ISO/SAE 21434-BASED AUTOMOTIVE RISKS ASSESSMENT REVISITED

AMIRA BARKI AND JEAN-BAPTISTE MANGÉ

ESCAR USA
MAY 21st, 2025

ISO/SAE 21434: Road vehicles – Cybersecurity engineering

- Published in August 2021, and widely used by automotive stakeholders
- Covers several cybersecurity topics, including **Threat Analysis and Risk Assessment (TARA)**

ISO/SAE 21434: TARA Limitations

- Some definitions are quite ambiguous, leaving too much room for interpretations (e.g., *High/Low/Very Low availability).*

It may lead to **different risk levels assessment for a same attack path.**

Problem 1 **:** Unclear attack feasibility criteria definitions

- Attack paths are defined irrespective of whether there is any attacker motivated to carry out such attack.

It may lead to the **identification of unrealistic attack paths during TARAs** (e.g., an attacker triggering a braking through the injection of brake commands coming from a laptop connected on the vehicle network).

Problem 2 **:** Lack of framework enabling to prioritize the attack paths to be studied

- Some attacks, that are quite easy to achieve but barely interest few attackers, can be are overrated compared to more difficult attacks that highly interest several attackers.

Problem 3 **:** Inability to distinguish those attacks through their associated Risk Levels

Risks Assessment Objectives

Risks assessment enable to determine a **Risk Level** for a given attack path and damage scenario combination.

based on

Source : ISO 21434

Risk Level	Feasibility			
Impact	**Very Low**	**Low**	**Medium**	**High**
Severe	2	3	4	
Major	1	2	3	
Moderate	1	2	2	
Negligible	1	1	1	2

Damage Scenario **Impact**

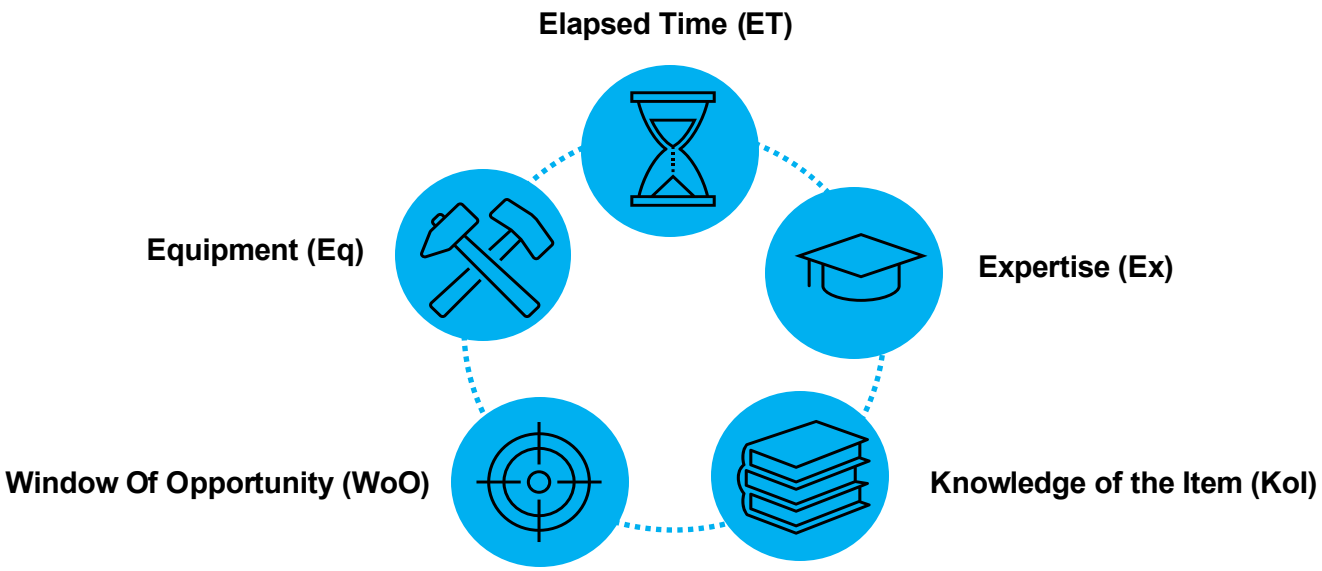
attack path **Feasibility**

Risk treatment option

- **Accept**
- **Reduce**
- **Avoid**
- **Transfer**

Feasibility rating

The most commonly used approach is **attack potential-based approach:**

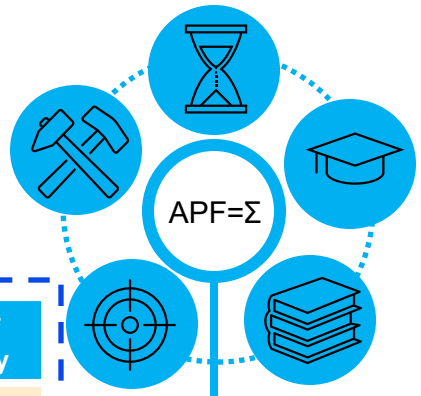


Attack potential-based feasibility rating

Elapsed Time	
Enumerate	Value
≤ 1 day	0
≤ 1 week	1
≤ 1 month	4
≤ 3 months	10
≤ 6 months	17
> 6 months	19

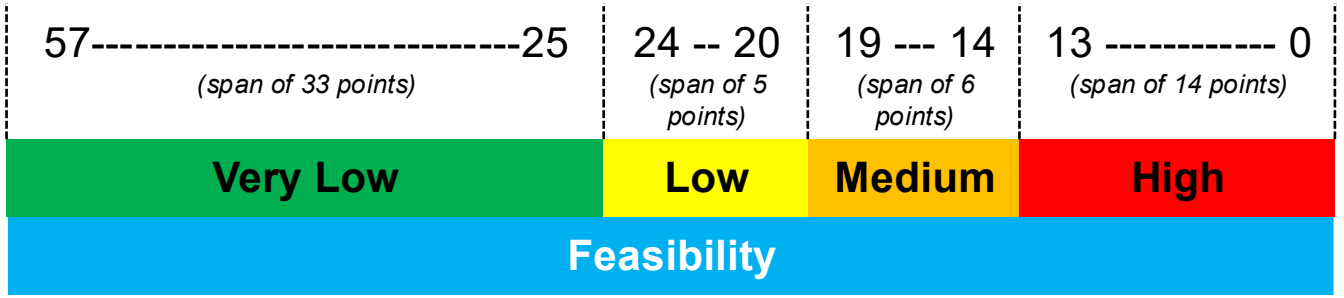
Equipment	
Enumerate	Value
Standard	0
Specialized	4
Bespoke	7
Multiple bespoke	9

Expertise	
Enumerate	Value
Layman	0
Proficient	3
Expert	6
Multiple Expert	8



Window of Opportunity	
Enumerate	Value
Unlimited	0
Easy	1
Moderate	4
Difficult/None	10

Knowledge Of the Item	
Enumerate	Value
Public	0
Restricted	3
Confidential	7
Strictly Confidential	11



Problem 1 : Unclear attack feasibility criteria definitions

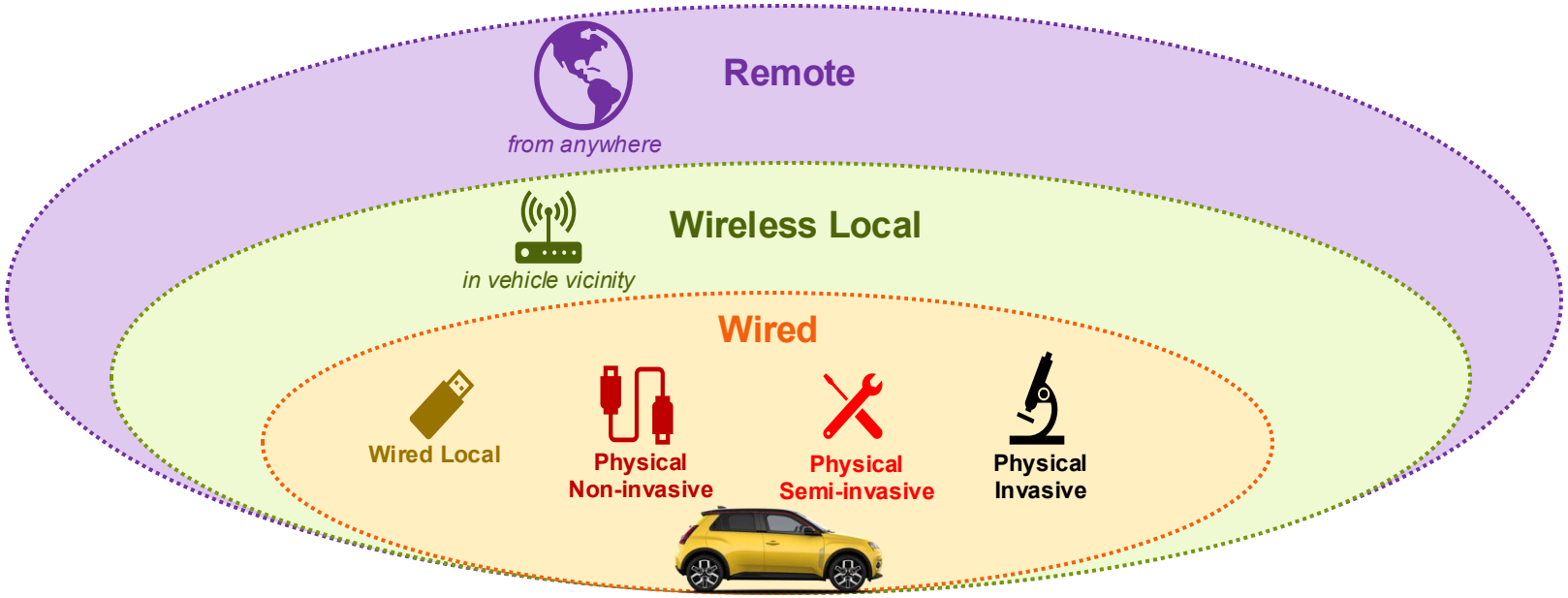
Source : ISO 21434

Risk Level	Feasibility			
Impact	Very Low	Low	Medium	High
Severe	2	3	4	5
Major	1	2	3	4
Moderate	1	2	2	3
Negligible	1	1	1	2

Window of Opportunity rating improvement

Computed based on the following 3 parameters:

- **Modus operandi**: access type and method required to carry out the attack
- Asset exposure
- Attacker's access privileges



Window of Opportunity rating improvement

Computed based on the following 3 parameters:

- Modus operandi
- **Asset exposure**: time window during which the targeted asset is exposed
- Attacker's access privileges

Always/frequently exposed

Sporadically exposed

Rarely exposed

Insufficiently exposed

Window of Opportunity rating improvement

Computed based on the following 3 parameters:

- Modus operandi
- Asset exposure
- **Attacker's access privileges**: whether the attacker has legitimate access to the targeted vehicle, or not

Authorized access

Unauthorized access

Window of Opportunity rating improvement

WoO determination:

Source : Internal

Modus operandi \ Asset exposure	Authorized access: Always / frequently exposed asset	Authorized access: Sporadically exposed asset	Authorized access: Rarely exposed asset	Authorized access: Insufficiently exposed asset	Unauthorized access: Always / frequently exposed asset	Unauthorized access: Sporadically exposed asset	Unauthorized access: Rarely exposed asset	Unauthorized access: Insufficiently exposed asset
Remote	Unlimited			None	Unlimited	Easy	Moderate	None
Wireless local					Easy	Moderate	Very Difficult	
Wired local					Moderate	Difficult		
Non-invasive physical					Moderate			
Semi-invasive physical	Easy				Difficult			
Invasive physical					Very Difficult			

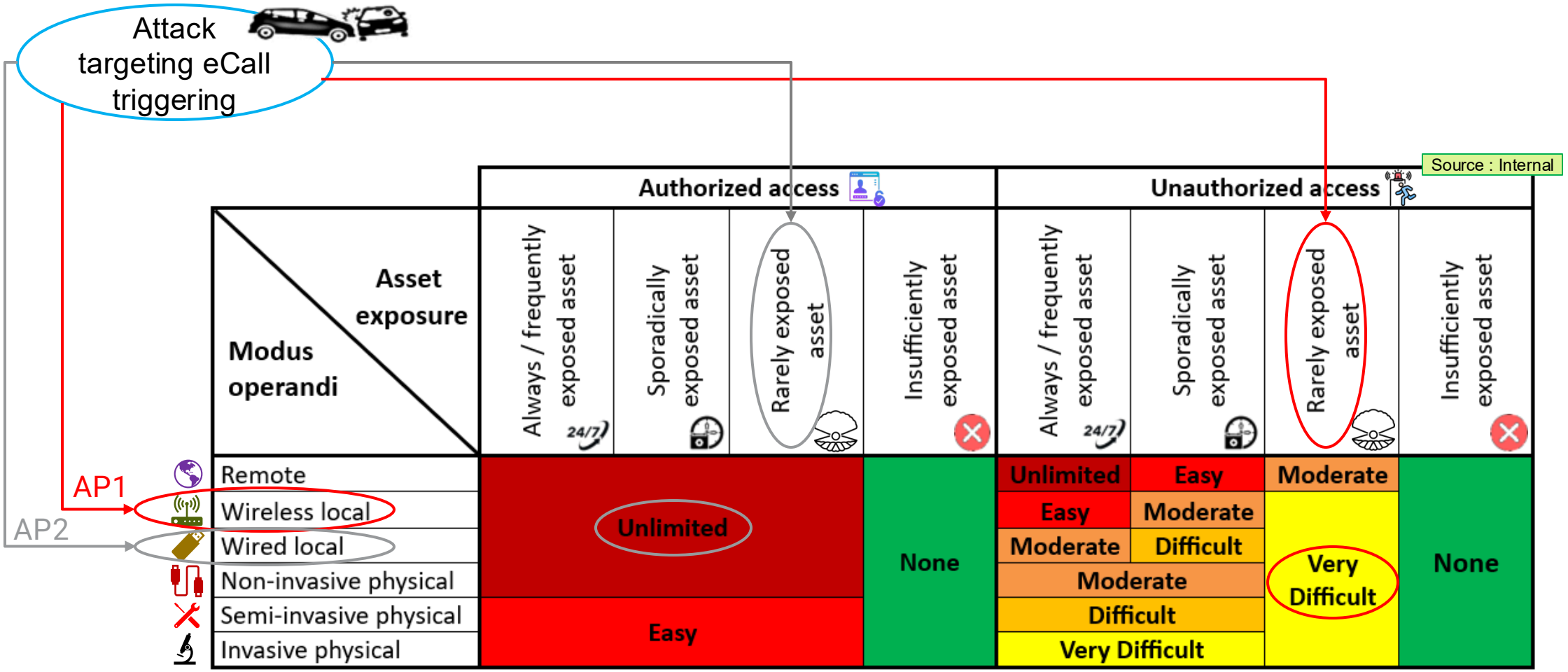
Window of Opportunity rating improvement – examples

CAN injection attack

Source : Internal

Modus operandi \ Asset exposure	Authorized access: Always / frequently exposed asset	Authorized access: Sporadically exposed asset	Authorized access: Rarely exposed asset	Authorized access: Insufficiently exposed asset	Unauthorized access: Always / frequently exposed asset	Unauthorized access: Sporadically exposed asset	Unauthorized access: Rarely exposed asset	Unauthorized access: Insufficiently exposed asset
Remote	Unlimited			None	Unlimited	Easy	Moderate	None
Wireless local					Easy	Moderate	Very Difficult	
Wired local					Moderate	Difficult		
Non-invasive physical					Moderate			
Semi-invasive physical	Easy				Difficult			
Invasive physical					Very Difficult			

Window of Opportunity rating improvement – examples



Window of Opportunity rating improvement

Source : ISO 21434

ISO/SAE 21434 Window of Opportunity rating scale	
Level	Value
Unlimited	0
Easy	1
Moderate	4
Difficult/None	10

Source : Internal

Our proposed Window of Opportunity rating scale	
Level	Value
Unlimited	0
Easy	2 UPDATED
Moderate	4
Difficult	10
Very difficult NEW	16
None	25 UPDATED

Problem 1 : Unclear attack feasibility criteria definitions

Automotive Threat Agents

Legitimate user

Insider

Dishonest repairer

Hacktivist

Thief

Organized Crime

Competitor

Researcher

State

Cyber Terrorist

Threat Agents Capabilities

Capability

The Capability of a threat agent reflects the attacker's ability to carry out a sophisticated attack.

It is **always the same** for a given threat agent **regardless of the system or feature under study**.

Source : Internal

Threat Agent Resources	Description
Very limited	The threat agent has very little resources
Modest	The threat agent has limited resources
Significant	The threat agent is well resourced
Almost unlimited	The threat agent is extremely well resourced

X

Source : Internal

Threat Agent Expertise	Description
Layman	The threat agent has no particular expertise or specific technical knowledge. He needs a detailed description of the different steps of a known easy attack to be able to reproduce it.
Proficient	The threat agent have a minimal level of knowledge and are quite familiar with typical attack techniques.
Expert	The threat agent is skilled enough to identify 0-day vulnerabilities and mount new attacks.
Multipe Expert	The threat agent has expertise in different fields related to automotive technologies and is able to mount quite complex new attacks.

Source : Internal

Capability level	Threat Agent Resources			
Threat Agent Expertise	Very Limited	Modest	Significant	Almost unlimited
Layman	**Very Little**	*Very Little*	*Little*	*Limited*
Proficient	**Little**	**Little**	*Limited*	*Significant*
Expert	*Little*	**Limited**	*Significant*	*Significant*
Multiple Expert	*Limited*	**Limited**	**Significant**	**Formidable**

Capability of Automotive Threat Agents

<Level> Resources and Expertise cross reference defined for a know Threat Agent

<Level> Pre-defined Resources and Expertise cross reference

AMPERE

Source : Internal

Capability level	Threat Agent Resources			
Threat Agent Expertise	**Very Limited**	**Modest**	**Significant**	**Almost unlimited**
Layman	**Very Little**  **Legitimate user**	*Very Little*	*Little*	*Limited*
Proficient	**Little**  **Insider**	**Little**  **Thief**  **Dishonest repairer**	*Limited*	*Significant*
Expert	*Little*	**Limited**  **Hacktivist**	*Significant*	*Significant*
Multiple Expert	*Limited*	**Limited**  **Researcher**	**Significant**  **Organized Crime**  **Competitor**  **Cyber Terrorist**	**Formidable**  **State**

Threat Level determination based on TVRA

Once the capability per Threat Agent defined, we can rely on TVRA methodology where a Threat Level is defined by combining the capability and the motivation levels

Source : Internal

Capability level	Threat Agent Resources			
Threat Agent Expertise	Very Limited	Modest	Significant	Almost unlimited
Layman	Very Little	*Very Little*	*Little*	*Limited*
Proficient	Little	Little	*Limited*	*Significant*
Expert	*Little*	Limited	*Significant*	*Significant*
Multiple Expert	*Limited*	Limited	Significant	Formidable

Source : TVRA

Motivation Level	Description
Indifferent (Very Low)	The system is considered to have limited to no value to the threat agent, thus the threat agent is very unlikely to attempt any attack on the system.
Curious (Low)	The system is considered to have minimal value to the threat agent. Threat agents may attempt to attack the system out of curiosity or opportunistic motivation. Non system deterrents may be sufficient to deter the threat agent from initiating the attack.
Interested (Medium)	The system is considered to have moderate value to the threat agent. The threat agent will attempt to attack the system on a frequent basis. It is also considered unlikely that the threat agent can be deterred from initiating the attack by the existence of non-system deterrents.
Committed (High)	The system is considered to have significant value to the threat agent. The threat agent will attempt to attack the system on a persistent and frequent basis. It is considered highly unlikely that the threat agent can be deterred from initiating the attack by the existence of non-system deterrents.
Focused (Very High)	Threat agent has a primary aim to attack the system.

Source : TVRA inspired

Threat level	Capability level				
Motivation levels	Very little	Little	Limited	Significant	Formidable
Indifferent (Very Low)	Negligible	Negligible	Low	Low	Low
Curious (Low)	Negligible	Negligible	Low	Low	Moderate
Interested (Medium)	Low*	Low	Moderate	Severe	Severe
Committed (High)	Low	Low	Moderate	Severe	Critical
Focused (Very High)	Low	Moderate	Severe	Critical	Critical

*Threat level modification from Negligible [TVRA] to Low [Internal]

What is the added value associated with the Threat Level?

Purpose of these preliminary tasks is to define the **Threat Level** ***per Threat Agent per Modus Operandi per Feared Event.***

This way we can filter out unrealistic attack paths and focus on most relevant ones.

What is the added value associated with the Threat Level?

Purpose of these preliminary tasks is to define the **Threat Level** ***per Threat Agent per Modus Operandi per Feared Event.***

This way we can filter out unrealistic attack paths and focus on most relevant ones.







Threat Level *per Threat Agent per Modus Operandi*		Threat Agent →	Legitimate user		Dishonest repairer		Hacktivist		Researcher		Organized Crim					
		Threat Agent Capability →	Very little		Little		Limited		Limited		Significant					
ID	Damage Scenario	Modus operandi	Motivation	Threat Level	Motivation	Threat Level	Motivation	Threat Level	Motivation	Threat Level	Motivation	Threat Le				
DS#1	Accid	Physical Invasive	Indifferent	Negligible	Indifferent	Negligible	Indifferent	Negligible	Curious	Low	Indifferent	Low			Interested	Critical
		Physical Semi-invasive	Indifferent	Negligible	Indifferent	Negligible	Indifferent	Negligible	Curious	Low	Indifferent	Low			Committed	Critical
		Physical Non-invasive	Indifferent	Negligible	Indifferent	Negligible	Indifferent	Negligible	Curious	Low	Curious	Low			Focused	Critical
DS#2	Illega to the **residual value** of the vehicle (mileage, fault lights, battery health, etc.)	Wired Local	Committed	Low	Committed	Low	Curious	Low	Curious	Low	Committed	Severe	Indifferent	Low	Indifferent	Low
		Wireless Local	Committed	Low	Committed	Low	Curious	Low	Curious	Low	Committed	Severe	Indifferent	Low	Indifferent	Low
		Remote	Indifferent	Negligible	Indifferent	Negligible	Curious	Low	Curious	Low	Committed	Severe	Indifferent	Low	Indifferent	Low

Problem 2 : Lack of framework enabling to prioritize the attack paths to be studied.

If the motivation is "**Indifferent**" or the Threat Level is "**Negligible**" → Related attack paths can be considered as irrelevant

Risk levels determination according to the Threat Level

Source : ISO 21434

Risk Level	Feasibility			
Impact	Very Low	Low	Medium	High
Severe	2	3	4	5
Major	1	2	3	4
Moderate	1	2	2	3
Negligible	1	1	1	2

With proposed approach, the resulting risk level associated to the relevant attack paths vary according to the Threat Level.

This enables to adequately reflect the risk raised by a given Threat Agent for a given Feared Event.

Source : Internal

Risk Level	Threat Level															
	Low (NEW)				Moderate (default)				Severe (NEW)				Critical (NEW)			
	Feasibility				Feasibility				Feasibility				Feasibility			
Impact	Very Low	Low	Medium	High	Very Low	Low	Medium	High	Very Low	Low	Medium	High	Very Low	Low	Medium	High
Severe	1	2	3	4	2	3	4	5	2	3	4	5	3	4	5	5
Major	1	2	2	3	1	2	3	4	2	3	4	4	2	3	4	5
Moderate	1	1	2	2	1	2	2	3	1	2	3	3	1	2	3	4
Negligible	1	1	1	1	1	1	1	2	1	1	2	2	1	1	2	3

Risk Levels with Threat Level consideration

Let's run some examples …

Dishonest repairer

A Dishonest repairer would like to tamper with Braking system, which has a **Severe** impact on **Safety**, and has found an attack path with **Medium** feasibility that relies on **Non-invasive physical** modus operandi.

→ "***Indifferent***" Motivation, so this attack path is considered as not relevant

Organized Crime

Organized Crime would like to reduce the total mileage, which has a **Major Financial** impact, and has found an attack path with **Medium** feasibility that relies on **Non-invasive physical** modus operandi.

↓ "***Severe***" Threat Level

Risk Level	Feasibility			
Impact	Very Low	Low	Medium	High
Severe	2	3	~~4~~	5
Major	1	2	3	4
Moderate	1	2	2	3
Negligible	1	1	1	2

Risk Level without Threat Level consideration

Source : Internal

	Threat Level															
Risk Level	Low				Moderate (default)				Severe				Critical			
	Feasibility				Feasibility				Feasibility				Feasibility			
Impact	Very Low	Low	Medium	High	Very Low	Low	Medium	High	Very Low	Low	Medium	High	Very Low	Low	Medium	High
Severe	1	2	3	4	2	3	4	5	2	3	4	5	3	4	5	5
Major	1	2	2	3	1	2	3	4	2	3	4	~~4~~	~~2~~	~~3~~	~~4~~	~~5~~
Moderate	1	1	2	2	1	2	2	3	1	2	3	3	1	2	3	4
Negligible	1	1	1	1	1	1	1	2	1	1	2	2	1	1	2	3

Risk Levels with Threat Level consideration

Let's run some examples …

Researcher

A Researcher would like to tamper with Braking system which has a **Severe** impact on **Safety**. He has found an attack path with **Medium** feasibility that relies on **Physical Non-invasive** modus operandi.

→ "***Low***" Threat Level

Organized Crime

Organized Crime would like to do the same but with a **Remote** modus operandi and has found an attack path with **Low** feasibility.

↓ "***Critical***" Threat Level

Risk Level	Feasibility			
Impact	Very Low	Low	Medium	High
Severe	2	3	4	5
Major	1	2	3	4
Moderate	1	2	2	3
Negligible	1	1	1	2

Risk Level without Threat Level consideration

Source : Internal

	Threat Level															
Risk Level	Low				Moderate (default)				Severe				Critical			
	Feasibility				Feasibility				Feasibility				Feasibility			
Impact	Very Low	Low	Medium	High	Very Low	Low	Medium	High	Very Low	Low	Medium	High	Very Low	Low	Medium	High
Severe	1	2	3	4	2	3	4	5	2	3	4	5	3	4	5	5
Major	1	2	2	3	1	2	3	4	2	3	4	4	2	3	4	5
Moderate	1	1	2	2	1	2	2	3	1	2	3	3	1	2	3	4
Negligible	1	1	1	1	1	1	1	2	1	1	2	2	1	1	2	3

Risk Levels with Threat Level consideration

Let's run some examples …

Researcher

A Researcher would like to tamper with Braking system which has a **Severe** impact on **Safety**. He has found an attack path with **Medium** feasibility that relies on **Physical Non-invasive** modus operandi.

→ "***Low***" Threat Level

Organized Crime

Organized Crime would like to do the same but with a **Remote** modus operandi and has found an attack path with **Low** feasibility.

↓ "***Critical***" Threat Level

Risk Level	Feasibility			
Impact	Very Low	Low	Medium	High
Severe	2	3	4	5
Major	1	2	3	4
Moderate	1			
Negligible	1			

Risk L
Threat Lev

Risk Level	Threat Level			
	Low	Moderate (default)	Severe	Critical

Problem 3 : Inability to distinguish those attacks through their associated Risk Levels

Moderate	1	1	2	2	1	2	2	3	1	2	3	3	1	2	3	4
Negligible	1	1	1	1	1	1	1	2	1	1	2	2	1	1	2	3

Risk Levels with Threat Level consideration

What about the link with real attacks?

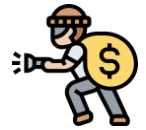
AMPERE

Public information used for Threat Intelligence :

Thieves used Non-invasive Physical modus operandi to bypass anti-theft protection and steal vehicles

We can check that real world attacks are correctly taken into account in our Threat Model and when relevant :

- Update Motivation for a relevant Modus Operandi
- Update risks assessment
- Create a new Damage Scenario and assess it



Threat Level *per Threat Agent per Modus Operandi*		**Threat Agent →**	**Thief**	
		Threat Agent Capabilities →	**Little**	
ID	**Damage Scenario**	**Modus operandi**	Motivation	**Threat Level**
DS#5	Illegal vehicle access and ignition	Physical Invasive	Indifferent	**Negligible**
		Physical Semi-invasive	Curious	**Low**
		Physical Non-invasive	Focused	**Moderate**
		Wired Local	Focused	**Moderate**
		Wireless Local	Focused	**Moderate**
		Remote	Focused	**Moderate**

We can also anticipate new attacks by setting higher motivations/Threat Level/etc. to see the impact of their modification on risk values.

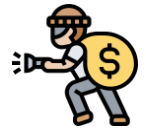
What about the link with real attacks?

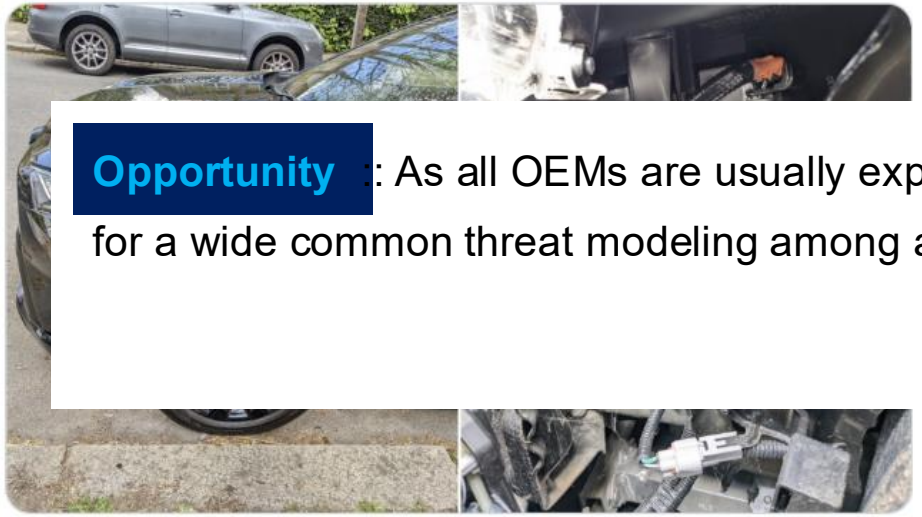
Public information used for Threat Intelligence :

Thieves used Non-invasive Physical modus operandi to bypass anti-theft protection and steal vehicles

We can check that real world attacks are correctly taken into account in our Threat Model and when relevant :

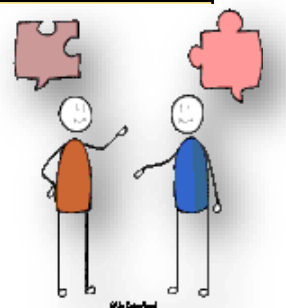
- Update Motivation for a relevant Modus Operandi
- Update risks assessment
- Create a new Damage Scenario and assess it





Threat Level		Threat Agent →	Thief
		Wired Local	Focused	Moderate
		Wireless Local	Focused	Moderate
		Remote	Focused	Moderate

Opportunity : As all OEMs are usually exposed to the same threats, all of this data could be highly shared for a wide common threat modeling among all interested OEMs, suppliers and partners.



We can also anticipate new attacks by setting higher motivations/Threat Level/etc. to see the impact of their modification on risk values.

AMPERE

Thank **you**

Contact information:
amira.barki@ampere.cars
jean-baptiste.mange@ampere.cars