AUTOMOTIVE SPIN ITALIA
21° WORKSHOP ON AUTOMOTIVE SOFTWARE & SYSTEM

CYBERSECURITY
BREMBO APPROACH TO TARA, A CASE STUDY ON STAND-ALONE EPB

Samuele Longoni

GCF R&D

01/06/23

AGENDA

01. INTRODUCTION

02. PRELIMINARY SETTINGS

03. TARA ANALYSIS

04. CONCLUSIONS

01. INTRODUCTION

WHAT IS TARA?

TARA is an engineering methodology to identify, prioritize and respond to cyber threats through the application of countermeasures that reduce the probability of a cyber attack.

T - Threat

A - Analysis

R - Risk

A - Assessment

WHAT IS TARA?

TARA is an engineering methodology to identify, prioritize and respond to cyber threats through the application of countermeasures that reduce the probability of a cyber attack.

T - Threat

A - Analysis

R - Risk

A - Assessment

GOALS

- Identify assets, their cybersecurity properties and their damage scenarios;
- Identify threat scenarios;
- Determine the impact rating of damage scenarios;
- Identify the attack paths that realize threat scenarios;
- Determine the ease with which attack paths can be exploited;
- Determine the risk values of threat scenarios;
- Select appropriate risk treatment options for threat scenarios.

REFERENCE STANDARDS

ISO/SAE 21434:

This normative specifies engineering requirements and work products for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces.

It gives “what” shall be done. Limited information on “how” it shall be done.

HEAVENS

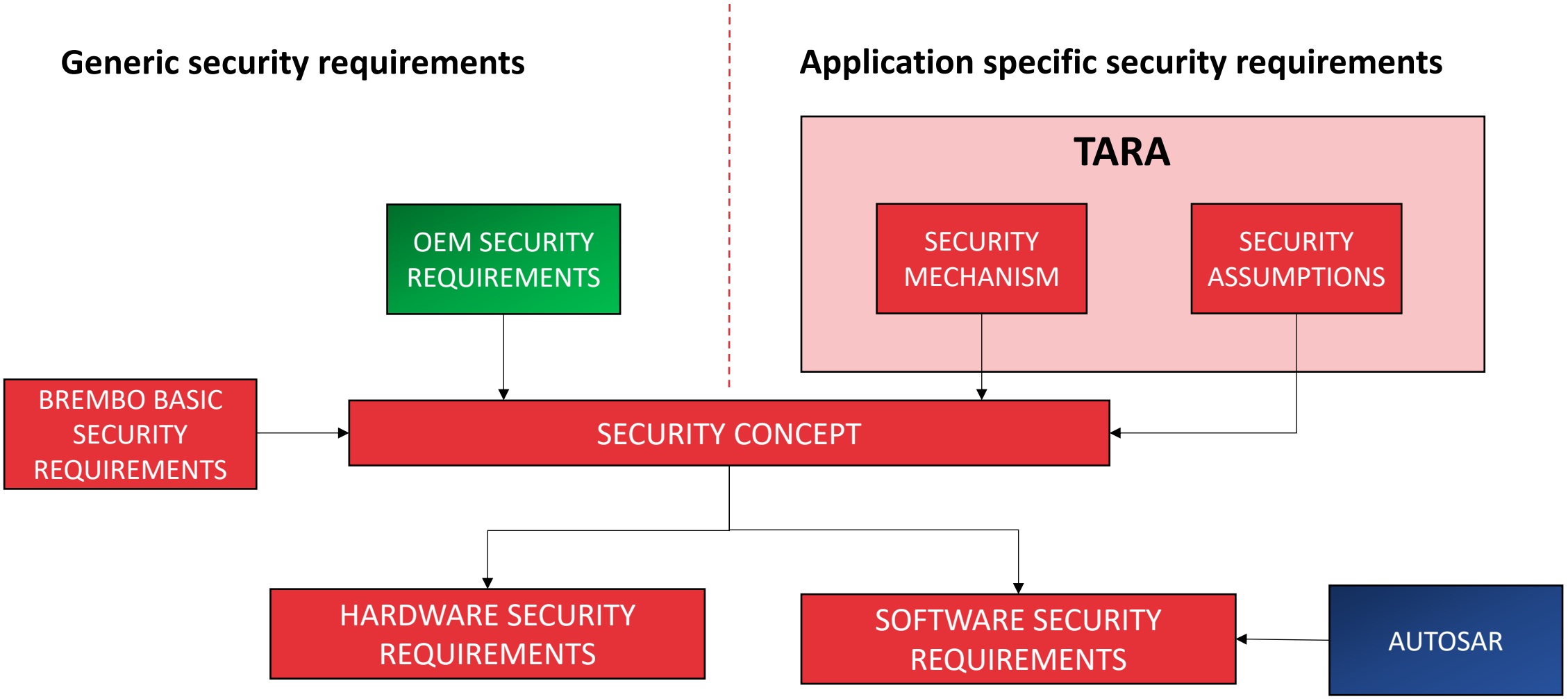
HEAling Vulnerabilities to Enhance Software Security and Safety

One of the Security Models proposed for automotive TARA, which presents a systematic approach of assessing security risks and deriving security requirements for the automotive Electrical/Electronic systems.

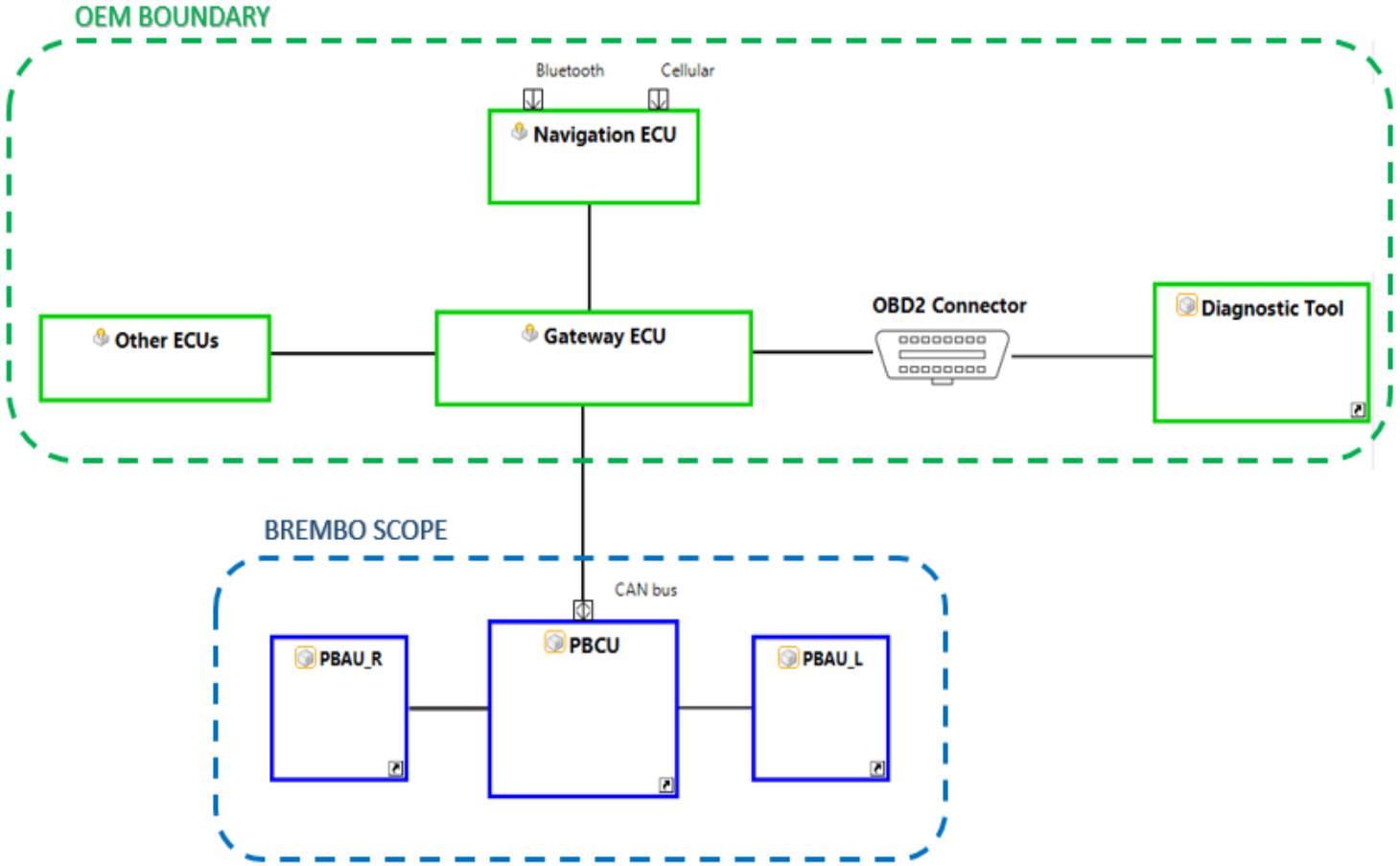
It gives more information on “how” it shall be done.

02.
PRELIMINARY SETTINGS

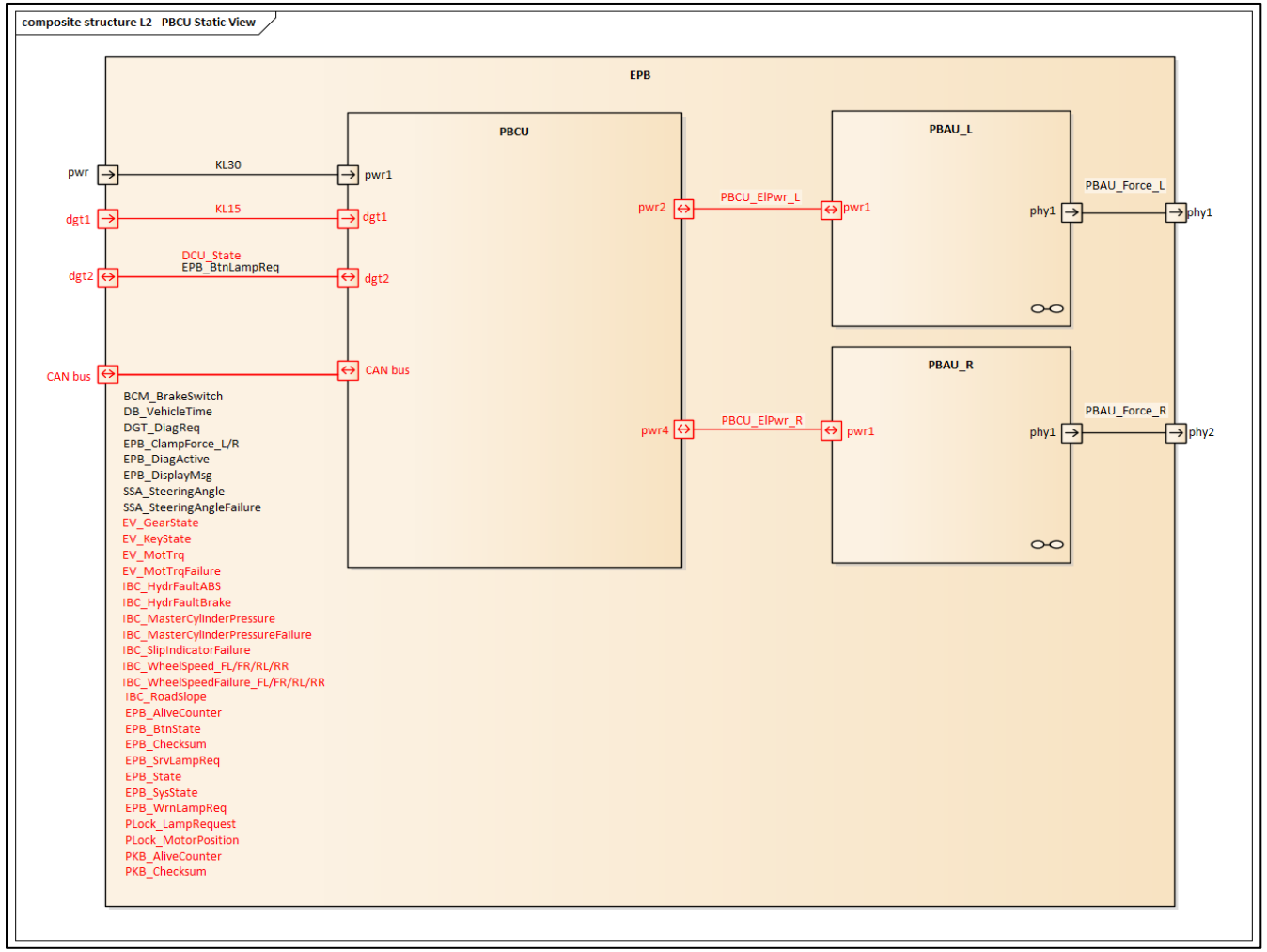
SECURITY CONCEPT DEFINITION



ANALYSIS PERIMETER



SYSTEM ARCHITECTURE



ASSUMPTIONS

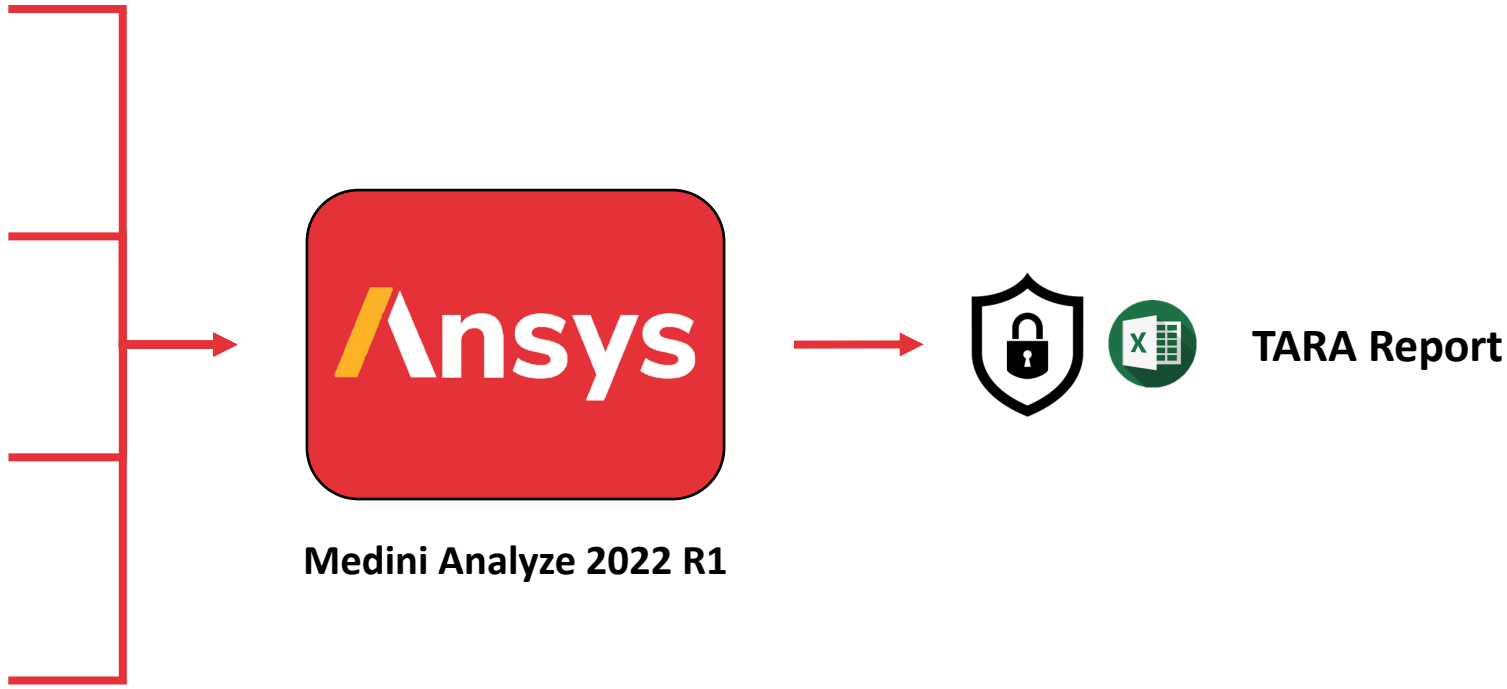
1. The OEM will be responsible of the **protection of the communication** between the nodes (external to the Brembo boundary) as well as the communication which occurs with the outside.

2. The **presence of a gateway** that filters information and avoids threats coming from the outside of the Brembo perimeter is necessary for the correct interpretation of the analysis.

3. The purpose of this analysis stops at the description and management of the threats that can occur only **within the EPB node**.

TOOL

- Security Concept Definition
- Analysis Perimeter
- System Architecture
- Assumptions



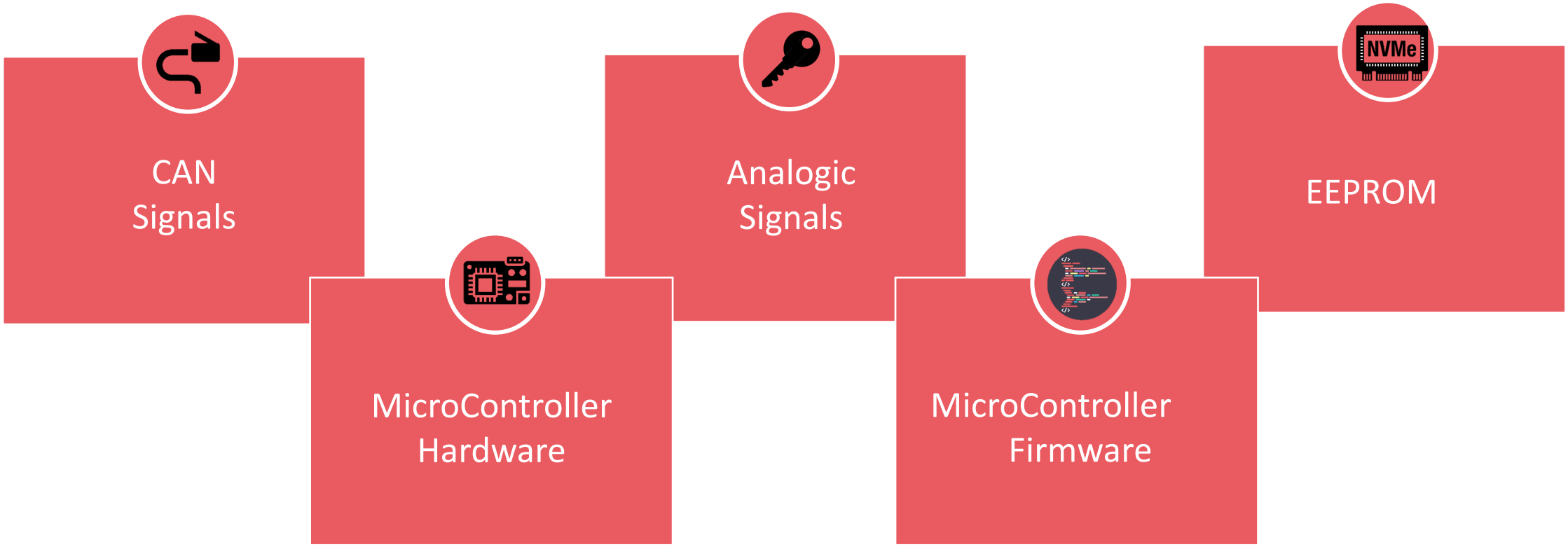
03.
TARA ANALYSIS

TARA
FLOW CHART

TARA 1/7
ASSET DEFINITION

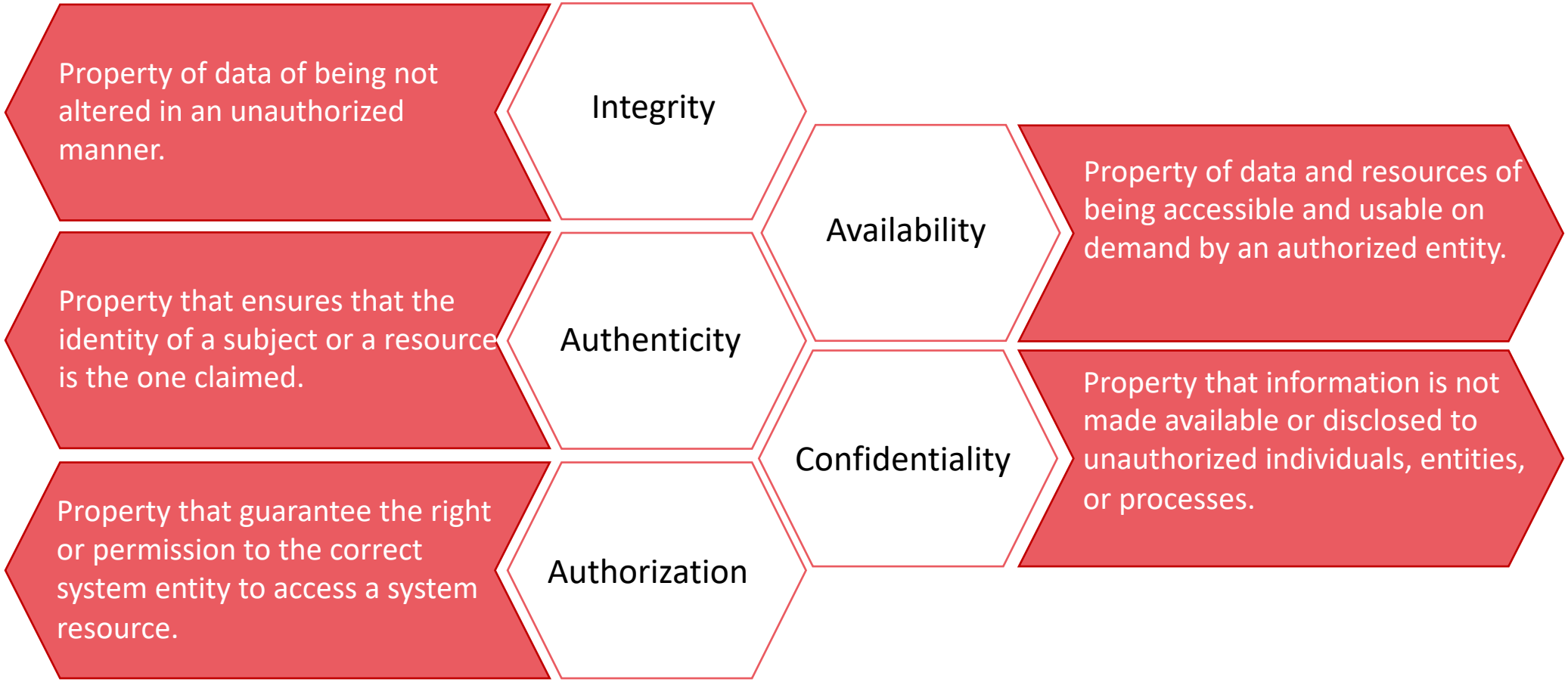
An **Asset** is an object that has value, or that contributes to the value of the System. It is a signal or a sub-system that can be subjected to threats and therefore can undermine the security and performance of the System itself.

Different kinds of assets:

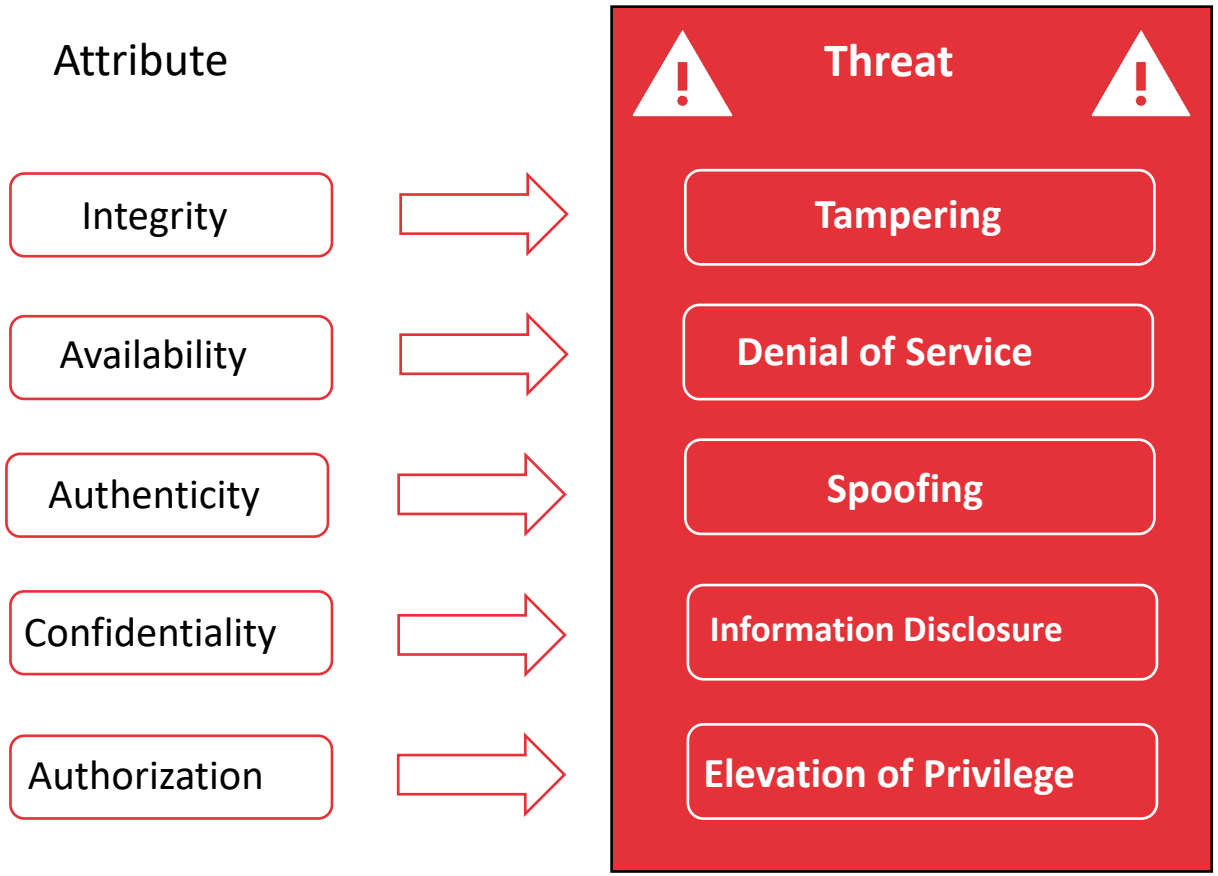


TARA 2/7
SECURITY ATTRIBUTE DEFINITION

An **Attribute** is an abstraction representing the basic properties or characteristics of an asset with respect to safeguarding information.



TARA 3/7
THREATS DEFINITION



Threat Description

- An intentional but unauthorized act resulting in the modification of a intended behavior of the system.

- Render a resource unavailable to its intended users by interrupting its normal functioning.

- Impersonating a legitimate resource or user.

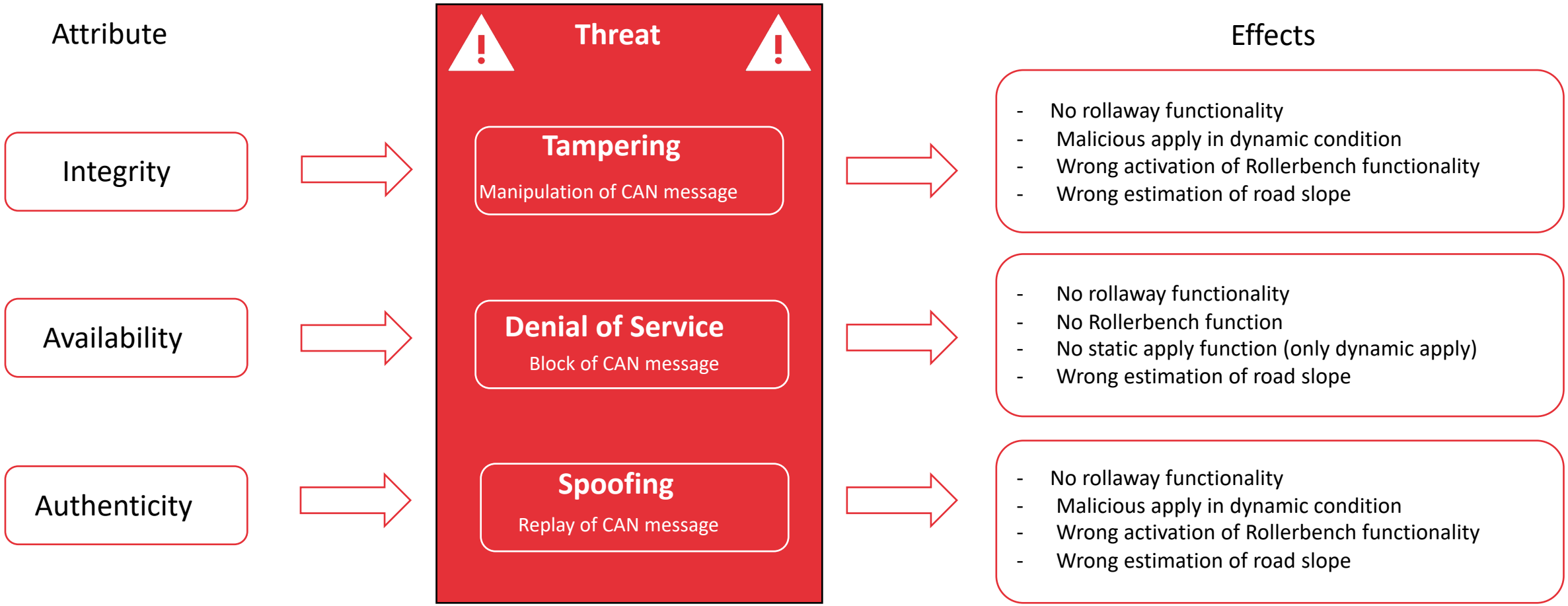
- Transfer, provision of access to or divulging in any other manner of information outside the entity holding the information.

- The process by which a user obtains a higher level of privilege than that for which he has been authorized.

Note: adopted Microsoft STRIDE model

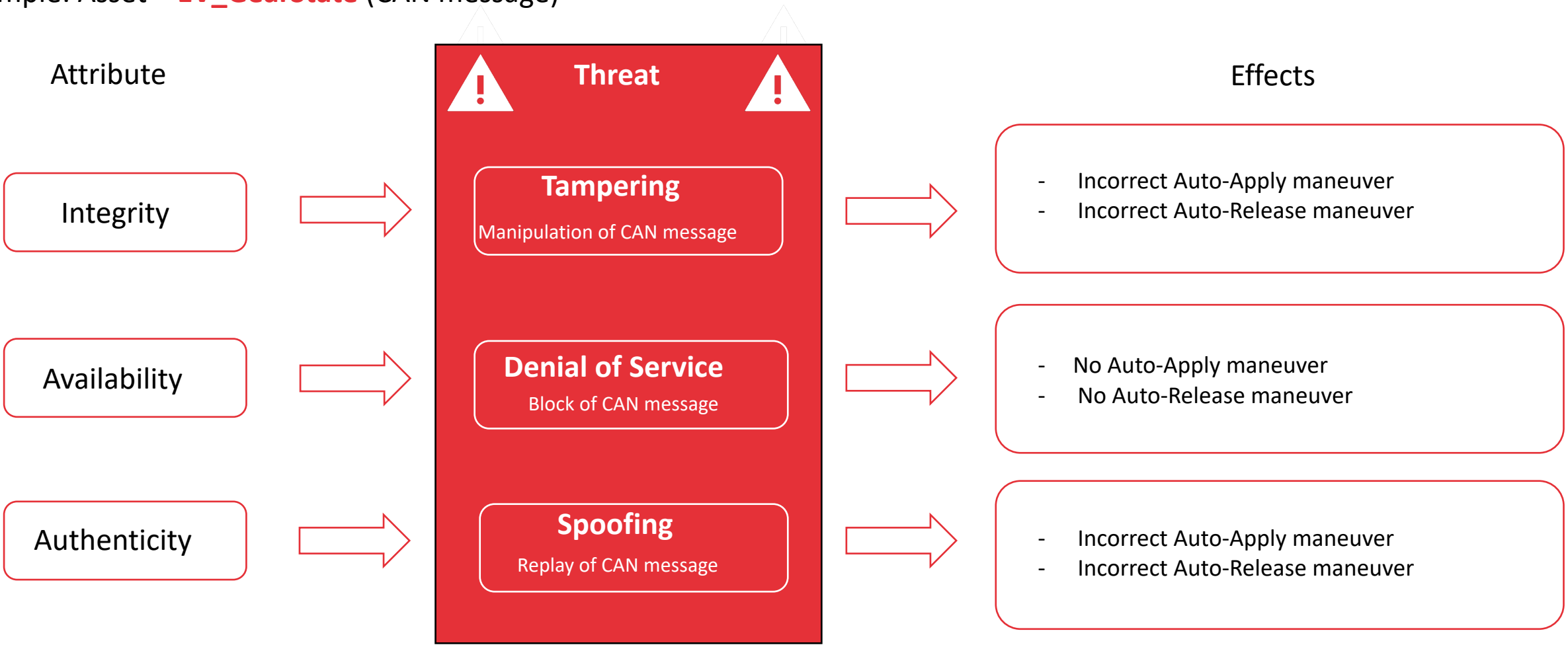
TARA 3/7
THREATS DEFINITION – EXAMPLE (1)

Example: Asset – **IBC_WheelSpeed** (CAN message)



TARA 3/7
THREATS DEFINITION – EXAMPLE (2)

Example: Asset – **EV_GearState** (CAN message)



TARA 4/7
IMPACT LEVEL DEFINITION

Safety Impact

Considers all impacts that violate the Safety Goals defined for the project.

Financial Impact

Considers all financial losses or damages that can be either direct or indirect. They may include product liability issues, legislation issues, product features.

Operational Impact

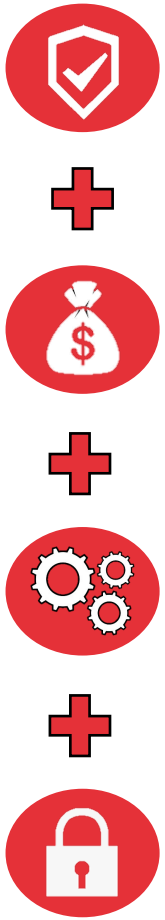
Considers operational damages caused by unwanted and unexpected incidents. They includes loss of secondary and comfort/entertainment functionalities of the vehicle.

Privacy and Legislation Impact

Considers damages caused by privacy violation of stakeholders and/or violation of legislation/regulations.

Note: adopted HEAVENS assessment method

TARA 4/7
IMPACT LEVEL DEFINITION



Sum of the values of the Impact parameters	Impact Level (or Severity Level)	Impact Level Value
0	No Impact	0
1 - 19	Low	1
20 – 99	Medium	2
100 - 999	High	3
≥ 1000	Critical	4

TARA 5/7
THREAT LEVEL DEFINITION

Equipment

It refers to the equipment required to identify or exploit vulnerability and/or mount an attack.

Window of opportunity

It combines access type (e.g. logical, physical…) and access duration (e.g. limited, unlimited…) that are required to mount an attack on the TOE by an attacker.

Knowledge about TOE

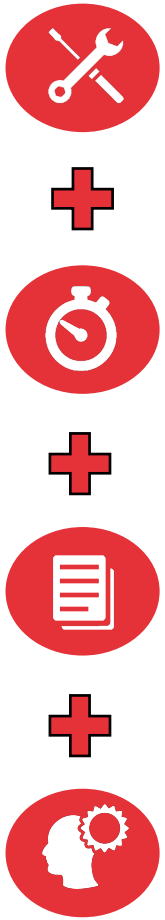
It refers to the availability of information about from an attacker perspective. This parameter points to the sources from where attackers can gain knowledge about the TOE and indicates how easy or difficult can be to acquire knowledge about the TOE.

Expertise

It refers to the level of generic knowledge of the underlying principles, product type or attack methods that are required to carry out an attack on the TOE.

Note: adopted HEAVENS assessment method

TARA 5/7
THREAT LEVEL DEFINITION



Sum of the values of the Threat parameters	Threat Level (or Likelihood Level)	Threat Level Value
> 9	None	0
7 - 9	Low	1
4 - 6	Medium	2
2 - 3	High	3
0 - 1	Critical	4

TARA 6/7
SECURITY LEVEL DEFINITION

Security Level (SL)		Impact Level (IL)				
		0	1	2	3	4
Threat Level (TL)	0	QM	QM	QM	QM	Low
	1	QM	Low	Low	Low	Medium
	2	QM	Low	Medium	Medium	High
	3	QM	Low	Medium	High	High
	4	Low	Medium	High	High	Critical

Note: adopted HEAVENS assessment method

TARA 6/7
SECURITY LEVEL DEFINITION

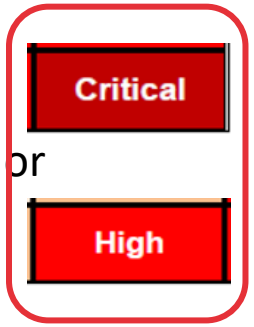
Security Level (SL)		Impact Level (IL)				
		0	1	2	3	4
Threat Level (TL)	0	QM	QM	QM	QM	Low
	1	QM	Low	Low	Low	Medium
	2	QM	Low	Medium	Medium	High
	3	QM	Low	Medium	High	High
	4	Low	Medium	High	High	Critical

OK – No Countermeasure needed

NOK – Need to define Countermeasures or Mitigations

TARA 7/7
SECURITY GOALS, MEASURES AND REQUIREMENTS DEFINITION

For Security Level equal to



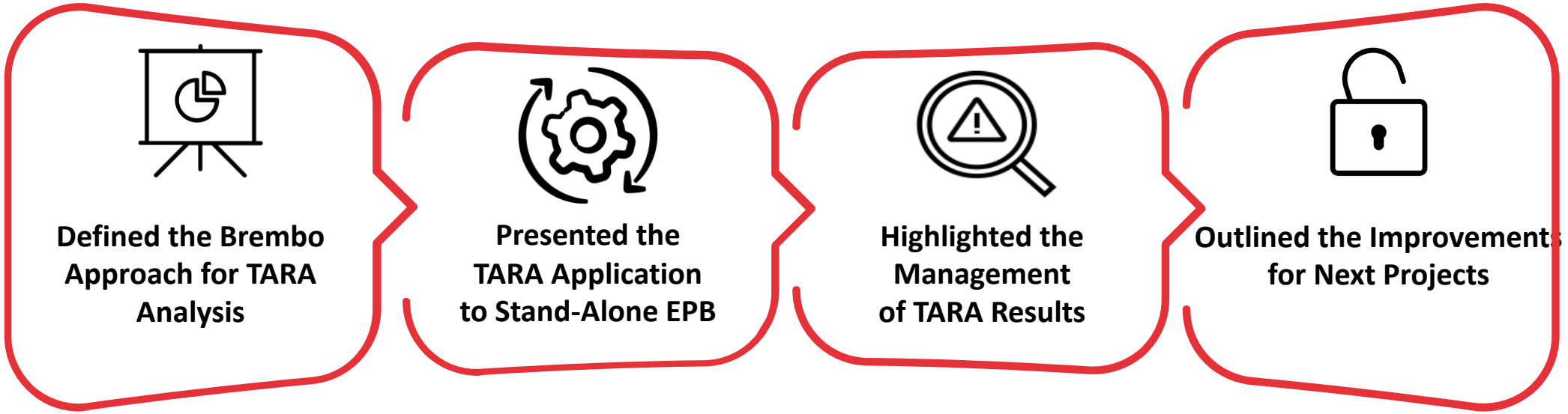
Mitigation is needed → Definition of **Security Goals**

ID	Security Goal
CG001	Protect CAN communication security relevant signals against spoofing, tampering and flooding threats.
…	…

Definition of **Security Goals** → Definition of **Security Measures** → Definition of **Security Requirements**

04.
CONCLUSIONS

CONCLUSIONS



THANK YOU