **damage scenarios** for the assets that are considered, and these should include:
  - Relation functionality – adverse consequences
  - Description of harm to road user
  - Relevant assets
- If the damage to the road user is negligible, then the damage scenario is ignored



Clause 15: TARA

Asset identification: Definitions

- CIA triad, well-know model for development of security policies. The fundamental principles of information security are:

  - **Confidentiality**: ensures the asset´s sensitive information is protected against unauthorized access and disclosure.

  - **Integrity**: protects data, assets or resources against unauthorized modifications

  - **Availability**: ensures that the data, asset, functionality is fully available to the authorized users at a given point

Clause 15: TARA

DEKRA DIGITAL

Asset identification: Example I

Consider the headlamp system given as example in the ISO 21434 and the CAN message **Lamp request** as a candidate asset

Asset	CS Properties			Damage scenario
	Confidentiality	Integrity	Availability	
Lamp request		✗	✗	Headlamp function was inhibited, so the vehicle cannot be driven at night
		✗		Collision caused by unintended turning-off headlamp during night

The damages caused by the loss of CS properties are not negligible. Therefore, the **lamp request is an asset**

Clause 15: TARA

Asset identification: Example I

Now consider the **oncoming car information** as a candidate asset

Asset	CS Properties			Damage scenario
	Confidentiality	Integrity	Availability	
Oncoming car information		✗		Drivers are blinded due to not change to low beam mode
			✗	Malfunctioning automatic high beam

The damages caused by the loss of CS properties are not negligible. Therefore, the **oncoming car information is an asset**

Clause 15: TARA

Asset identification: Example II

Consider the Bluetooth connection between your mobile phone and the infotainment system. The infotainment system has access to your music, but also personal data such as contacts, messages, ...

Asset	CS Properties			Damage scenario
	Confidentiality	Integrity	Availability	
Personal data	✗			Share or unauthorized access to personal information without driver´s consent
		✗		False contact data transmitted to the infotainment system

The damages caused by the loss of CS properties are not negligible. Therefore, the **Bluetooth personal data is considered as an asset**

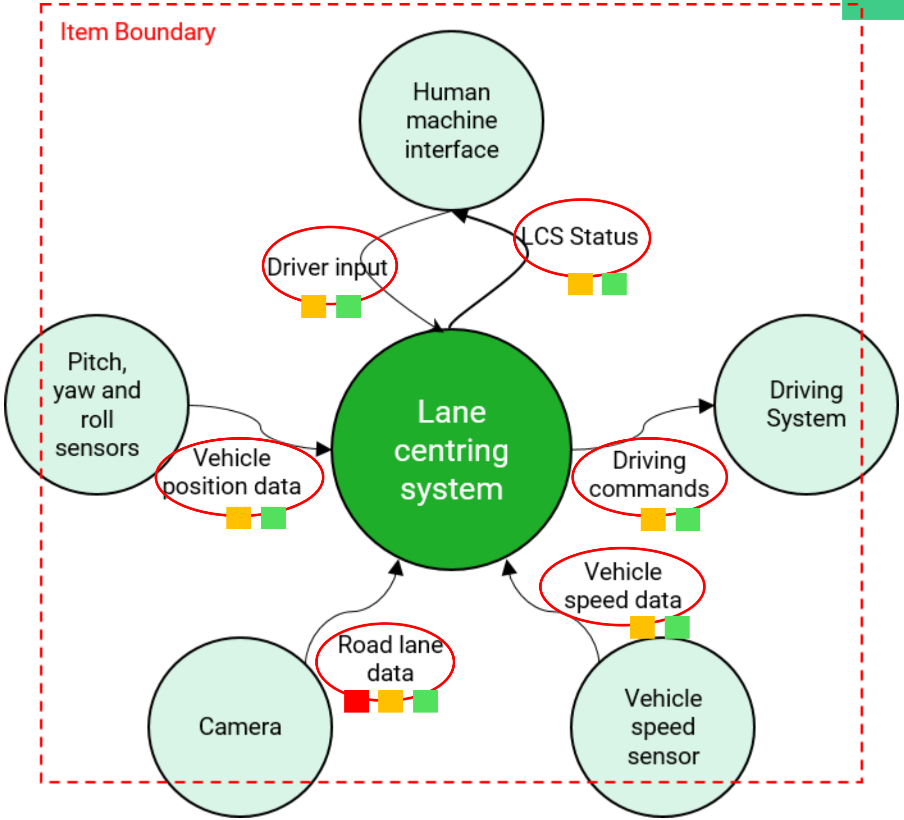
Example (Case study)

Clause 15: TARA

Asset Identification

Identify the cybersecurity relevant assets

- Asset
- Confidentiality
- Integrity
- Availability



Clause 15: TARA

Assets and damage scenarios

Asset	Security property	Damage scenario
Road lane data	Confidentiality	The confidentiality of camera data is compromised and the private details such as the location or private property of the vehicle user is revealed
	Integrity	The system sends incorrect driving commands due to loss of integrity of camera data
	Availability	The lane centering system not available due to loss of camera data
Vehicle speed data	Integrity	The integrity of vehicle speed data is compromised, and the system doesn't work as indented because of incorrect driving commands
	Availability	The loss of speed data leads to loss of the functionality
Vehicle position data	Integrity	The system doesn't work as intended as incorrect drive commands are generated due to loss of integrity of vehicle position data
	Availability	The lane centering system is not available due to loss of vehicle position data

Clause 15: TARA

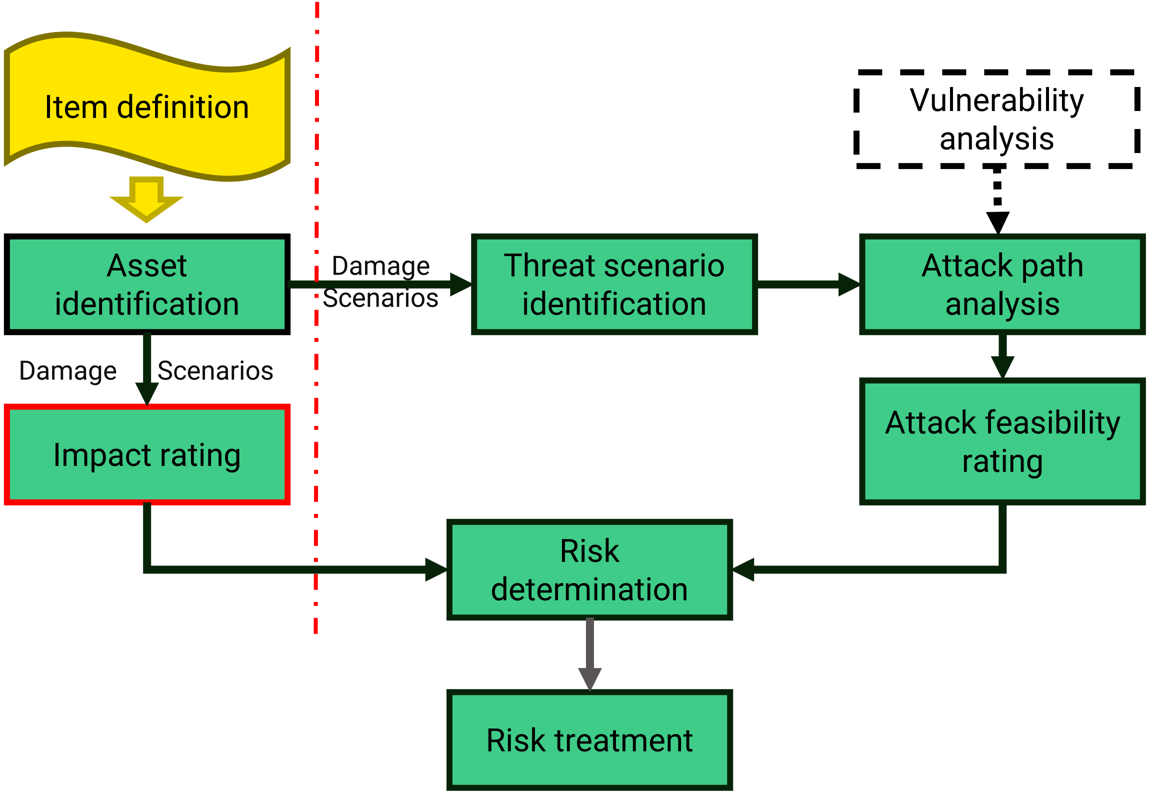
Assets and damage scenarios

Asset	Security property	Damage scenario
Driving commands	Integrity	Loss of integrity of driving commands compromise the safety of the vehicle due to incorrect driving commands
	Availability	The lane centering system is not available due to loss of driving commands
Driver input	Integrity	Unintended turn off or on lane centering system and wrong driver notification messages
	Availability	The lane keeping system cannot be turned on or off
LCS Status	Integrity	Incorrect system status is sent to the driver due to lack of integrity
	Availability	The system status is not available to the driver when required

Impact rating

Clause 15: TARA

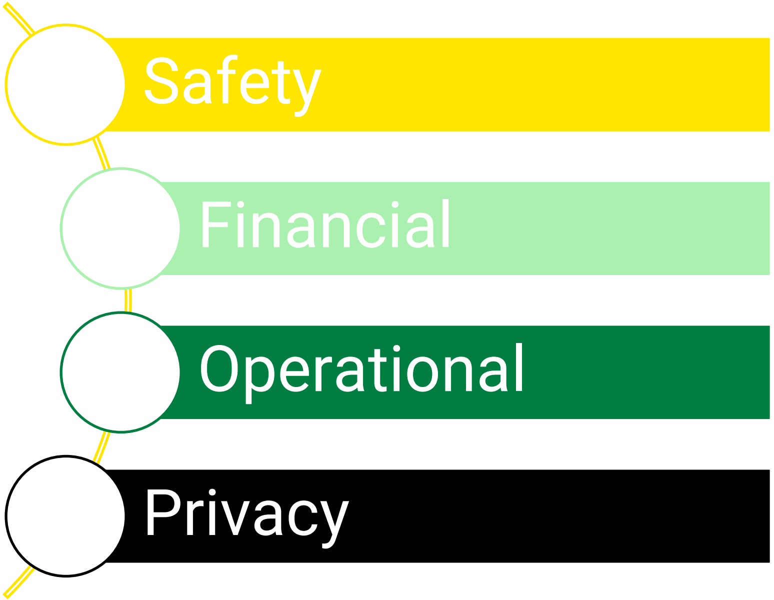
Impact rating



Clause 15: TARA

Impact rating: Key requirements

- The severity of impacts caused by the damage scenarios are assessed
- **Safety**, **financial**, **operational** and **privacy** impacts are core impact categories
  - Safety related impacts are derived from ISO 26262
- Additional categories can be considered (explanation needs to be added)
- Impact levels are **severe**, **major**, **moderate** and **negligible**
- If a category is rated as severe and the other categories are less critical, then further analysis may be omitted
- Impact can be transferred to an assurance company



Clause 15: TARA

DEKRA DIGITAL

Impact rating: Classification

	Severe	Major	Moderate	Negligible
Safety	Life-threatening injuries (survival uncertain), fatal injuries	Severe and life-threatening injuries (survival probable)	Light and moderate injuries	No injuries
Financial	Catastrophic consequences which the affected road user might not overcome	Substantial consequences which the affected road user will be able to overcome	Inconvenient consequences which the affected road user will be able to overcome with limited resources	No effect, negligible consequences or is irrelevant to the road user
Operational	Loss or impairment of a core vehicle function (vehicle not working or showing unexpected behavior of core functions)	Loss or impairment of an important vehicle function (significant annoyance of the driver)	Partial degradation of a vehicle function (user satisfaction negatively affected)	No impairment or non-perceivable impairment of a vehicle function
Privacy	Significant or even irreversible impact to the road user. Highly sensitive and easy to link to a personally identifiable information (PII)	Serious impact to the road user. The information is highly sensitive and difficult, or sensitive and easy to link to a PII principal	Inconvenient consequences to the road user. The information is sensitive but difficult, or not sensitive but easy to link to a PII principal	No effect, negligible consequences or is irrelevant to the road user. The information is not sensitive and difficult to link to a PII principal

Clause 15: TARA

Impact rating: Example I

Consider the headlamp system given as example in the ISO 21434

Asset	Damage scenario	Impact category	Impact rating
Lamp request	Headlamp function was inhibited, so the vehicle cannot be driven at night	Operational	?
	Collision caused by unintended turning-off headlamp	Safety	?
Oncoming car information	Malfunctioning automatic high beam	Operational	?

Clause 15: TARA

DEKRA DIGITAL

Impact rating: Example I

Consider the headlamp system given as example in the ISO 21434

Asset	Damage scenario	Impact category	Impact rating
Lamp request	Headlamp function was inhibited, so the vehicle cannot be driven at night	Operational	Major
	Collision caused by unintended turning-off headlamp	Safety	Severe
Oncoming car information	Malfunctioning automatic high beam	Operational	Moderate

Clause 15: TARA

DEKRA DIGITAL

Impact rating: Example II

Consider the Bluetooth connection between the mobile phone and the infotainment system

Asset	Damage scenario	Impact category	Impact rating
Personal data from mobile phone	Unauthorized access to personal information	Privacy	Major
	False contact data transmitted to the infotainment system	Financial	Moderate

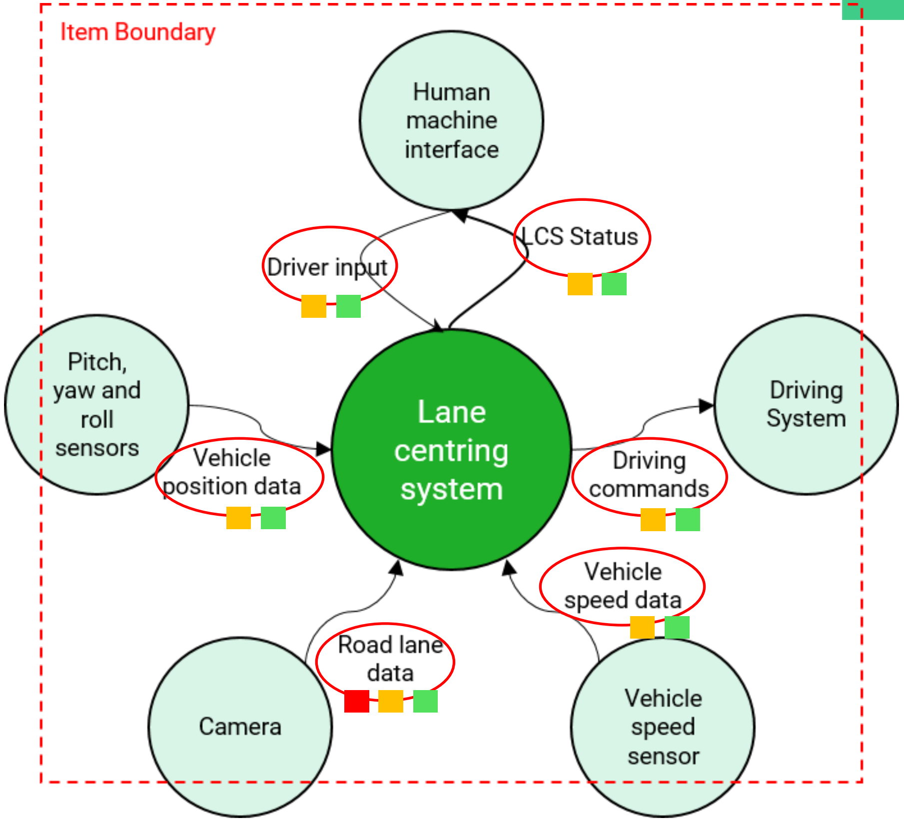
Example (Case study)

Clause 15: TARA

Asset Identification

Identify the cybersecurity relevant assets

- Asset
- Confidentiality
- Integrity
- Availability



Clause 15: TARA

DEKRA DIGITAL

Impact severity

Damage scenario	Safety	Financial	Operational	Privacy
The confidentiality of camera data is compromised and the private details such as the location or private property of the vehicle user is revealed				

Clause 15: TARA

DEKRA DIGITAL

Impact severity

Damage scenario	Safety	Financial	Operational	Privacy
The confidentiality of camera data is compromised and the private details such as the location or private property of the vehicle user is revealed	Negligible	Negligible	Negligible	Moderate

<u>Rationale:</u>

- The camera is used to detect the road lanes, while exposed does not create considerable safety, financial or operational impacts
- Since the camera captures the road lanes, no personally identified information is exposed
- Information about the location can be decoded and may be linked to a person. Hence rated as **moderate**

Clause 15: TARA

DEKRA DIGITAL

Impact severity

Damage scenario	Safety	Financial	Operational	Privacy
The system sends incorrect driving commands due to loss of integrity of camera data	Severe	Moderate	Major	Negligible

Rationale:

- Incorrect camera data may steer the vehicle off-course. May result in **severe safety impacts**
- It might cost to repair or replace the camera which leads to **moderate financial impacts**
- The LCS cannot be trusted due to incorrect camera data and the functionality cannot be used, creating **major operational impact** (Loss of functionality)
- Private impacts are neglected as no PIIs are involved

Clause 15: TARA

Impact severity

Damage scenario	Safety	Financial	Operational	Privacy
The LCS not available due to loss of camera data	Severe	Moderate	Major	Negligible

Rationale:

- Sudden loss of LCS due to loss of camera data could create a **severe safety impact** if the driver is not aware or in case of autonomous drive
- Repairing the vehicle may cause **moderate financial impact**
- Apart from safety, loss of function creates a **major operational impact**

Clause 15: TARA

DEKRA DIGITAL

Impact severity

Damage scenario	Safety	Financial	Operational	Privacy
The integrity of vehicle speed data is compromised, and the system doesn't work as indented because of incorrect driving commands	Severe	Moderate	Major	Negligible

Rationale:

- Incorrect vehicle speed data could lead to crash as the steering angle is determined from vehicle speed hence, severe safety impact
- Vehicle repair necessary (e.g. replace sensor, vehicle repair in the event of crash)
- Major operational impact as the LCS couldn’t be trusted and cannot be used

Clause 15: TARA

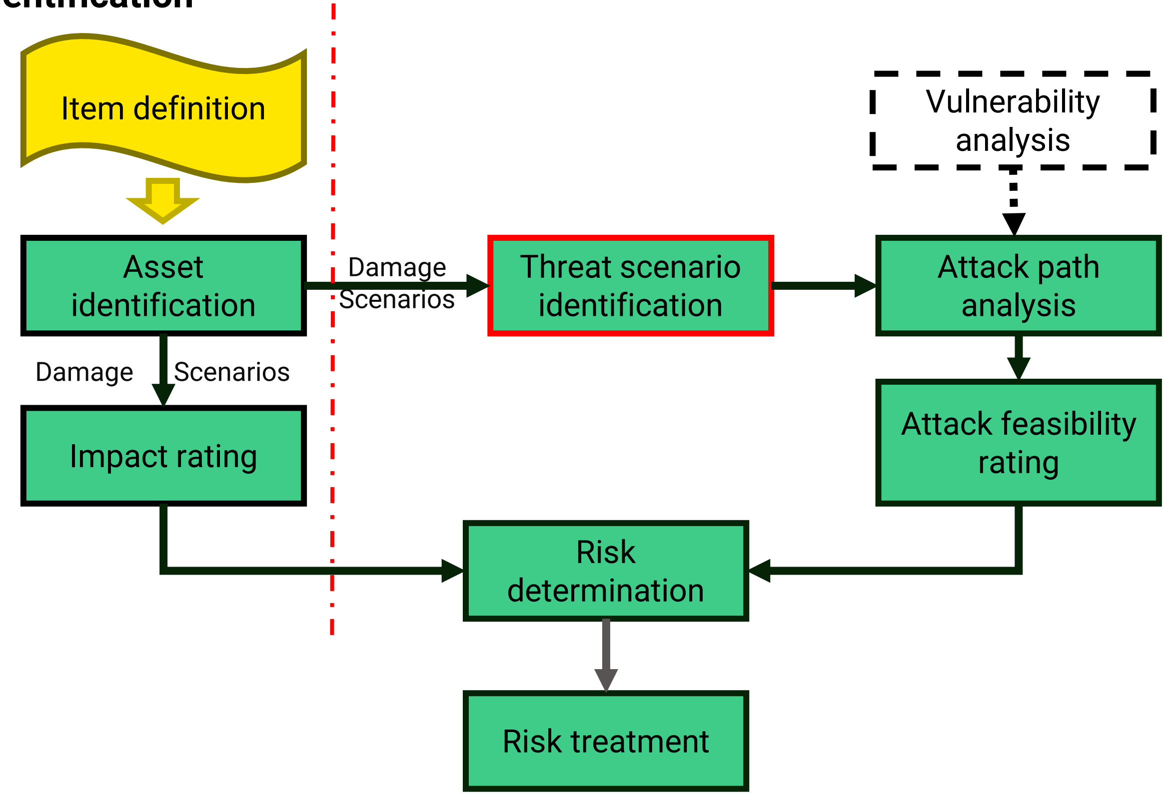
Impact severity

Damage Scenario	Safety	Financial	Operational	Privacy
The confidentiality of camera data is compromised and the private details such as the location or private property of the vehicle user is revealed	Negligible	Negligible	Negligible	Moderate
The system sends incorrect driving commands due to loss of integrity of camera data	Severe	Moderate	Major	Negligible
The lane centering system not available due to loss of camera data	Severe	Moderate	Major	Negligible
The integrity of vehicle speed data is compromised, and the system doesn't work as indented because of incorrect driving commands	Severe	Moderate	Major	Negligible
The loss of speed data leads to loss of the functionality	Severe	Moderate	Major	Negligible
Loss of integrity of driving commands compromise the safety of the vehicle due to incorrect driving commands	Severe	Moderate	Major	Negligible
The lane centering system is not available due to loss of driving commands	Severe	Moderate	Major	Negligible
The system doesn’t work as intended as incorrect drive commands are generated due to loss of integrity of vehicle position data	Severe	Moderate	Major	Negligible
The lane centering system is not available due to loss of vehicle position data	Severe	Moderate	Major	Negligible
Unintended turn off or on lane centering system and wrong driver notification messages	Severe	Moderate	Major	Negligible
The lane keeping system cannot be turned on or off	Negligible	Negligible	Major	Negligible
The driver doesn't receive the notifications from lane centering system	Moderate	Moderate	Moderate	Negligible

Threat scenario identification

Clause 15: TARA

Threat scenario identification



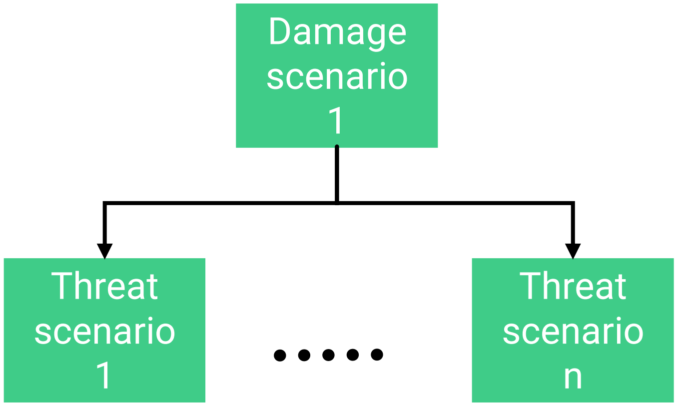
Clause 15: TARA

DEKRA DIGITAL

Threat scenario identification. Key requirements

"A threat scenario is a potential cause of compromise of cybersecurity properties of one or more assets in order to realize a damage scenario"- ISO21434

- **Threat scenario** can include:
  - Targeted asset
  - Compromised CS properties
  - Cause of compromise
- For each damage scenario, multiple threat scenarios can be identified
- Methods like group discussion, elicitation of malicious cases, threat modelling approaches (EVITA,TVRA, PASTA or STRIDE) can be used



Clause 15: TARA

Comparative threat modelling approaches

	STRIDE	EVITA	TVRA	PASTA
Definition	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege	E-safety Vehicle Intrusion protected Applications	Threat. Vulnerability, Risk Analysis	Proccess for Attack Simulation and Threat Analysis
Proposed by	Microsoft	European Community (17th Framework Programme)	ETSI	verSprite
Characteristics	• The threats are categorized based on the goals and purposes of the attacks • Relates threats with security properties	• Adopt ASIL of ISO26262 • Threats are defined in based on primary functions (e.g., fake messages, gain root access, corrupt data)	• Identify potential risk to a system based on the likelihood of an attack and the impact that would have on the system	• Align business objectives with technical requirements • Simulate attacks and analyze threats, in order to minimize the risk and associated impact to the business
Security Objectives	Operational, Safety, Privacy and Financial	Operational, Safety, Privacy and Financial	Related to the asset and its environment	Industry, geographic, local market, business

Clause 15: TARA

DEKRA DIGITAL

Comparative threat modelling approaches

	STRIDE	EVITA	TVRA	PASTA
Threats	• Spoofing • Tampering • Repudiation • Information disclosure • Denial of service • Elevation of privilege	Generic security threats (fake or corrupt messages, DoS, exploit implementation flaws, jamming, etc)	• Interception • Manipulation • Denial of service • Repudiation of sending • Repudiation of receiving	• Spoofing/Impersonation • Tampering of data • Repudiation • DoS • Elevation of privileges • Extortion • Research
Security properties	**Extend CIA model** • Authenticity • Integrity • Non-repudiability • Confidentiality • Availability • Authorization	• Authenticity • Integrity • Controlled access • Freshness • Non-repudiability • Anonymity • Privacy • Confidentiality • Availability	**C.I.A.A.A** • Confidentiality • Integrity • Availability • Authenticity • Accountability	**C.I.A.C** • Confidentiality • Integrity • Availability • Compliance
Impact rating	-	5 severity clases (S0-S4)	3 severity levels (low, medium, high)	-

Clause 15: TARA

Comparative threat modelling approaches

	STRIDE	EVITA	TVRA	PASTA
Process	• Decompose system into relevant components • Analyze each component susceptible to threats • Mitigate threats • Repeat process until find a secure solution (some threats can still remain)	• Define potential use cases • Define generic security threats and security properties compromised • Severity classification according security objectives • Evaluation of attack potential • Determine attack probability • Risk analysis	• Identification TOE • Identification of objectives • Identification of functional security requirements • Systematic inventory of assets • Systematic identification of vulnerabilities and threat level • Calculation of the likelihood of the attack and its impact • Establishment of the risk • Security countermeasure identification • Countermeasure cost-benefic identification • Specification of detailed requirements	• Define objectives • Define the technical scope • Decompose application • Analyze threats • Vulnerabilities and weaknesses analysis • Model attacks • Risk and impact analysis

Clause 15: TARA

DEKRA DIGITAL

Threat scenario identification: Example

Consider the headlamp system and identify the threat scenarios existing:

Damage scenario	Threat scenario
Collision caused by unintended turning-off headlamp	• **Target asset**: lamp request • **CS property compromised**: integrity • **Cause of compromise**: The signal sent to the Power switch actuator is spoofed. Consequently, the headlamp turns off when not intended
	• **Target asset**: lamp request • **CS property compromised**: integrity • **Cause of compromise**: tampering with a signal sent by Body Control ECU. Therefore, the headlamp turns off unintentionally
Malfunctioning automatic high beam	• **Target asset**: oncoming car information message • **CS property compromised**: availability • **Cause of compromise**: denial of service of oncoming car information message

Example (Case study)

Clause 15: TARA

Threat Scenario Identification

Damage scenario	Threat scenario
The confidentiality of camera data is compromised and the private details such as the location or private property of the vehicle user is revealed	• **Target asset**: camera data • **CS property compromised**: confidentiality • **STRIDE attack method :** information disclosure • **Cause of compromise**: Addition of malicious hardware in the communication channel allows the attacker to read camera data
The system sends incorrect driving commands due to loss of integrity of camera data	• **Target asset**: camera data • **CS property compromised**: integrity • **STRIDE attack method :** spoofing • **Cause of compromise**: The camera input is spoofed by the attacker and the camera sends wrong data
	• **Target asset**: camera data • **CS property compromised**: integrity • **STRIDE attack method :** tampering • **Cause of compromise**: The camera is tampered by the attacker and the camera sends wrong data

Clause 15: TARA

DEKRA DIGITAL

Threat Scenario Identification

Damage scenario	Threat scenario
The integrity of vehicle speed data is compromised, and the system doesn't work as intended due to incorrect driving signals	• **Target asset**: vehicle speed data • **CS property compromised**: integrity • **STRIDE attack method :** tampering • **Cause of compromise**: The vehicle speed data is tampered via hardware replacement
	• **Target asset**: vehicle speed data • **CS property compromised**: integrity • **STRIDE attack method :** tampering • **Cause of compromise**: Vehicle speed data is tampered through a malicious program

Clause 15: TARA

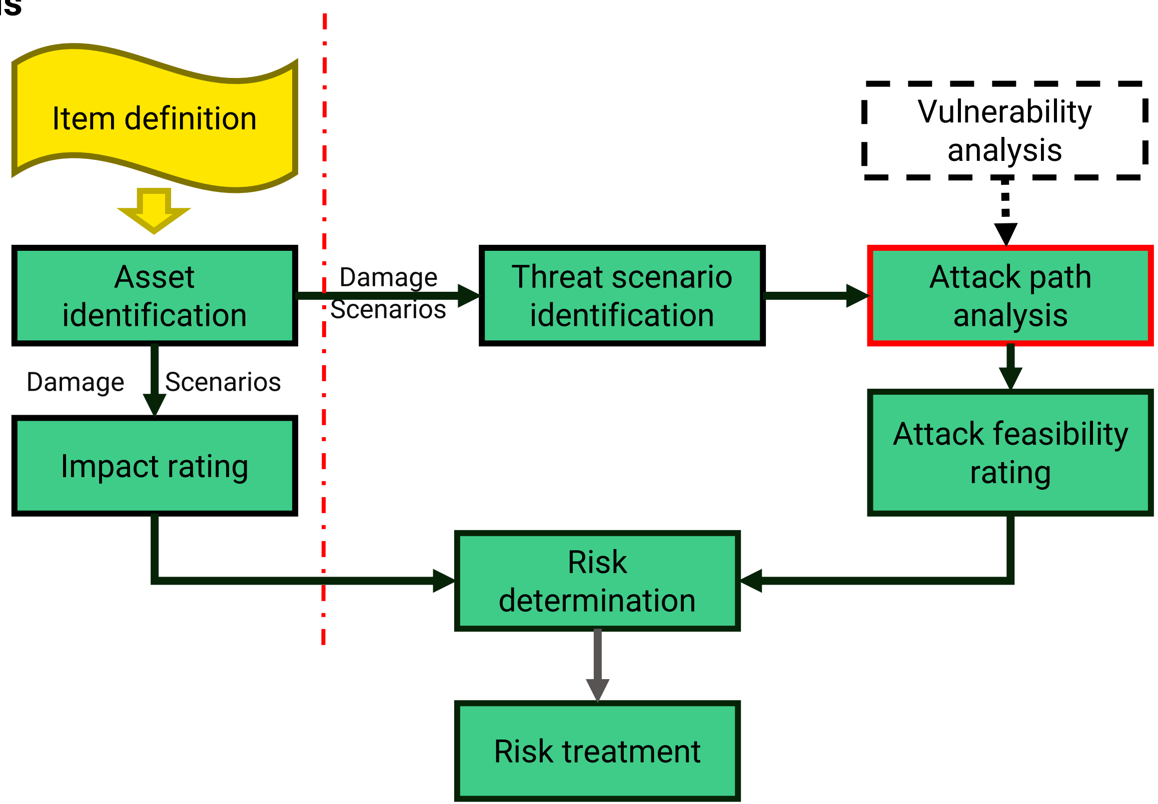
Threat Scenario Identification

Damage scenario	Threat scenario
The confidentiality of camera data is compromised and the private details such as the location or private property of the vehicle user is revealed	The attacker is able to attach a hardware device to the vehicle network. This allows the attacker to read the camera data
The system sends incorrect driving commands due to loss of integrity of camera data	The camera input is spoofed by the attacker and the camera sends wrong data
	The camera is tampered by the attacker and the camera sends wrong data
The lane centering system not available due to loss of camera data	The communication of camera data is severed by the attacker such that the road lane data is not usable
The integrity of vehicle speed data is compromised, and the system doesn't work as intended because of incorrect driving commands	The speed sensor data is tampered which in turn sends incorrect speed data
The loss of speed data leads to loss of the functionality	The communication of vehicle speed data is severed by the attacker such that the speed data is not usable
Loss of integrity of driving commands compromise the safety of the vehicle due to incorrect driving commands	The lane centering system is corrupted via malicious codes which sends incorrect driving commands
The lane centering system is not available due to loss of driving commands	The driving commands are made useless due to loss of communication.
The system doesn’t work as intended as incorrect drive commands are generated due to loss of integrity of vehicle position data	The pitch and yaw sensors are tampered by an attacker and the sensors send incorrect signals
The lane centering system is not available due to loss of vehicle position data	The communication of pitch and yaw sensors are tampered
Unintended turn off or on lane centering system and wrong driver notification messages	The driver inputs and notifications are tampered using some malicious program
The lane keeping system cannot be turned on or off	The turn on or off signals is disrupted using malicious software
The driver doesn't receive the notifications from lane centring system	The lane centering system is corrupted via malicious codes hence the notifications are blocked

Attack path analysis

Clause 15: TARA

Attack path analysis



Clause 15: TARA

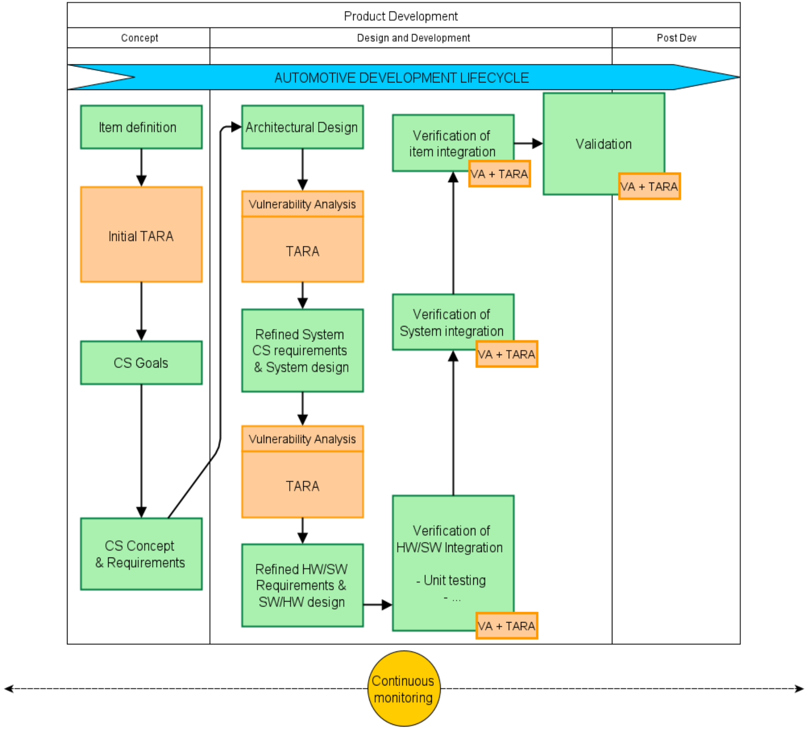
Attack path analysis: Key requirements

Supporting information:

- Weaknesses from CS events
- Weaknesses during product development
- Architectural design
- Identified attack paths
- Vulnerability analysis

Analyse threat scenarios to identify attack paths, based on:

- Top-down approach
- Bottom-up approach



Attacks paths can be updated when more information becomes available after perform a vulnerability analysis (during product development)

Clause 15: TARA

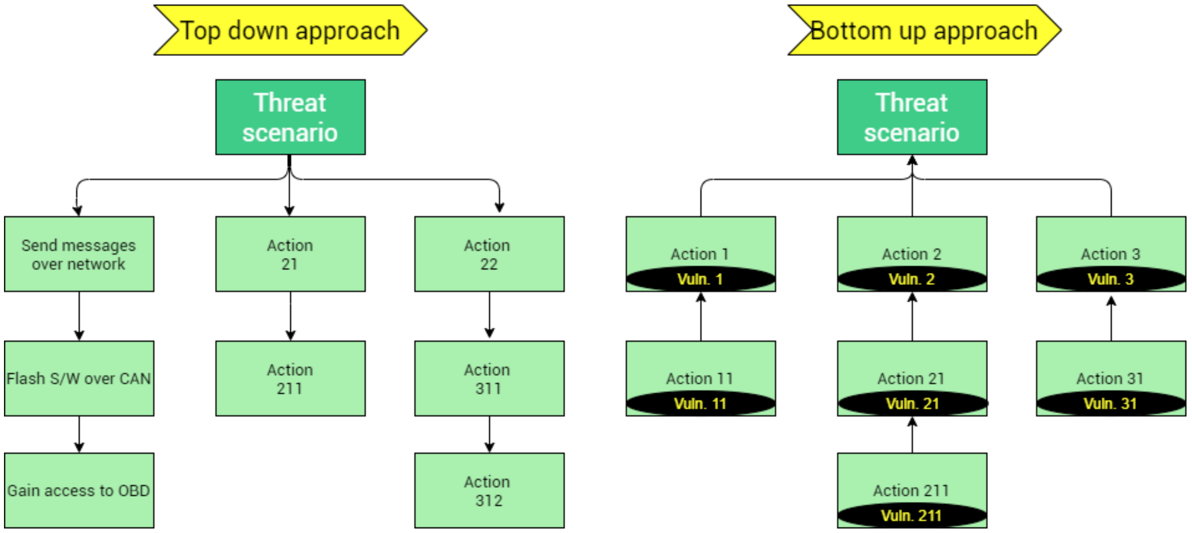
Attack path analysis: Approaches to identify attack paths

Top-down approach (Deductive):

- Developer's view
- Used during initial stages of development (left side of the V-model)
- Analyse the different ways in which a threat scenario can be realized
- Examples: attack trees, attack graphs

Bottom-up approach (Inductive):

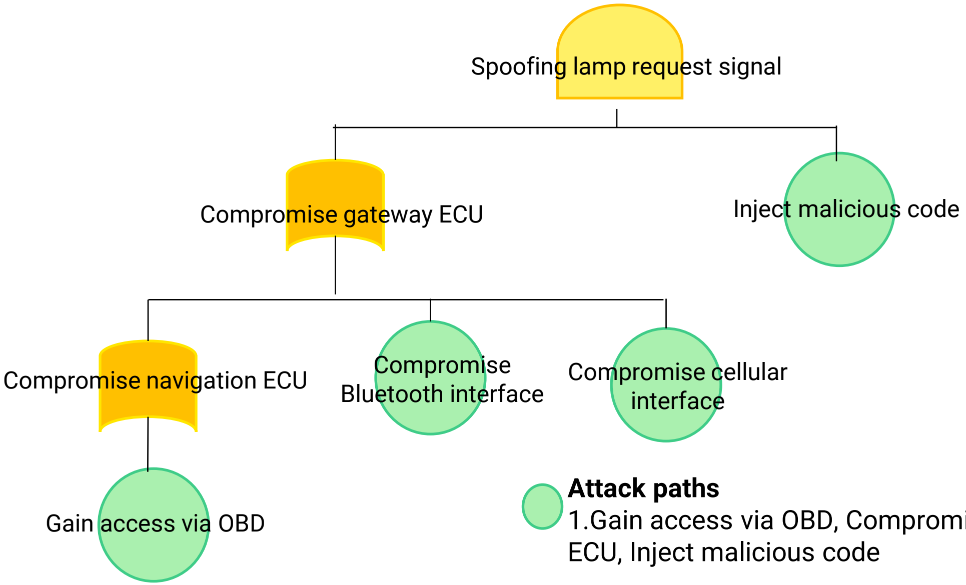
- Attacker's view
- Used during later stages of development (right side of the V-model)
- Mostly used for vulnerability analysis



Clause 15: TARA

Attack path analysis: Attack Tree Example I

- Hierarchical conceptual diagrams that show how low-level activities interact and combine to reach the attacker’s objective (Threat scenario)
- The tree root is the goal for the attack, and the leaves are the ways to achieve that goal
- Intermediates nodes are AND/ OR nodes:
  - AND :all underneath actions must be performed
  - OR :at least one action underneath must be performed
- Easy to use when there is an understanding of the system



There are 3 attack paths for this threat scenario

Asset: Lamp request

CS properties: Integrity and Availability

Threat scenario: Spoofing lamp request signal

Attack paths

1.Gain access via OBD, Compromise Gateway ECU, Inject malicious code

2. Compromise Bluetooth Interface, Compromise Navigation ECU, Compromise Gateway ECU, Inject malicious code

3. Compromise cellular interface, Compromise Navigation ECU, Compromise Gateway ECU, Inject malicious code

Intermediate node

Root node

Clause 15: TARA

Attack path analysis: Attack Tree Example II

Asset: Oncoming car information

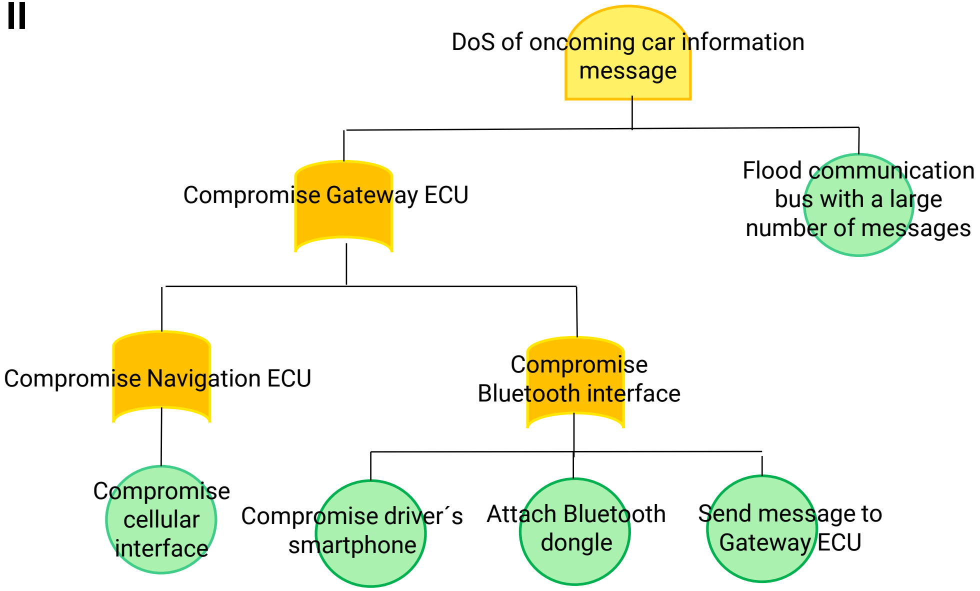
CS properties: Integrity and Availability

Threat scenario: DoS of oncoming information message

Attack paths

Intermediate node

Root node



There are 2 attack pa this threat scenario

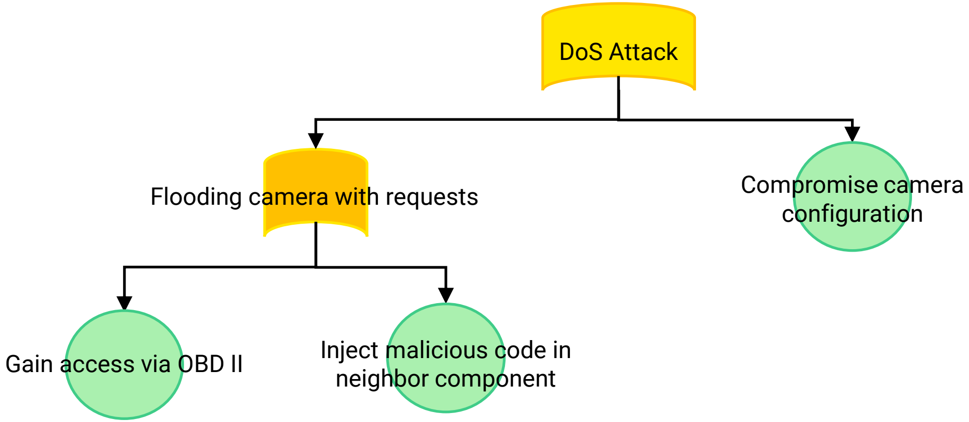
Example (Case study)

Clause 15: TARA

Attack analysis

Threat scenario : The lane centering system not available due to loss of camera data

Attack method : Denial of Service

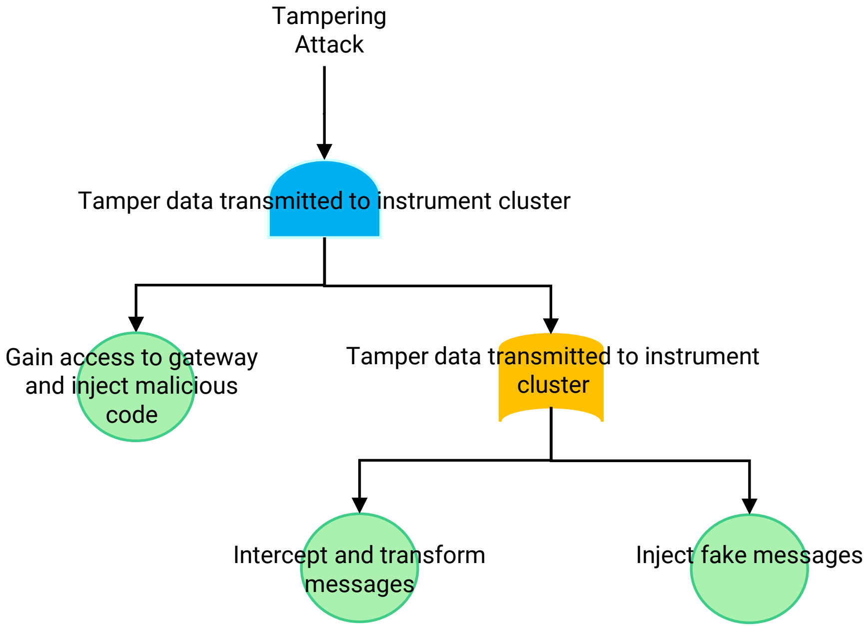


Clause 15: TARA

Attack analysis

Threat scenario : LCS status information is tampered, wrongly showing that it is enabled.

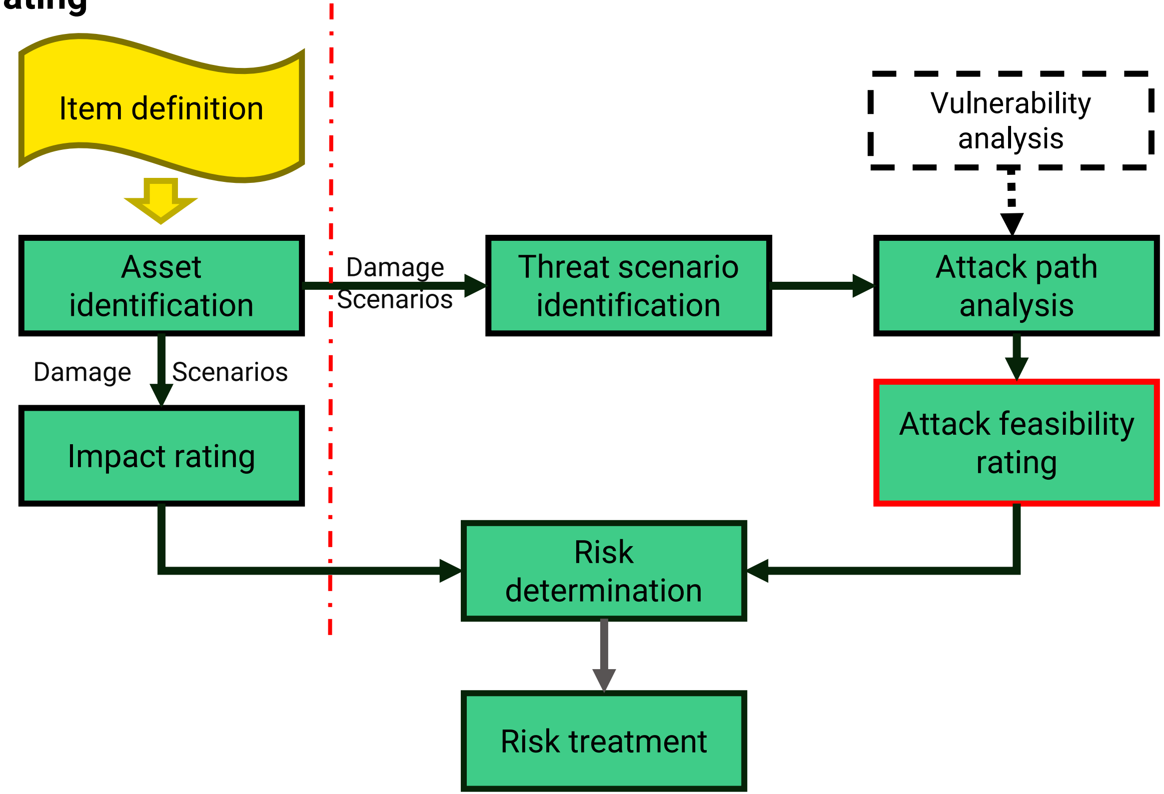
Attack method : Tampering



Attack feasibility rating

Clause 15: TARA

Attack feasibility rating



Clause 15: TARA

DEKRA DIGITAL

Attack feasibility rating: Key requirements

"Attack feasibility is an attribute of an attack path describing the ease of successfully carrying out the corresponding set of actions" – ISO21434

- Attack feasibility rating performed for each attack path

Attack feasibility rating	Description
High	Attack path can be completed using low effort
Medium	Attack path can be completed using medium effort
Low	Attack path can be completed using high effort
Very low	Attack path can be completed using very high effort

Clause 15: TARA

Attack feasibility rating: Approaches

Attack feasibility rating approaches

- Attack potential based approach
- CVSS based approach
- Attack vector based approach

Depends on information available and phase in the lifecycle

Clause 15: TARA

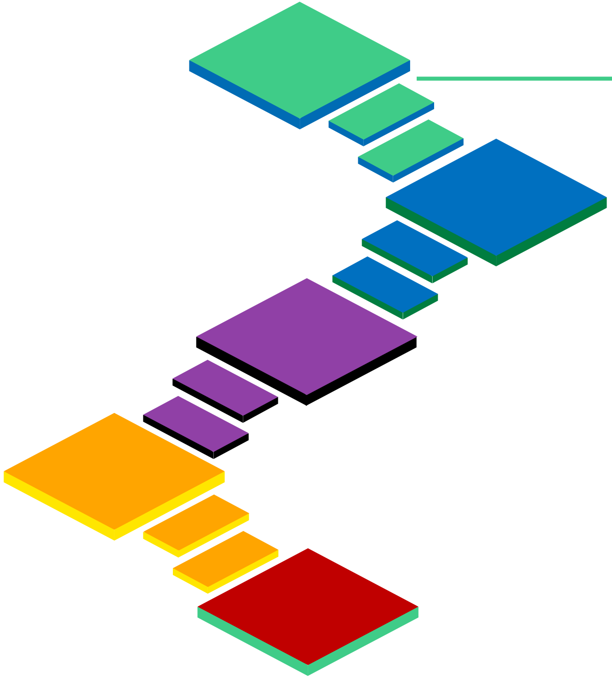
Attack feasibility rating

Attack potential based approach

- Attack feasibility determined from attack potential
- Effort required to successfully perform an attack on an item or component
- Expressed in terms of an attacker´s expertise and resources
- Determined by 5 core factors (ISO/IEC 18045)
- For each factor, different levels and their corresponding values are defined
- The attack potential is the sum of the values

Clause 15: TARA

Attack potential based approach: Factors determining attack potential



Elapsed time

Time required to identify and exploit a vulnerability.

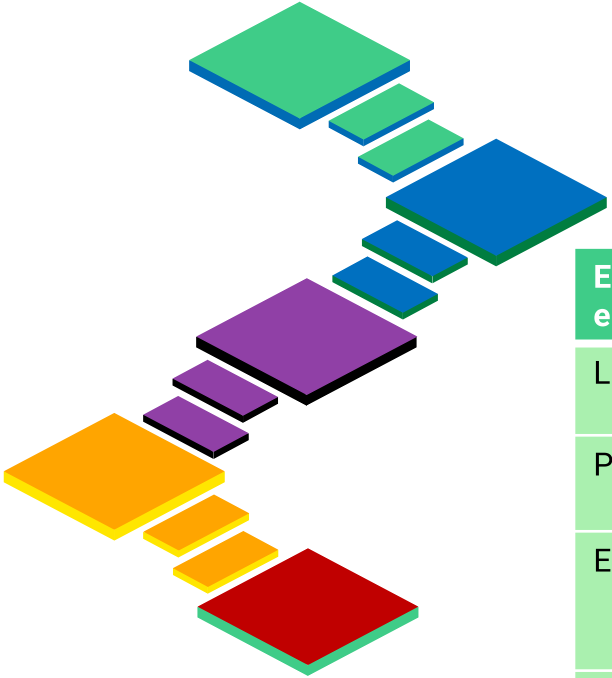
Elapsed Time	
Enumerate	**Value**
< 1 week	0
< 1 month	1
< 6 months	4
<= 3 years	10
> 3 years	19

Elapsed time rating is also based on the knowledge and resources of the attacker.

Greater attacker´s capability → Less elapsed time

Clause 15: TARA

Attack potential based approach: Factors determining attack potential



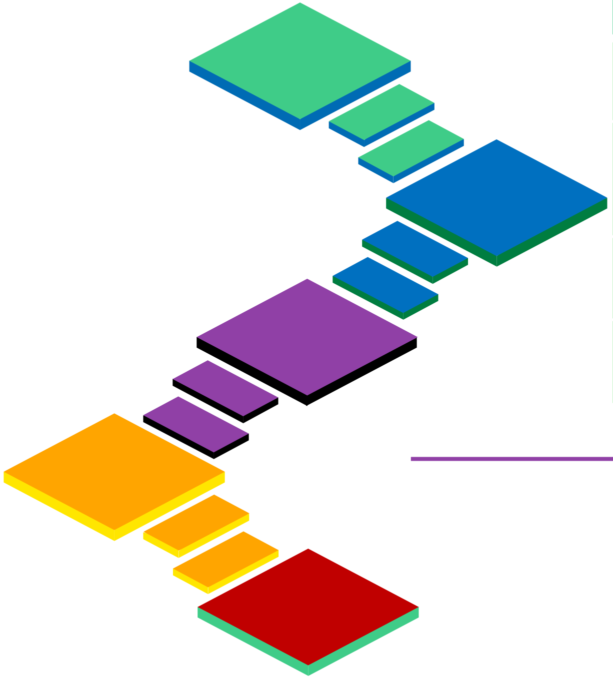
Related to the capabilities of the attacker, e.g: skills, experience, etc.

Specialist expertise

Enumerate	Description	Value
Layman	No previous experience as an attacker	0
Proficient	Familiar with security aspects of the product/system and simple attack methods	3
Expert	Familiar with the algorithms, protocols, HW, structures, security behavior, principles and concepts of security, etc. implemented in the product/system	6
Multiple experts	Experience in different fields to perform a complete attack	8

Clause 15: TARA

Attack potential based approach: Factors determining attack potential



Enumerate	Description	Value
Public	Public information concerning the item/component (Homepage, Internet)	0
Restricted	Restricted information concerning the item/component (Internal documentation, requirements, design specifications). Shared between OEMs and suppliers, previous agreement	3
Confidential	Confidential information about the item/component. Shared within an organization	7
Strictly confidential	Strictly confidential information about the item/component. Only a few individuals have access	11

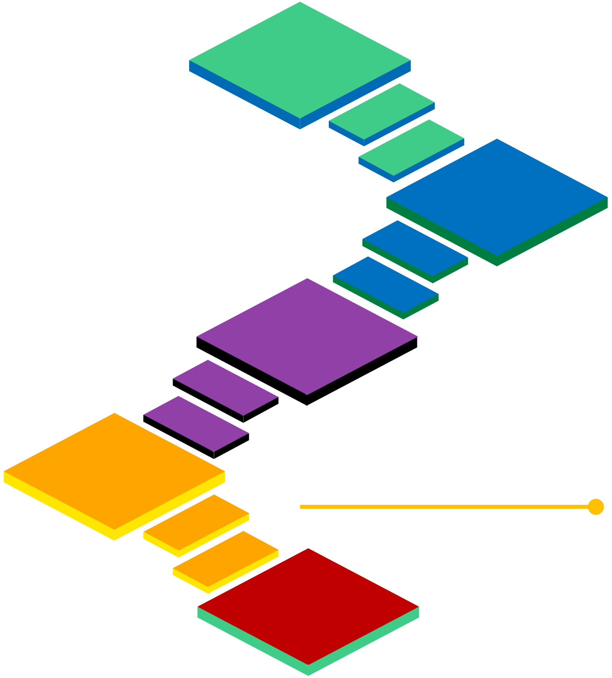
Knowledge of the item or component

Information the attacker has obtained about the item or component

Clause 15: TARA

DEKRA DIGITAL

Attack potential based approach: Factors determining attack potential



Enumerate	Description	Value
Unlimited	Remote or physical access to the item/ component without any time limitation	0
Easy	Remote or physical access to the item/component during a limited time (during Bluetooth pairing or remote SW update)	1
Moderate	Remote or physical access limited to the item/component (access via OBD port)	4
Difficult	Impractical remote or physical access to the item/component	10

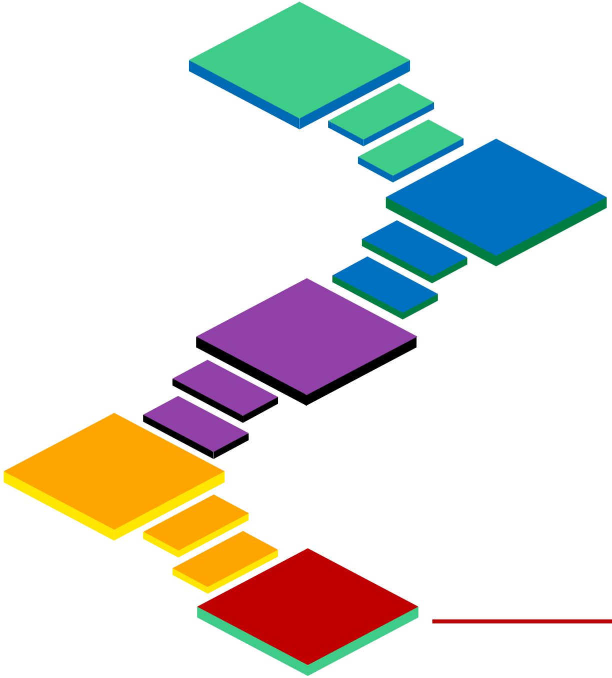
Window of opportunity

Access conditions to successfully perform an attack

- Access type: logical (remote) and physical
- Access duration: unlimited and limited

Clause 15: TARA

Attack potential based approach: Factors determining attack potential



Enumerate	Description	Value
Standard	Equipment is available to the attacker (Laptop, CAN adapter, OS debugger,…)	0
Specialized	Equipment is not available to the attacker but can be acquired without effort (HiL, HW debugging device)	4
Bespoke	Equipment is specially produced and not available to the public. High cost and its distribution is controlled, even restricted.	7
Multiple bespoke	Use of different bespoke equipment for distinct steps of an attack	9

Equipment

Tools available to discover the vulnerability and/or execute the attack

Clause 15:TARA

Attack potential based approach: Attack potential and feasibility determination

- For each attack path, the above-mentioned parameters are evaluated, and the sum of the values is calculated to determine the attack feasibility associated.

Sum of values	Attack potential	Attack feasibility
0 – 9	Basic	High
10 – 13	Enhanced basic	
14 – 19	Moderate	Medium
20 – 24	High	Low
=> 25	Beyond high	Very low

Clause 15:TARA

Attack potential based approach: Example

- ET Elapsed Time
- SE Specialist Expertise
- KoIC Knowledge of the item or component
- WoO Windows of Opportunity
- Eq Equipment

DEKRA DIGITAL

Threat scenario	Attack path	Attack feasibility assessment						
		ET	SE	KoIC	WoO	Eq	Value	Attack feasibilty rating
DoS of oncoming car information message *Organization can apply rationale to each of the ratings based on their own policy	a. Compromise Navigation ECU from cellular interface b. Navigation ECU transmits malicious control signals b. Gateway ECU forwards malicious signals to Power Switch Actuator c. Floods the communication bus with a larger number of messages	1	8	7	0	4	20	Low
	a. Attaches a Bluetooth-enabled OBD b. Compromise driver´s smartphone with Bluetooth interface c. Sends message via smartphone and Bluetooth dongle to Gateway ECU d. Gateway ECU forwards malicious signals to Power Switch Actuator e. Floods the communication bus with a larger number of messages	1	8	7	4 *physical access required	4	24	Low

Clause 15: TARA

Attack feasibility rating: CVSS-based approach

- The Common Vulnerability Scoring System (CVSS) is an open framework to indicate the severity of vulnerabilities
- Maintained by the Forum of Incident Response and Security Teams (FIRST)
- Define three metric groups**:**
  - **Base metrics**: intrinsic characteristics of a vulnerability. Constant over time and in different user environments. Categorized into **exploitability** metrics and **impact** metrics

  * Only exploitability metrics are considered

  - **Temporal metrics**: characteristics of a vulnerability that change over time
  - **Environment metrics**: characteristics of a vulnerability that are relevant and unique to a particular user´s environment

Clause 15: TARA

Attack feasibility rating: CVSS-based approach

Base metrics

Exploitability
- Attack vector
- Attack complexity
- Privileges required
- User interaction

Impact
- Confidentiality impact
- Integrity impact
- Availability impact

Temporal metrics
- Exploit code maturity
- Remediation level
- Report confidence

Environmental metrics
- Modified Base metrics
- Confidentiality requirement
- Integrity requirement
- Availability requirement

Clause 15: TARA

DEKRA DIGITAL

Attack feasibility rating: CVSS-based approach

Base Metrics. Attack Vector

- Level of access required for an attacker to exploit the vulnerability

Metric	Description	Value
Network (N)	Vulnerabilities are remotely exploitable, from one or more network hops away and including exploitation over the Internet	0.85
Adjacent (A)	Vulnerabilities requires network adjacency for exploitation. Attack must be launched from the same physical or logical network	0.62
Local (L)	Vulnerabilities are not exploitable over a network. Attacker must access the system locally, remotely or requires social engineering	0.55
Physical (P)	Attacker physically interact with the vulnerable component	0.2

Clause 15: TARA

Attack feasibility rating: CVSS-based approach

Base Metrics. Attack Complexity

- Conditions required to exploit a vulnerability.

Metric	Description	Value
Low (L)	There are no specific pre-conditions required. Attack is successful repeatedly times	0.77
High (H)	Attacker needs preparation, time and effort to be performed successfully	0.44

Clause 15: TARA

Attack feasibility rating: CVSS-based approach

Base Metrics. Privileges required

- Level of privileges an attacker must have before successful exploit a vulnerability

Metric	Description	Value
None (N)	No privileges or special access required	0.85
Low (L)	The attacker requires basic user level privileges. Only access to non-sensitive resources	0.62
High (H)	The attacker requires administrative privileges.	0.27

Base Metrics. User interaction

- Determine whether the user must participate in the successful compromise of the vulnerability.

Metric	Description	Value
None (N)	No user interaction is required	0.85
Required (R)	User must interact for the successful exploitation of a vulnerability	0.62

Clause 15: TARA

Attack feasibility rating: CVSS-based approach

- Exploitability

Exploitability = 8.22 x Attack vector x Attack complexity x Privileges required x User interaction

Attack feasibility rating	CVSS exploitability value
High	2.96 - 3.89
Medium	2.00 - 2.95
Low	1.06 - 1.99
Very low	0.12 – 1.05

- Impact, determined by CIA model

Clause 15: TARA

Attack feasibility rating: Attack vector-based approach

- Similar to CVSS-based approach
- Evaluate predominant attack vector of each attack path
- If the attack is performed remotely, then the attack feasibility is higher

Attack feasibility rating	Criteria
High	**Network**: potential attack path is related to the network without limitations (cellular network directly connected on the Internet)
Medium	**Adjacent**: potential attack path is related to the network, but it is limited physically or remotely (Bluetooth interface)
Low	**Local**: potential attack path is not related to the network and threat agents require direct access to the item (USB, memory cards)
Very low	**Physical**: threat agents require physical access

Clause 15: TARA

DEKRA DIGITAL

Attack vector-based approach: Example

Considering the lamp request example included in ISO 21434. Determine the attack feasibility rating using the attack vector based-approach:

Attack path	Attack feasibility rating
a. Compromises navigation ECU from Cellular interface b. Compromised navigation ECU transmits malicious control signal c. Gateway ECU forwards malicious signal to power switch actuator d. Malicious signals spoof the lamp request	High *Cellular directly connected to Internet
a. Compromises navigation ECU from Bluetooth interface b. Compromised navigation ECU transmits malicious control signal c. Gateway ECU forwards malicious signal to power switch actuator d. Malicious signals spoof the lamp request	Medium
a. Gets local access to OBD connector b. Sends malicious control signals from OBD connector c. Gateway ECU forwards malicious signal to power switch actuator d. Malicious signals spoof the lamp request	Low *Access physically to the item

Example (Case study)

Clause 15: TARA

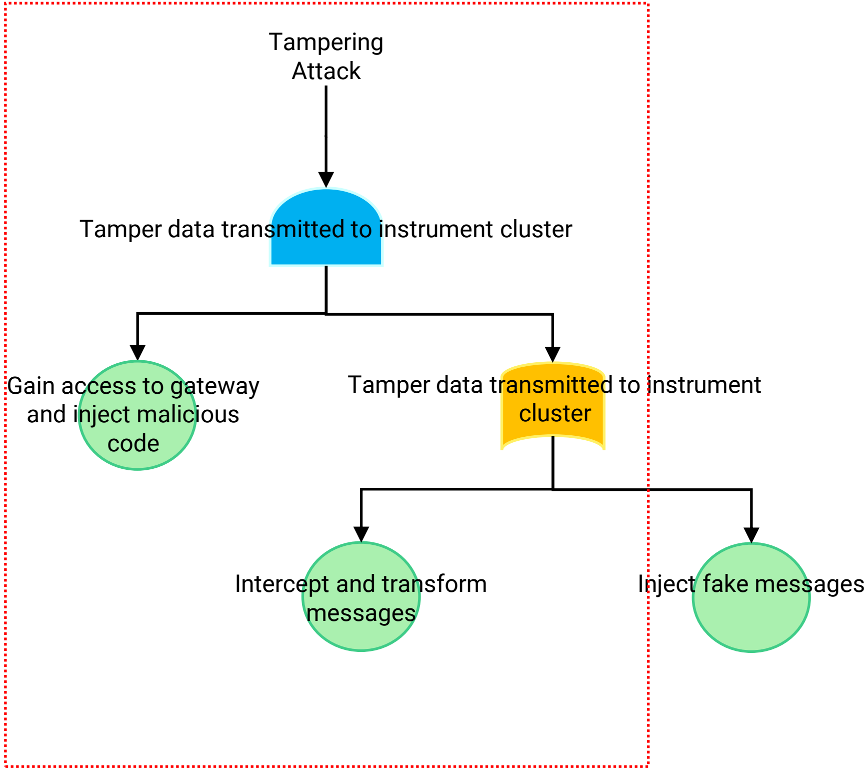
Attack feasibility (Attack potential based)

The attacker wants to tamper the LCS notification in order to always show it as enabled.

In order to do so :

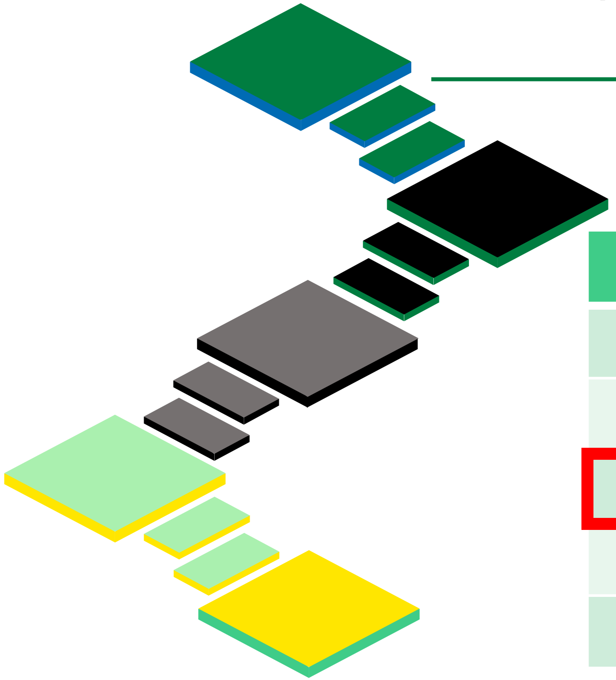
- The attacker needs access to the central gateway, and inject malicious runnable code
- The code shall be able to intercept the “LCS disabled” messages and transform them as “LCS enabled” messages

Considered attack for analysis



Clause 15: TARA

Attack feasibility (Attack potential based)



Factors determining attack potential

Elapsed time

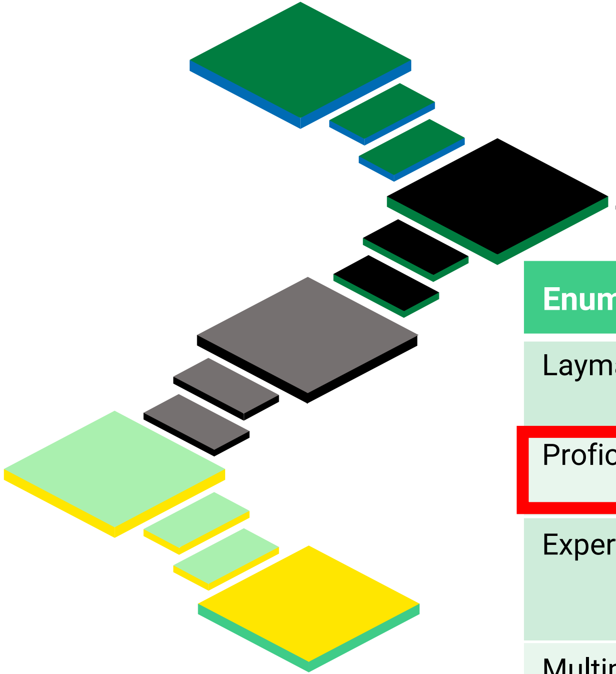
Time taken to identify and exploit a vulnerability.

Enumerate	Value
< 1 week	0
< 1 month	1
< 6 months	4
<= 3 years	10
> 3 years	19

Note: The elapsed time is rated based on the expert knowledge at the time of rating, there are some methods that excludes this factor (e.g. HEAVENS) as elapsed time depends on the knowledge, expertise and resources of the attacker. i.e. greater the attacker's capability, lesser the elapsed time.

Clause 15: TARA

Attack feasibility (Attack potential based)



Factors determining attack potential

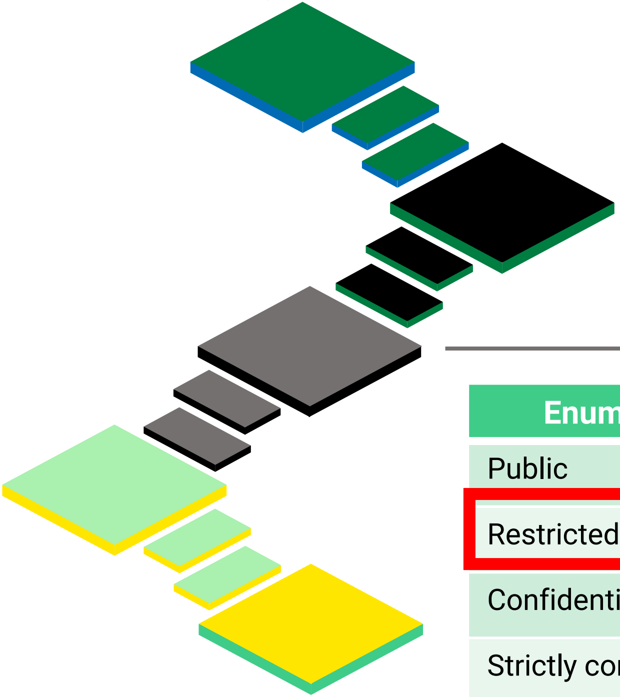
Specialist expertise — Required level of knowledge of underlying principles, attack methods, etc.

Enumerate	Description	Value
Layman	Unknowledgeable compared to experts or proficient persons, with no particular expertise	0
Proficient	Knowledgeable in that they are familiar with the security behavior of the product or system type.	3
Expert	Familiar with the underlying algorithms, protocols, hardware, structures, security behavior, principles and concepts of security, etc. implemented in the product or system type	6
Multiple experts	different fields of expertise are required at an Expert level for distinct steps of an attack	8

Clause 15: TARA

Attack feasibility (Attack potential based)

Factors determining attack potential



Knowledge of the TOE

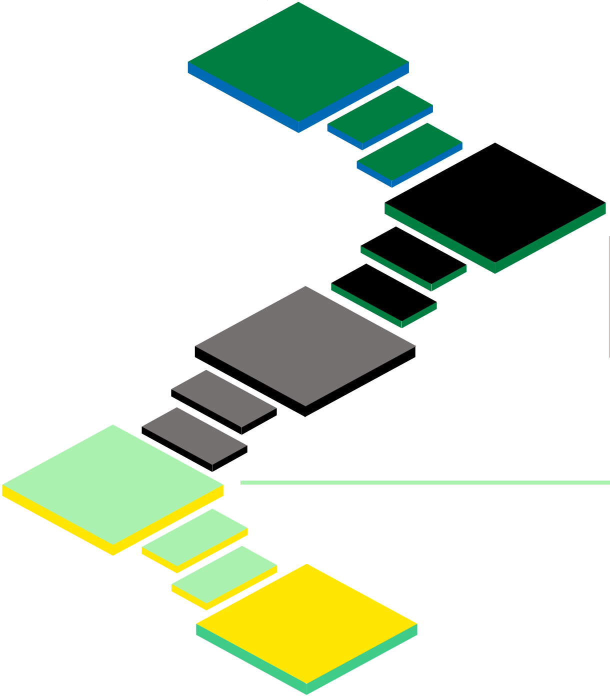
Design and operation knowledge about TOE

Enumerate	Description	Value
Public	Public information concerning the item or component.	0
Restricted	Restricted information concerning the item or component.	3
Confidential	Confidential information about the item or component.	7
Strictly confidential	Strictly confidential information about the item or component.	11

Clause 15: TARA

DEKRA DIGITAL

Attack feasibility (Attack potential based)



Factors determining attack potential

Enumerate	Description	Value
Unlimited	High availability without any time limitation. Remote access without physical presence or time limitation as well as unlimited physical access to the item or component.	0
Easy	High availability and limited access time. Remote access without physical presence, as well as limited physical access to the item or component	1
Moderate	Low availability of the item or component. Limited physical and/or logical access. Physical access to the vehicle interior or exterior without using any special tools.	4
Difficult	Very low availability of the item or component. Impractical level of access to the item or component to perform the attack	10

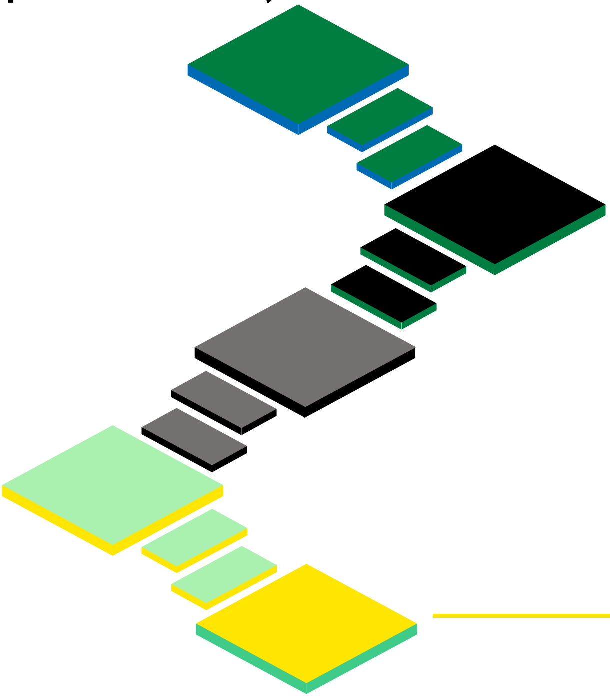
Window of opportunity

Required by the attacker to launch successful attack without being detected.

Clause 15: TARA

DEKRA DIGITAL

Attack feasibility (Attack potential based)



Factors determining attack potential

Enumerate	Description	Value
Standard	Equipment is readily available to the attacker, either for the identification of a vulnerability or to mount an attack.	0
Specialized	Equipment is not readily available to the attacker but can be acquired without undue effort.	4
Bespoke	Equipment is not readily available to the public (e.g., black market) as it may need to be specially produced (e.g., very sophisticated software), or because the equipment is so specialized that its distribution is controlled, possibly even restricted	7
Multiple bespoke	This rating is used for a situation, where different types of bespoke equipment are required for distinct steps of an attack.	9

Equipment

Equipment required for exploitation (IT, HW, SW).

Clause 15: TARA

DEKRA DIGITAL

Attack feasibility (Attack potential based)

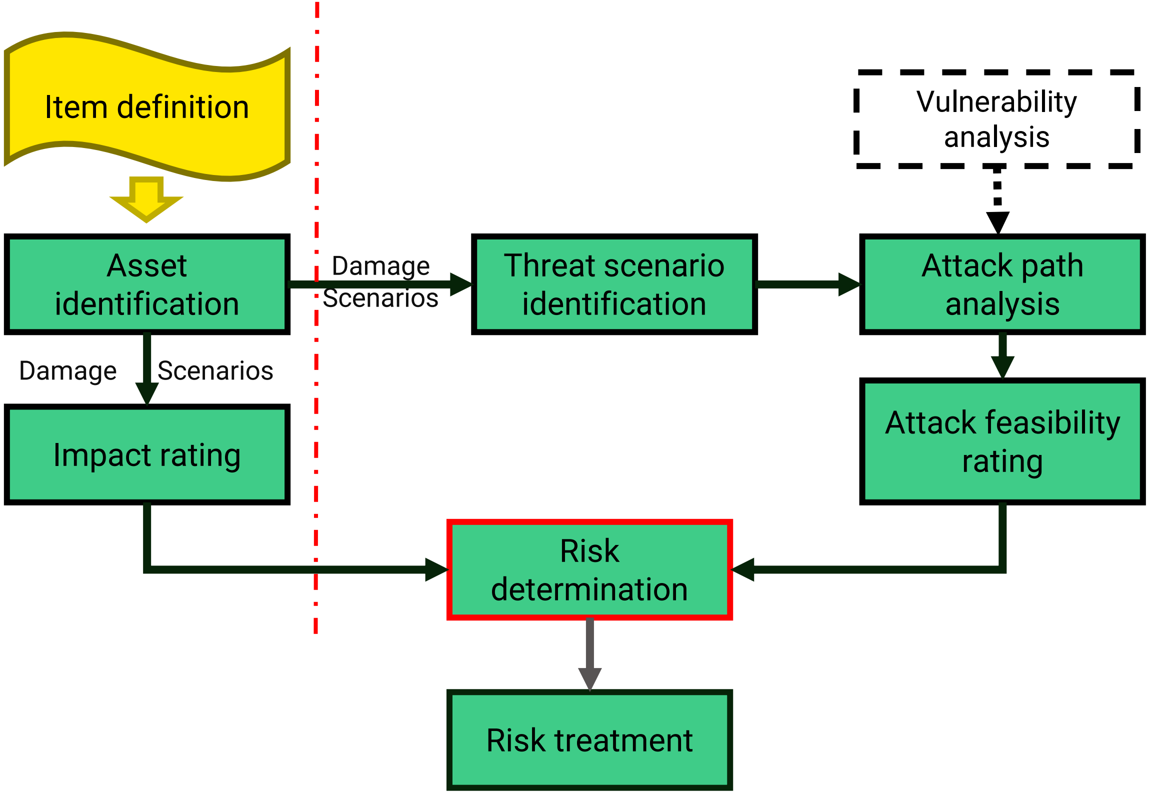
Result:

Parameter	Rating	Value	Rationale
Elapsed time	<= 6 months	4	The system is immature, and no security controls or components are present at this stage
Specialist expertise	Proficient	3	To create a malware the attacker should have a good understanding of the security behavior of the system
Knowledge of the TOE	Restricted	3	Information such as design documents are necessary
Window of opportunity	Moderate	4	Attacker can reach the physical ports easily
Equipment	Specialized	4	The attacker is able to create and launch an attack using tools that can be acquired easily
	Sum	22	Attack feasibility **Low**

Risk determination

Clause 15: TARA

Risk determination



Clause 15: TARA

Risk determination

- Determine risk value for each threat scenario, considering impact and attack feasibility ratings
- If more than one category is impacted (S, F, O, P), determine the risk value for each of them
- Risk value should be between 1 and 5; (1 = minimal risk)
- Methods
  - Risk matrices
  - Risk formulas

Clause 15: TARA

Risk determination: Risk Matrix

- Defined by the organisation

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

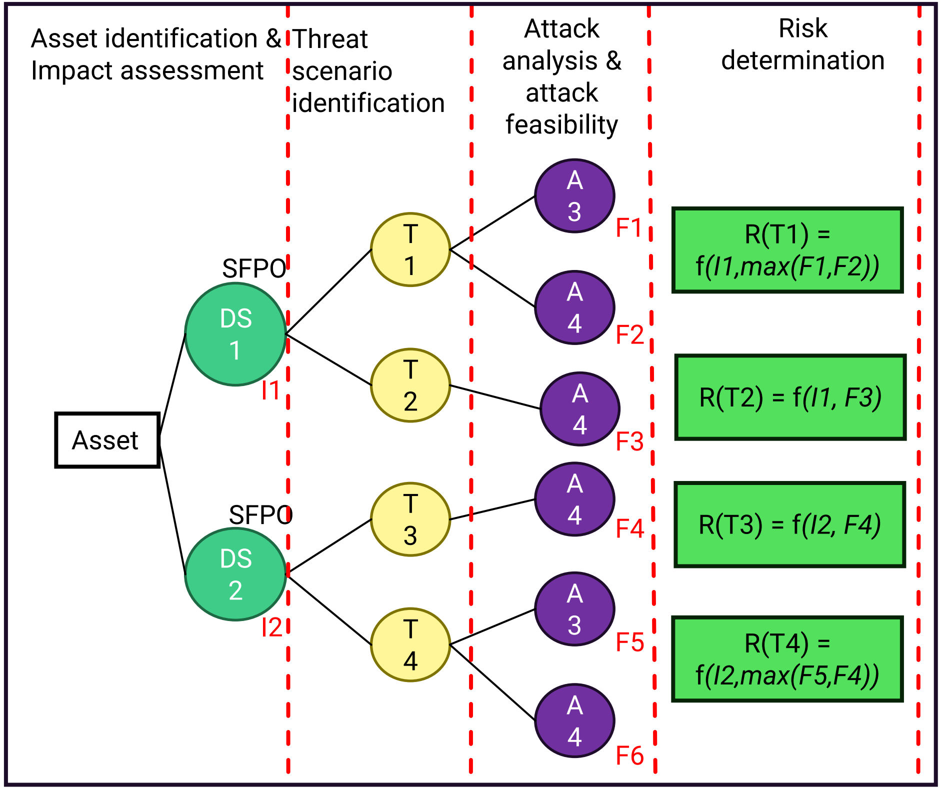
Risk determination: Risk Formula

- Defined by the organization

Risk = 1 + Impact x Attack feasibility

Clause 15: TARA

Risk determination



Legend:

DS → Damage scenario

I → Impact severity

T → Threat scenario

A → Attack path

F → Attack feasibility

R → Risk

Clause 15: TARA

Risk determination: Example

- Risk matrix

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

Threat scenario	Attack feasibility rating	Impact rating	Risk value
Spoofing of lamp request signal	High	Severe	5
DoS of oncoming car information	Low	Moderate	2

- Risk formula

- Defined a risk formula. For example:

  R = 1 + I x F

- Requires translation to numerical values

- Considering the spoofing lamp request example:
  F, High = 2 and
  I, Severe = 2,
  therefore R= 5

Impact rating	Numerical value
Negligible	0
Moderate	1
Major	1,5
Severe	2

Attack feasibility rating	Numerical value
Very low	0
Low	1
Medium	1,5
High	2

Example (Case study)

Clause 15: TARA

DEKRA DIGITAL

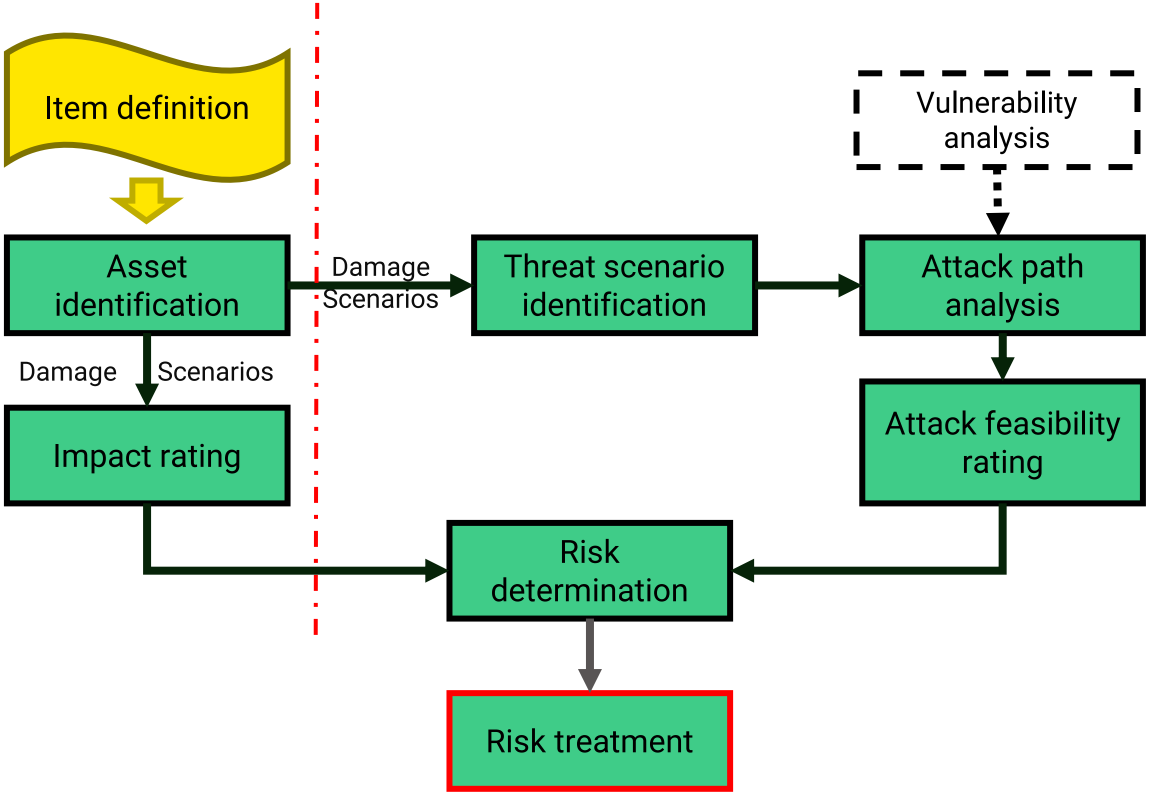
Risk Determination

Threat scenario	Attack feasibility level	Aggregated attack feasibility	Impact severity				Risk			
			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	Low	Negligible	Negligible	Negligible	Moderate	1	1	1	2
The camera input is spoofed by the attacker and the camera sends wrong data	High	High	Severe	Moderate	Major	Negligible	5	3	4	1
The camera is tampered by the attacker and the camera sends wrong data	High	High	Severe	Moderate	Major	Negligible	5	3	4	1
The communication of camera data is severed by the attacker such that the road lane data is not usable	High	High	Severe	Moderate	Major	Negligible	5	3	4	1
	Very low	High	Severe	Moderate	Major	Negligible	5	3	4	1
The speed sensor data is tampered which in turn sends incorrect speed data	Medium	Medium	Severe	Moderate	Major	Negligible	4	2	3	1
The communication of vehicle speed data is severed by the attacker such that the speed data is not usable	High	High	Severe	Moderate	Major	Negligible	5	3	4	1
	Medium	High	Severe	Moderate	Major	Negligible	5	3	4	1
The lane centering system is corrupted via malicious codes which sends incorrect driving commands	Low	Low	Severe	Moderate	Major	Negligible	3	2	2	1
The driving commands are made useless due to loss of communication.	Low	Low	Severe	Moderate	Major	Negligible	3	2	2	1
The pitch and yaw sensors are tampered by an attacker and the sensors send incorrect signals	Medium	High	Severe	Moderate	Major	Negligible	5	3	4	1
The communication of pitch and yaw sensors are tampered	High	High	Severe	Moderate	Major	Negligible	5	3	4	1
The driver inputs and notifications are tampered using some malicious program	Low	Low	Severe	Moderate	Major	Negligible	3	2	2	1
The turn on or off signals is disrupted using malicious software	Low	Low	Negligible	Negligible	Major	Negligible	1	1	2	1
The lane centering system is corrupted via malicious codes hence the notifications are blocked	Low	Low	Moderate	Moderate	Moderate	Negligible	2	2	2	1

Risk Treatment

Clause 15: TARA

Risk treatment



Clause 15: TARA

Risk treatment

Based on the risk value obtained, apply one or more risk treatment options :

- **Risk avoidance :** Deciding to avoid the risk by not implementing a functionality or not using the risk source (ex : decide not to use remote diagnostics). In this case, the **concept phase should be re-iterated** to adapt to the removal of the risk source.

- **Risk reduction :** Reducing the risk by establishing **CS goals** in order lower the risk value to an acceptable level (reducing impact or feasibility). (Annex 5 of R155 should be a basis for mitigations)

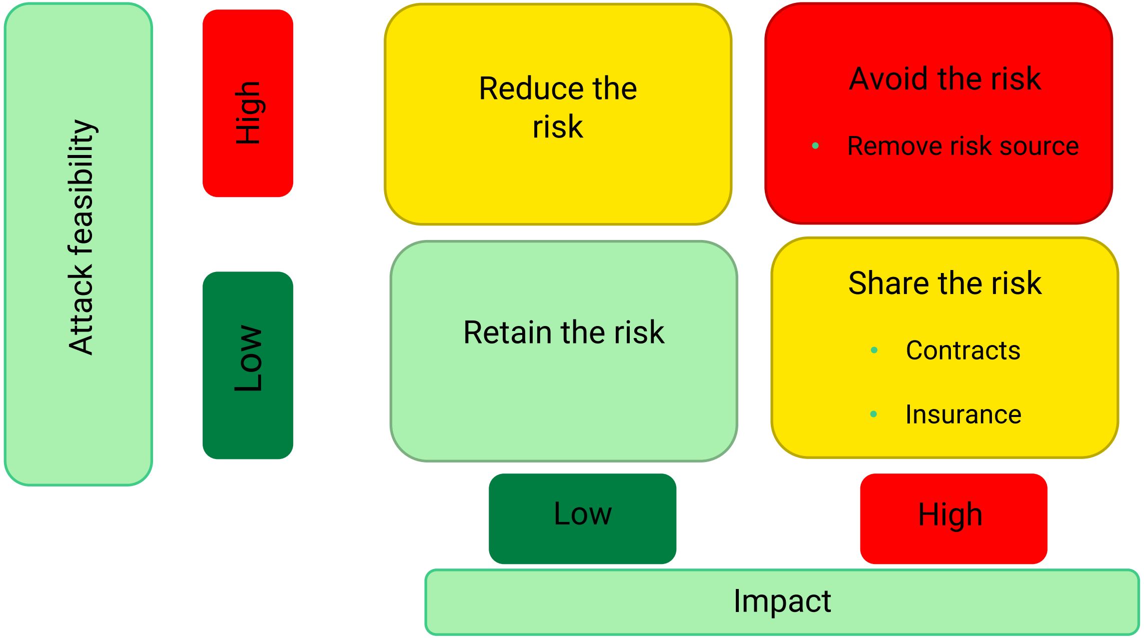
- **Risk sharing / transferring** : Lowering the impact to lower the risk by transferring or sharing the risk with another party (ex : insurance, supplier). In this case, a **CS claim** has to be established with the rationale explaining why the risk can be shared/transferred.

- **Risk acceptance :** Risk is considered low enough and is accepted as it is. A **CS claim** containing the rationale has to be established.

Clause 15: TARA

Risk Treatment

- Below find some very basic guidance on what could be preferred risk treatment options depending on the attack feasibility and impact level. **This is only a guide but every single case must be individually analysed and justified**



Note: Provide rationale (CS claims) in case of retaining and sharing the risk

Example (Case study)

Clause 15: TARA

DEKRA DIGITAL

Risk Treatment

Threat scenario:

The confidentiality of camera data is compromised and the private details such as the location or private property of the vehicle user are revealed

Impact rating: Privacy: **Moderate**, other categories: Negligible

Attack feasibility: Low

Risk rating: 2 (based on the risk matrix given in this presentation)

Risk treatment:

- Since the privacy risk is medium and no personal data is leaked, and the attack feasibility is low, the risk can be retained or shared with the users (the vehicle user)

Clause 15: TARA

Risk Treatment

Threat scenario:

The integrity of vehicle speed data is compromised, and the system doesn't work as indented because of incorrect driving commands

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

Attack feasibility: **medium**

Risk rating: 4 (based on the risk matrix given in this presentation)

Risk treatment: Since there is a high safety risk, the risk must be mitigated till the residual risk is acceptable

Clause 15: TARA

Risk Treatment

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	Severe	Moderate	Major	Negligible	5	3	4	1	Reduction
	High	Severe	Moderate	Major	Negligible	5	3	4	1	
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	Severe	Moderate	Major	Negligible	5	3	4	1	Reduction
	High	Severe	Moderate	Major	Negligible	5	3	4	1	
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 15: TARA

Work Products

TARA Methods	Work Products
Asset identification	• [WP-05-01] Damage scenarios • [WP-05-02] Assets with CS properties
Threat scenario identification	• [WP-05-03] Threat scenarios
Impact rating	• [WP-05-04] Impact ratings with associated impact categories
Attack path analysis	• [WP-05-05] Attack paths
Attack feasibility rating	• [WP-05-06] Attack feasibility ratings
Risk value determination	• [WP-05-07] Risk values
Risk treatment decision	• [WP-05-08] Risk treatment decisions

Clause 15: TARA

Summary

- **Asset identification**
  - Enumerates the assets of the item
  - Describes CS properties compromised of the assets, and their damage scenarios
- **Impact rating**
  - Evaluates damage scenarios according to the consequences that may have for the road user (functional safety, financial, operational and privacy)
- **Threat scenario identification**
  - Analyzes the assets again and determines what threat scenarios may arise
- **Attack path analysis**
  - Determines paths of a potential attacker
- **Attack feasibility rating**
  - Evaluates effort required to perform a potential attack (elapsed time, specialist of expertise, knowledge of item, etc)
- **Risk value determination**
  - Determines risk of an attack, depends on the impact of the damage scenario and the attack feasibilty of the attack paths
- **Risk treatment decision**
  - Determines an option for dealing with the risk (avoid, reduce, retain or share the risk)

DEKRA DIGITAL

Thank you for your attention