THREATGET A TOOL FOR PRACTICAL CYBERSECURITY ANALYSIS AND ASSESSMENT

FUSACOM 25. Get-2-Gether

Christoph Schmittner
Erwin Schoitsch

Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)

TERMINOLOGY

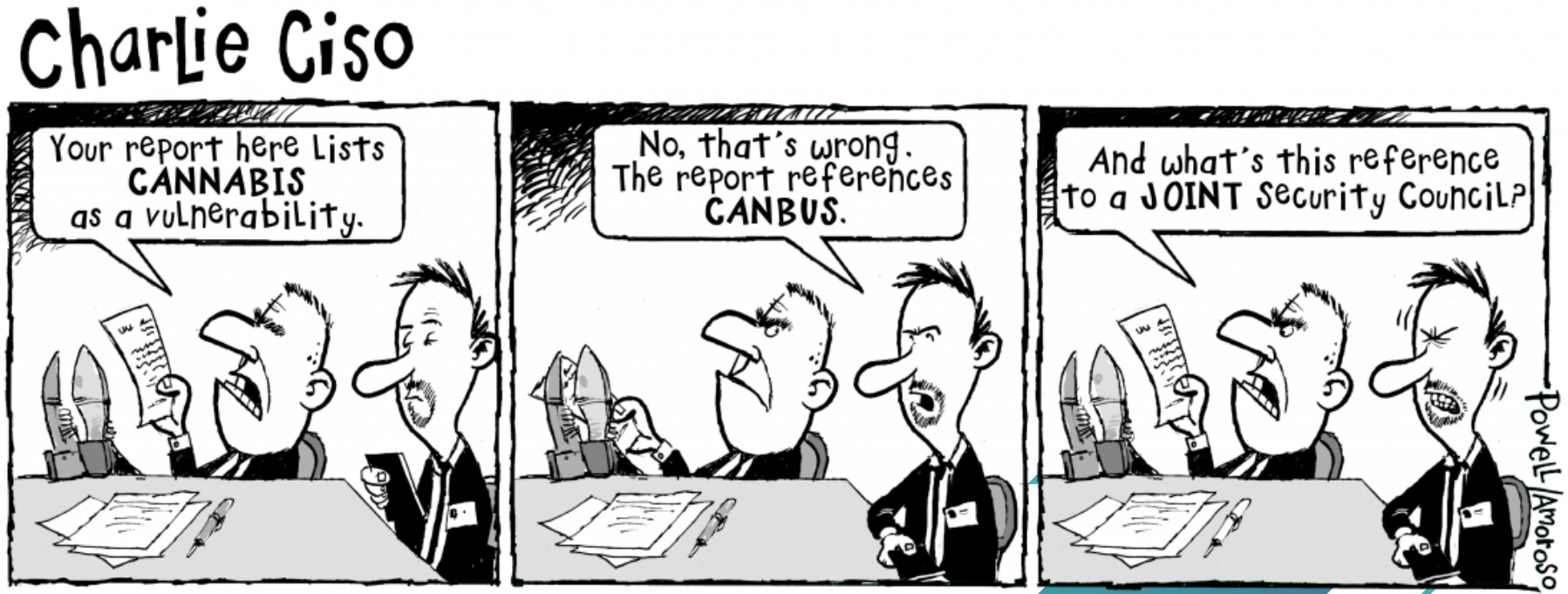
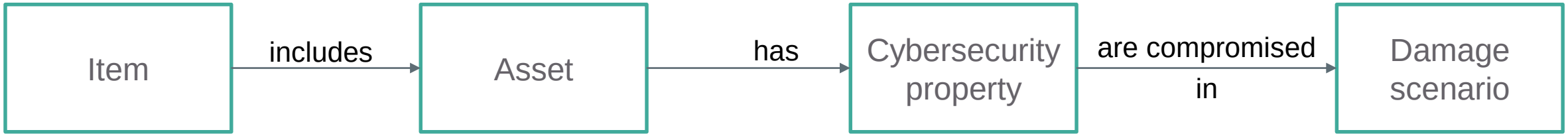


Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)

AUTOMOTIVE CYBERSECURITY

What do we protect

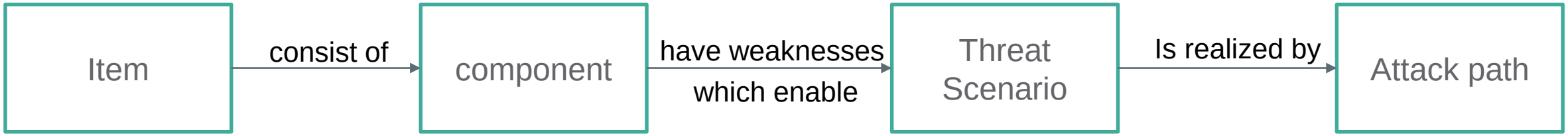


- Item: something which implements a function at vehicle level
- Asset: something of value
- Cybersecurity Property: attribute (CIA) of an asset which is important
- Damage scenario: violation of that property, causing an impact

Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)

AUTOMOTIVE CYBERSECURITY

What could attack us

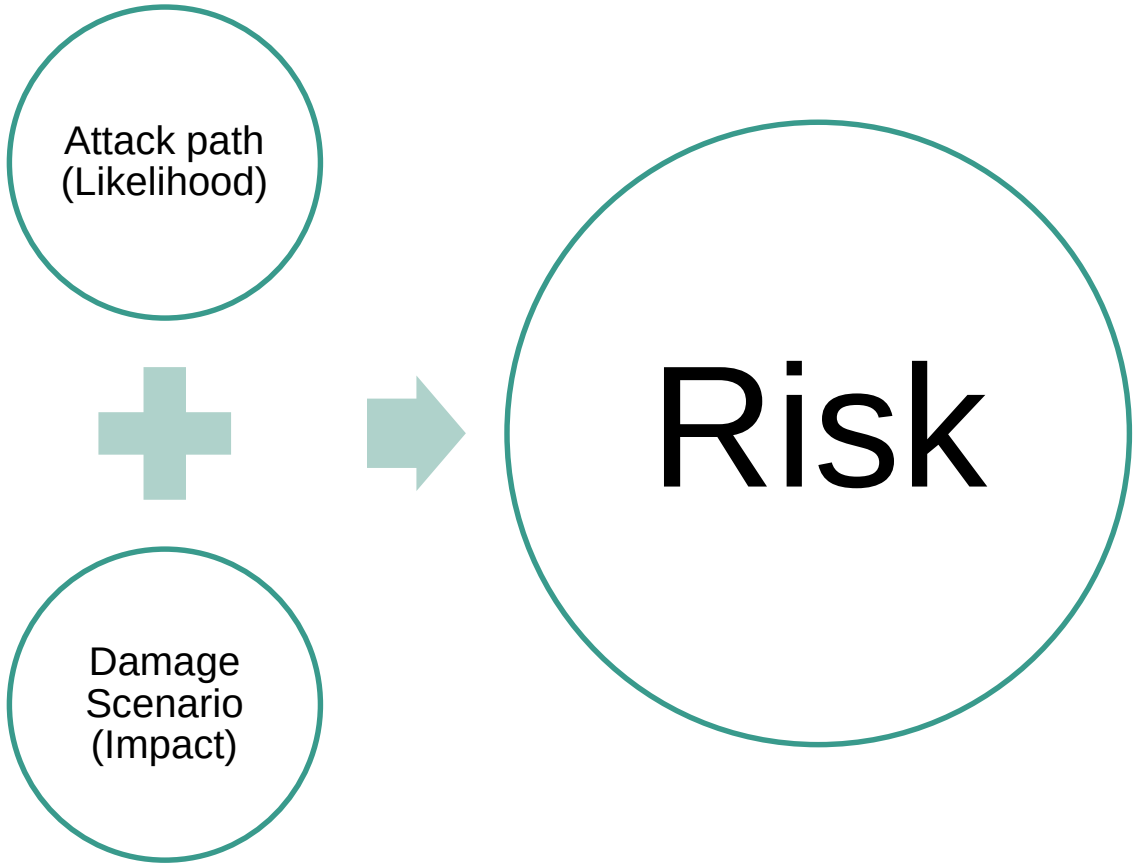


- Item: something which implements a function at vehicle level
- Components: part of the item
- Threat Scenario: something which exploits a weakness in an component
- Attack path: set of action which realize a threat scenario with a certain feasibility

Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)

AUTOMOTIVE CYBERSECURITY

What is the risk



Risk Matrix

Impact \ Likelihood	Very low	Low	Medium	High
Severe	1	3	4	5
Major	1	2	3	4
Moderate	1	2	2	3
Negligible	1	1	1	1

Note: Only values from 1 to 5 are allowed

Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)

THREATGET

Automotive Threat Modeling

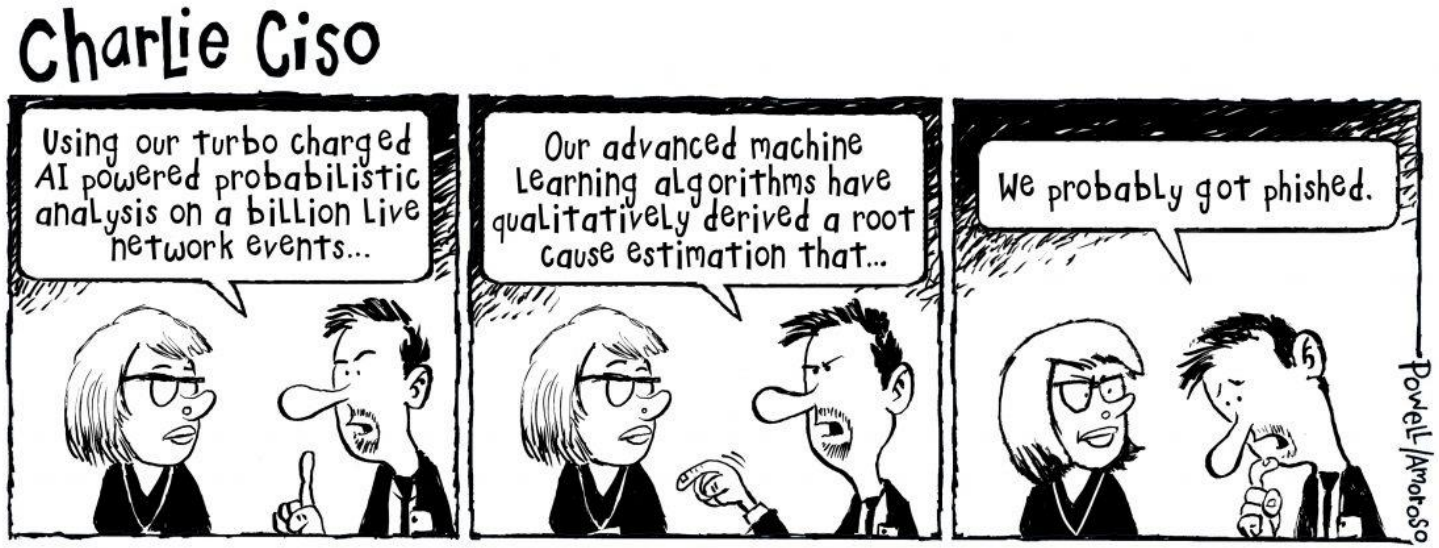


Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)

APPROACH

1. Identify all Assets and their cybersecurity properties

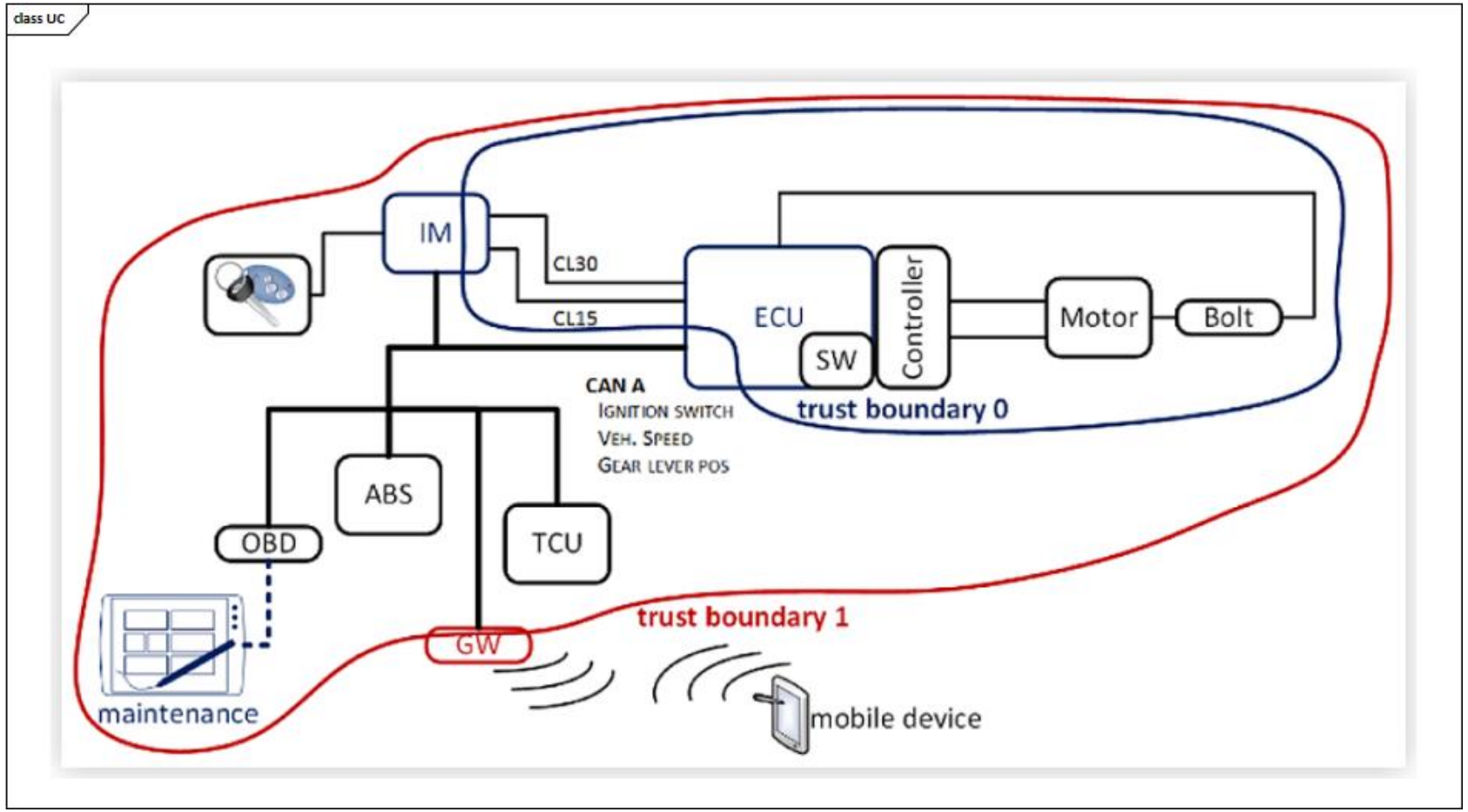
1. Model system and communication architecture

2. Analyze Model for Threats and Attack Paths based on Threat Database

3. Evaluate which attack path lead to a violation of an cybersecurity property

4. Manage identified risks

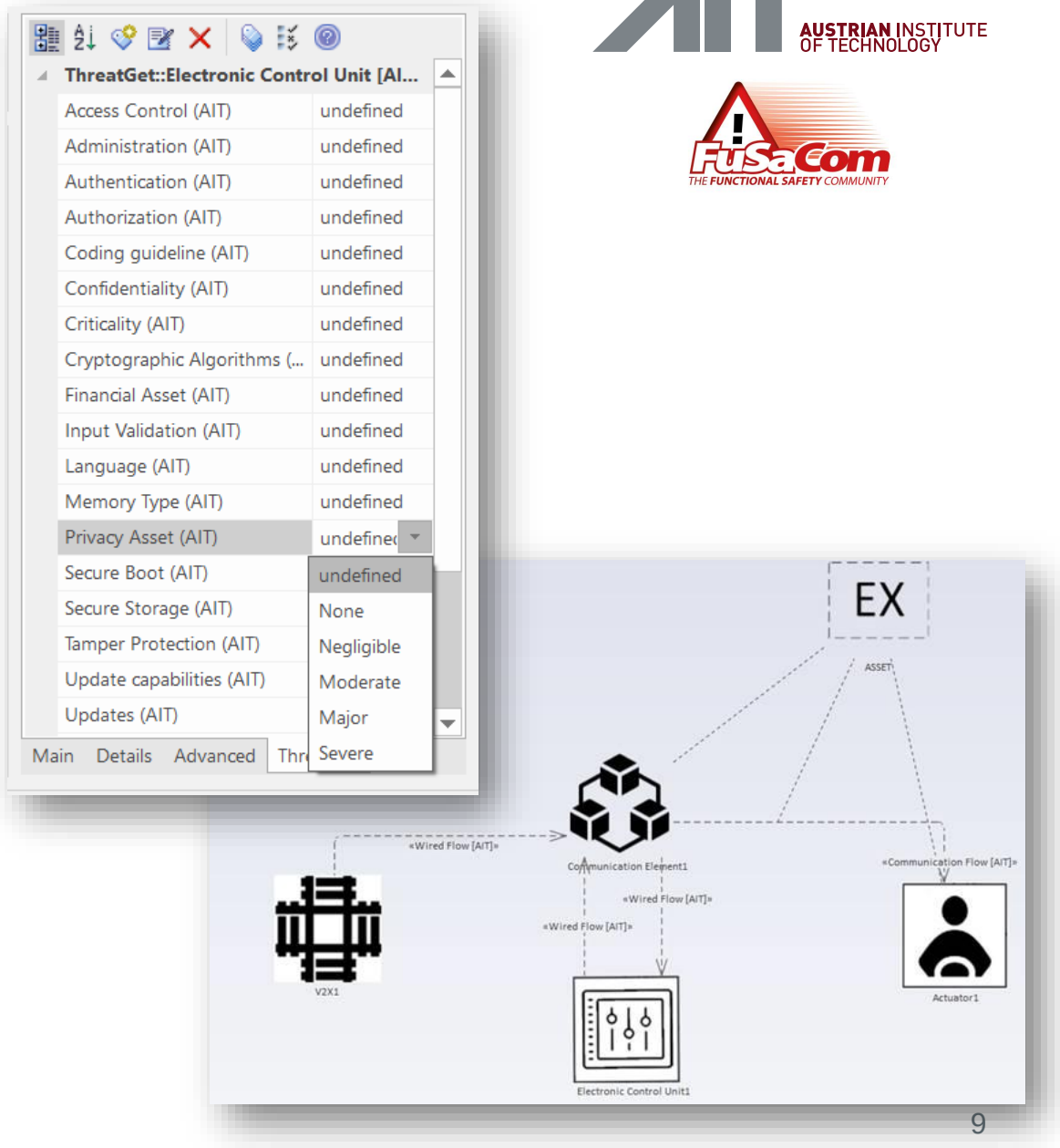
USE CASE – ELECTRONIC STEERING COLUMN LOCK



Macher, Georg, Harald Sporer, Eugen Brenner, and Christian Kreiner. "Supporting cyber-security based on hardware-software interface definition." In European Conference on Software Process Improvement, pp. 148-159. Springer, Cham, 2016.

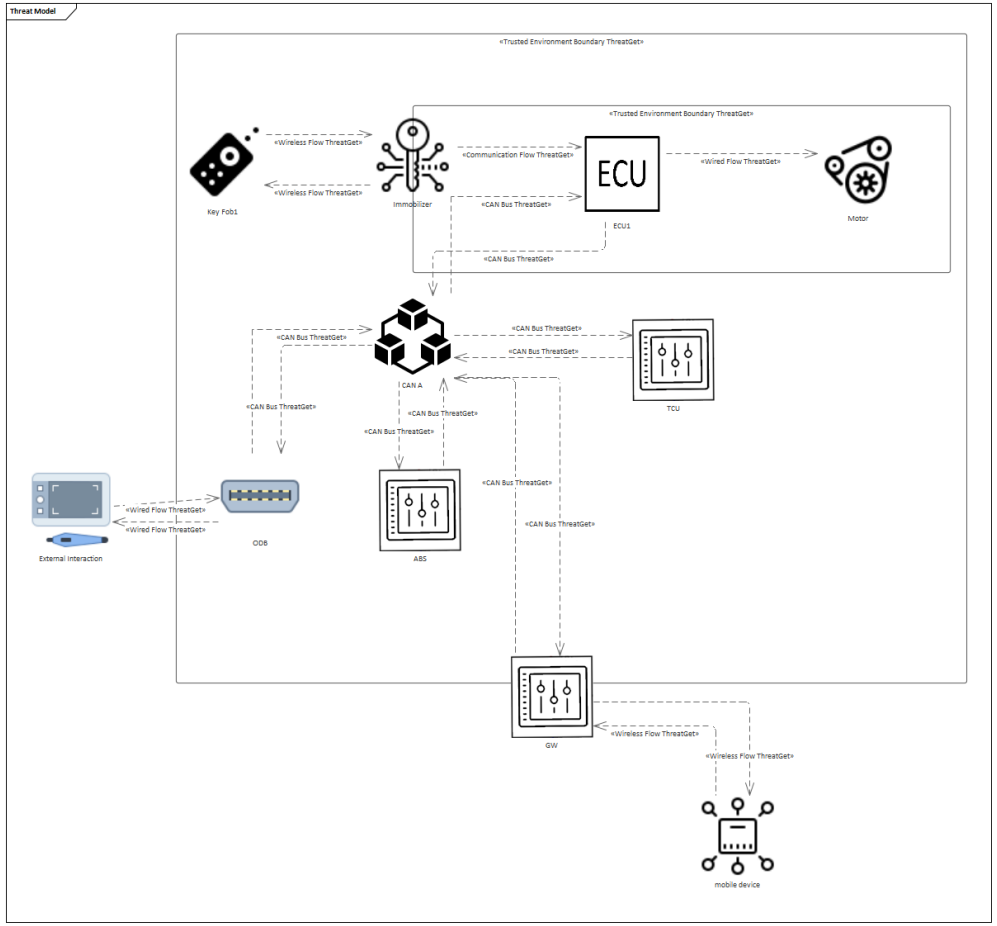
WHAT DO WE PROTECT (ASSETS)

- Assets can be modeled as separate elements
  - Extendable list of relevance to:
    - Safety, Financial, Operational, Privacy, …
  - Contains relevant CS property
    - Confidentiality, Integrity, Availability



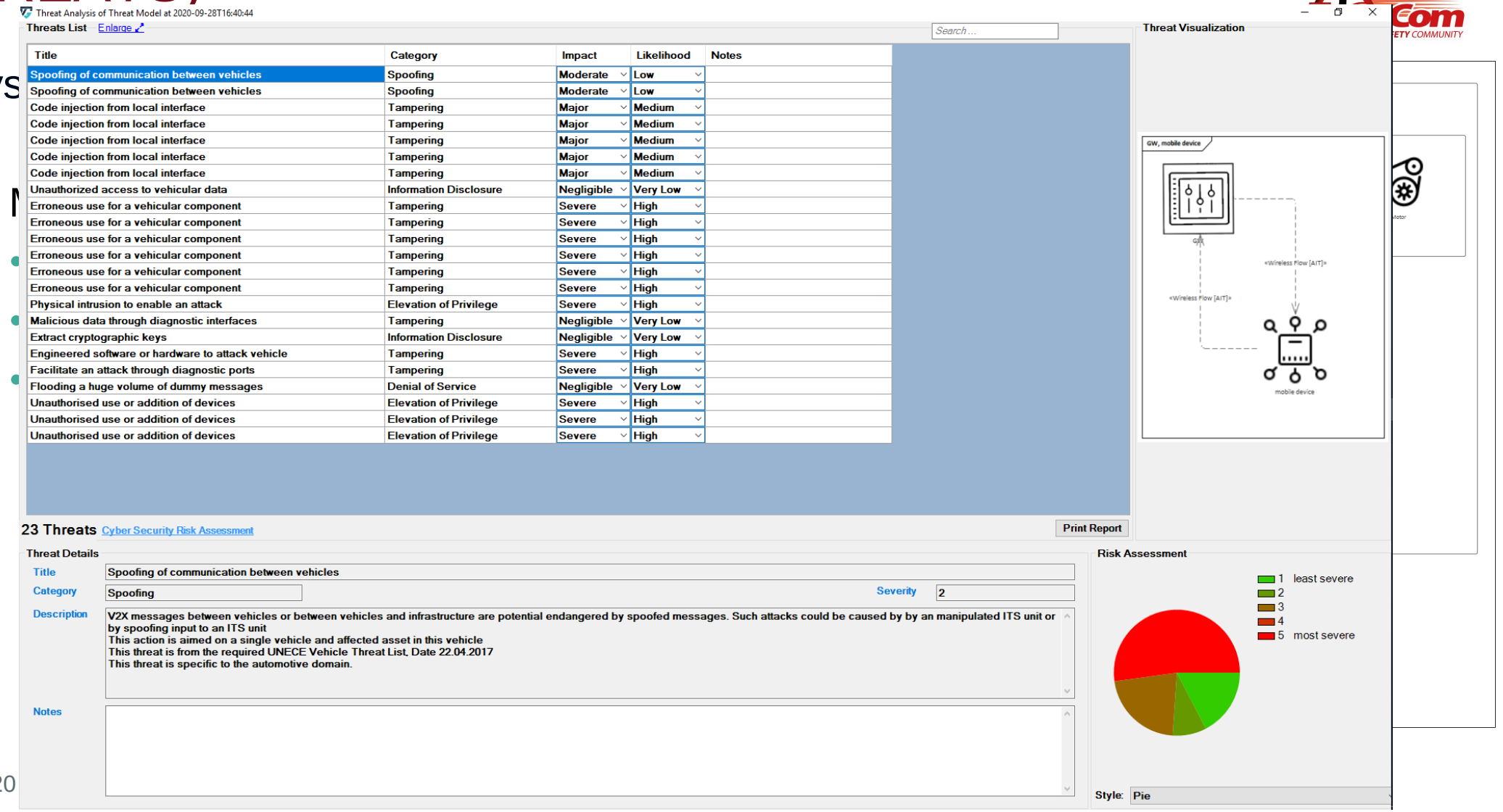
WHAT COULD ATTACK US (THREATS)

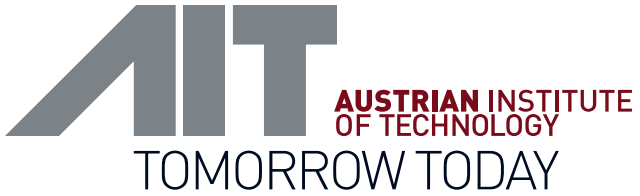
- System Model
  - Modeling of:
    - Security properties
    - System properties
    - Communication properties
  - Connect Assets to:
    - Communication flows
    - System elements



WHAT COULD ATTACK US (THREATS)

- Sys
  - M
    -
    -
    -





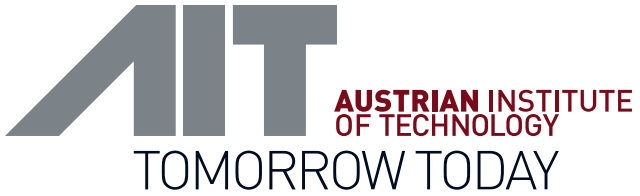
THANK YOU!

Christoph Schmittner, Erwin Schoitsch

28.09.2020

https://www.threatget.com/


FuSaCom
THE FUNCTIONAL SAFETY COMMUNITY

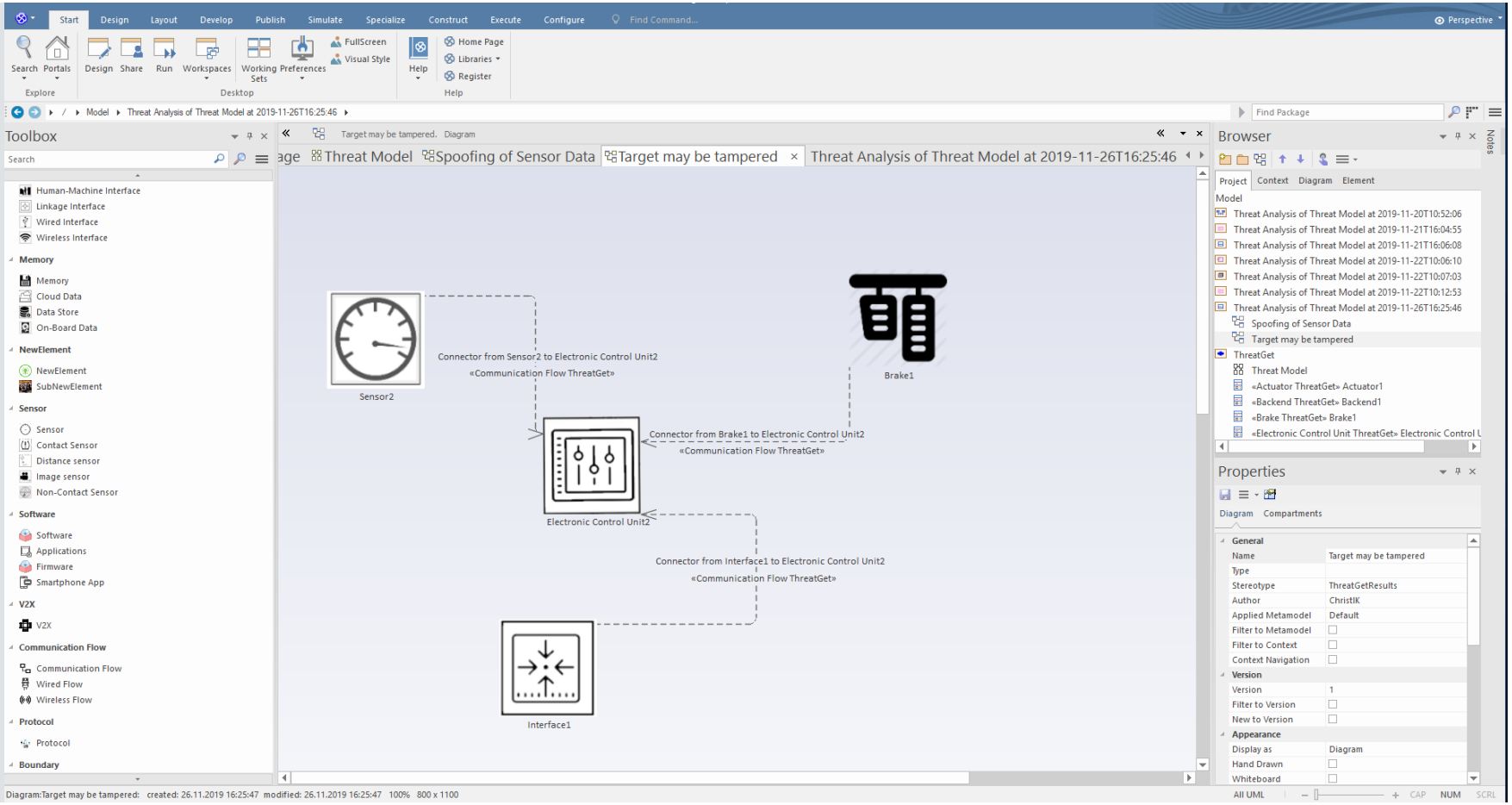

AUSTRIAN INSTITUTE
OF TECHNOLOGY
TOMORROW TODAY

BACKUP

MODEL-BASED ENGINEERING

Security Model

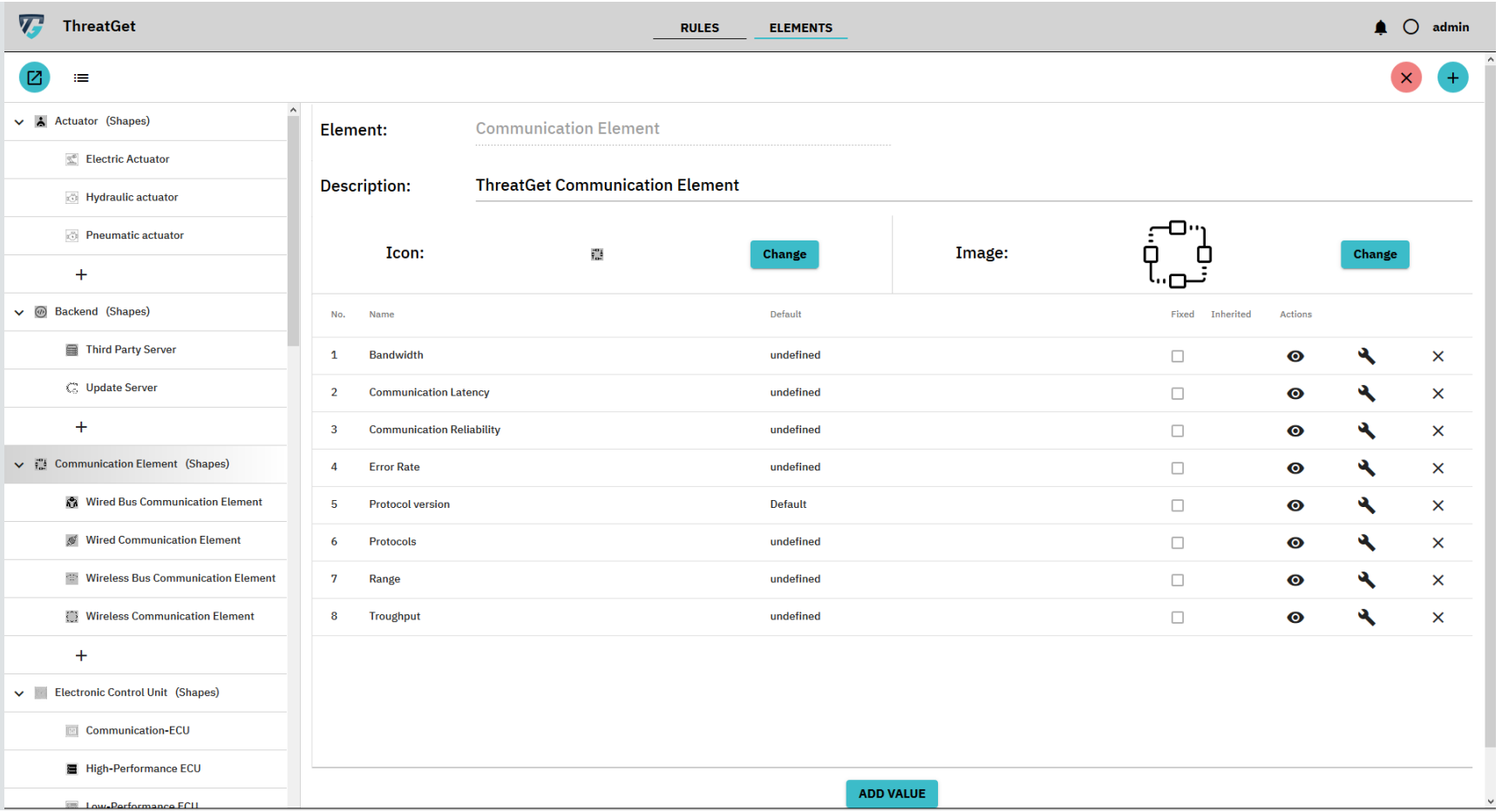
- **ThreatGet is integrated into Enterprise Architect Tool**
- **Security model and system model are connected**



DOMAIN ELEMENTS

Domain Elements

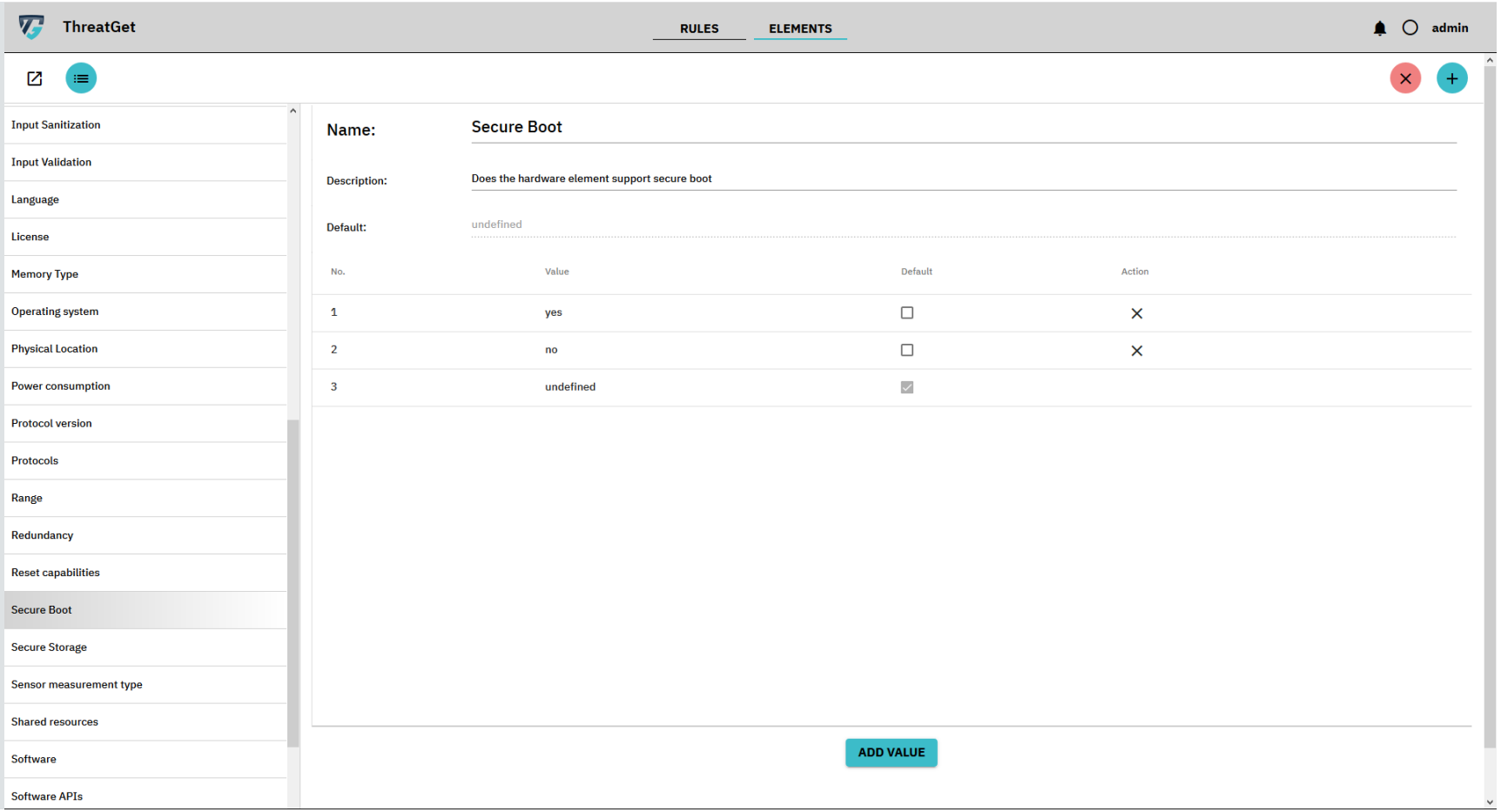
- **Set of common elements for a domain**
- **Inheritance and Refinement**
- **Customizable**



SECURITY PROPERTIES

Security Properties

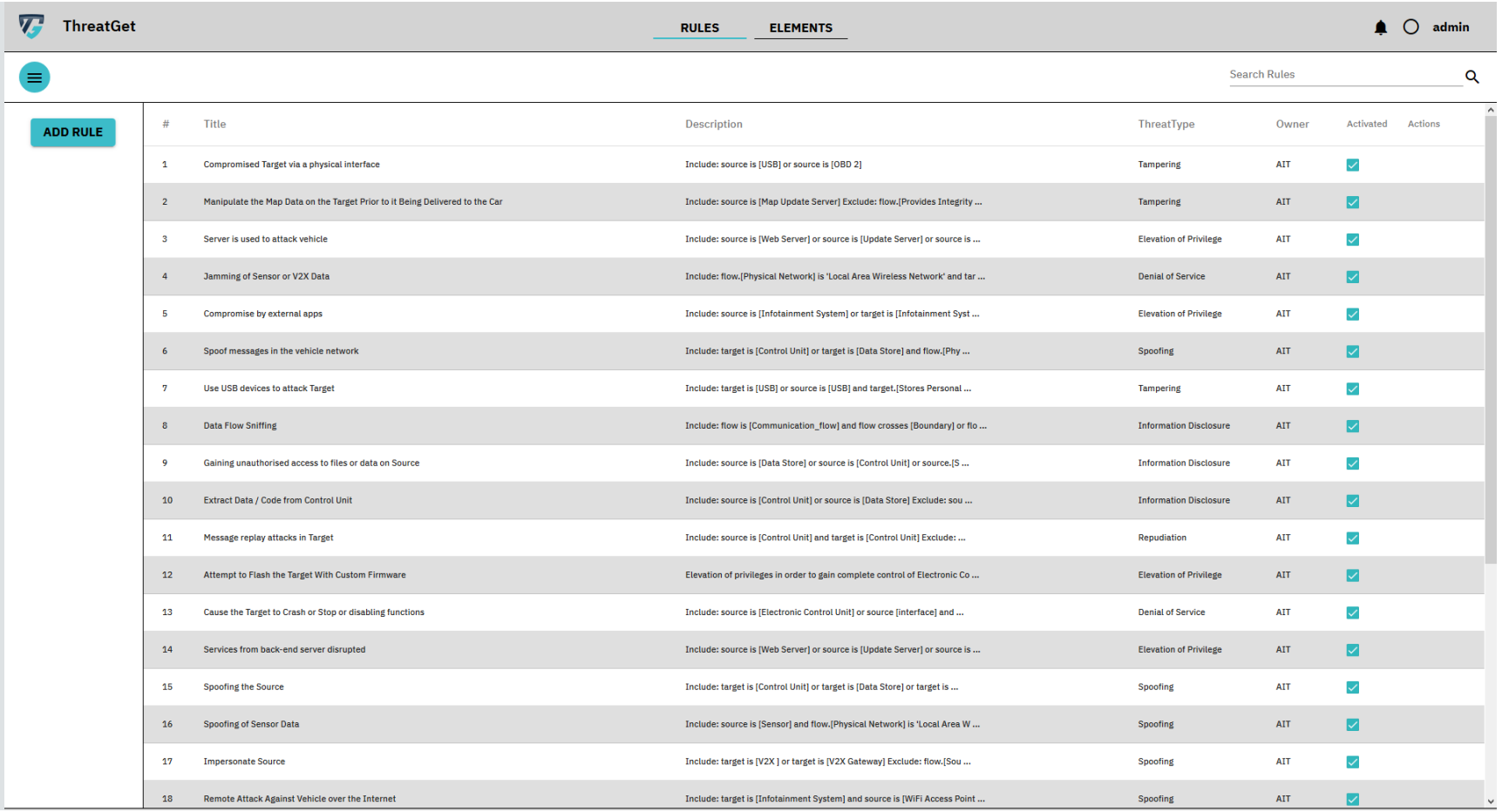
- **Relevant security properties, including assets**
- **Assignable to elements**
- **Customizable**



AUTOMATED SECURITY ASSESSMENT

Rule Engine

- **Rules describe potential weaknesses**
- **Multi-hops attack and attack flows**
- **Risk evaluation based on weakness and assets**

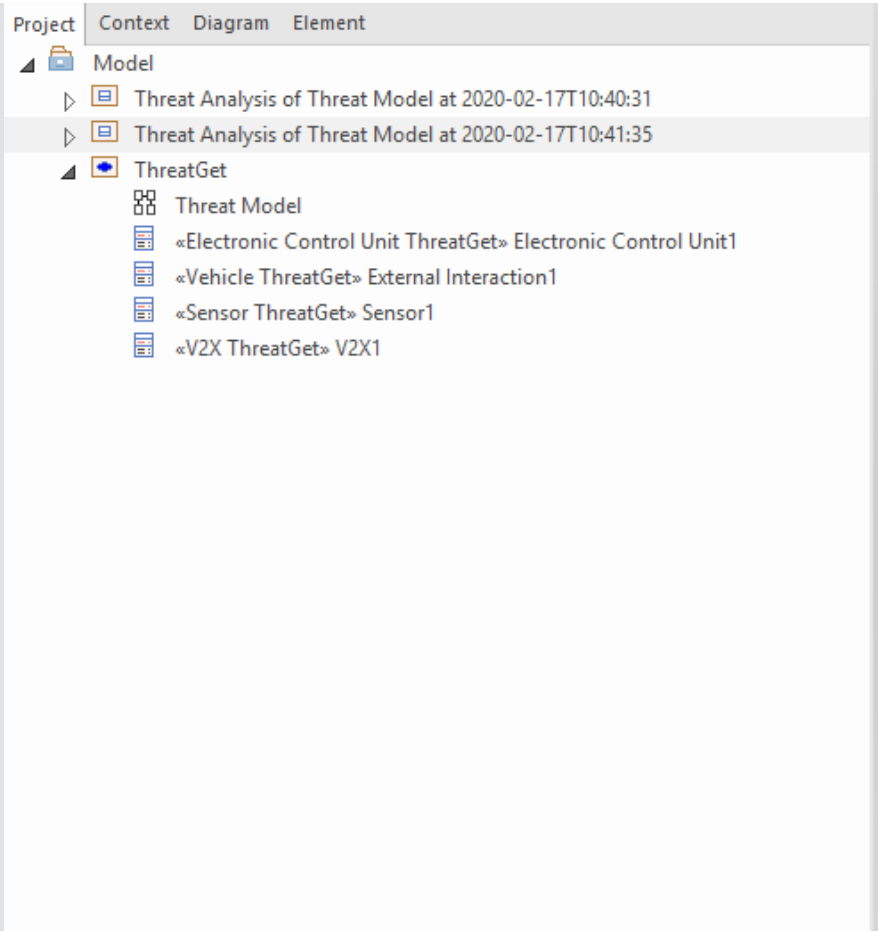


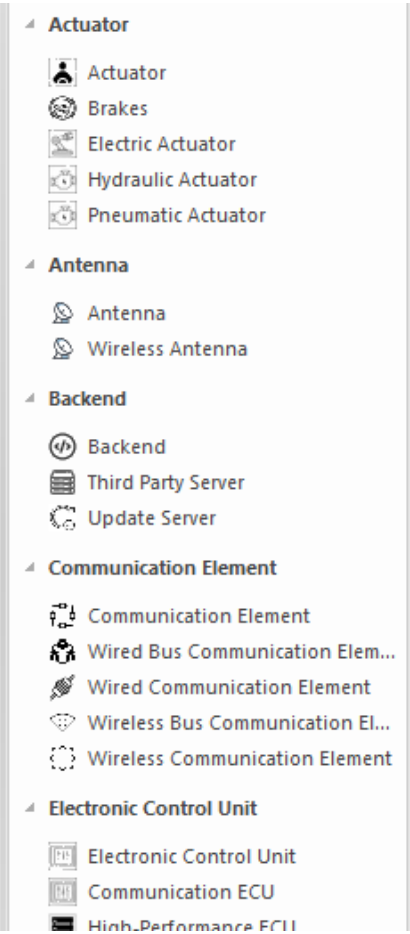
#	Title	Description	ThreatType	Owner	Activated	Actions
1	Compromised Target via a physical interface	Include: source is [USB] or source is [OBD 2]	Tampering	AIT	☑	
2	Manipulate the Map Data on the Target Prior to it Being Delivered to the Car	Include: source is [Map Update Server] Exclude: flow.[Provides Integrity ...	Tampering	AIT	☑	
3	Server is used to attack vehicle	Include: source is [Web Server] or source is [Update Server] or source is ...	Elevation of Privilege	AIT	☑	
4	Jamming of Sensor or V2X Data	Include: flow.[Physical Network] is 'Local Area Wireless Network' and tar ...	Denial of Service	AIT	☑	
5	Compromise by external apps	Include: source is [Infotainment System] or target is [Infotainment Syst ...	Elevation of Privilege	AIT	☑	
6	Spoof messages in the vehicle network	Include: target is [Control Unit] or target is [Data Store] and flow.[Phy ...	Spoofing	AIT	☑	
7	Use USB devices to attack Target	Include: target is [USB] or source is [USB] and target.[Stores Personal ...	Tampering	AIT	☑	
8	Data Flow Sniffing	Include: flow is [Communication_flow] and flow crosses [Boundary] or flo ...	Information Disclosure	AIT	☑	
9	Gaining unauthorised access to files or data on Source	Include: source is [Data Store] or source is [Control Unit] or source.[S ...	Information Disclosure	AIT	☑	
10	Extract Data / Code from Control Unit	Include: source is [Control Unit] or source is [Data Store] Exclude: sou ...	Information Disclosure	AIT	☑	
11	Message replay attacks in Target	Include: source is [Control Unit] and target is [Control Unit] Exclude: ...	Repudiation	AIT	☑	
12	Attempt to Flash the Target With Custom Firmware	Elevation of privileges in order to gain complete control of Electronic Co ...	Elevation of Privilege	AIT	☑	
13	Cause the Target to Crash or Stop or disabling functions	Include: source is [Electronic Control Unit] or source [interface] and ...	Denial of Service	AIT	☑	
14	Services from back-end server disrupted	Include: source is [Web Server] or source is [Update Server] or source is ...	Elevation of Privilege	AIT	☑	
15	Spoofing the Source	Include: target is [Control Unit] or target is [Data Store] or target is ...	Spoofing	AIT	☑	
16	Spoofing of Sensor Data	Include: source is [Sensor] and flow.[Physical Network] is 'Local Area W ...	Spoofing	AIT	☑	
17	Impersonate Source	Include: target is [V2X] or target is [V2X Gateway] Exclude: flow.[Sou ...	Spoofing	AIT	☑	
18	Remote Attack Against Vehicle over the Internet	Include: target is [Infotainment System] and source is [WiFi Access Point ...	Spoofing	AIT	☑	

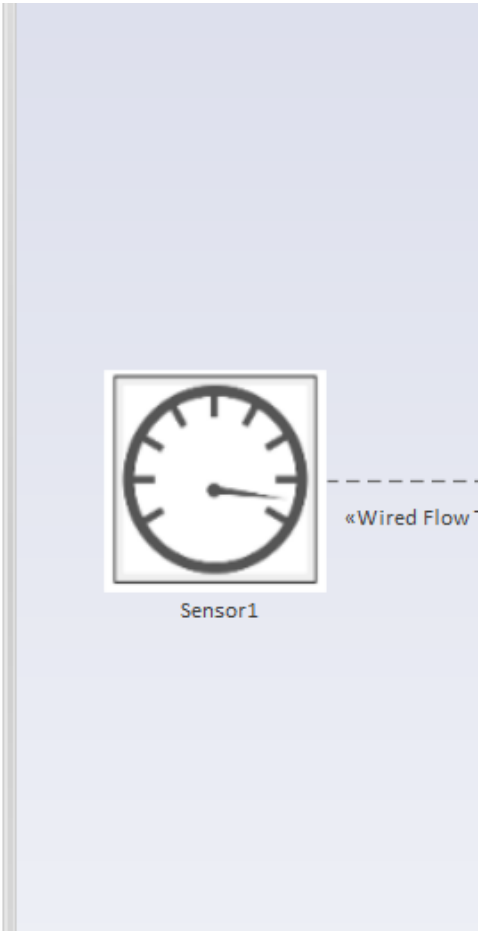
VERSIONING

Traceability of Analysis

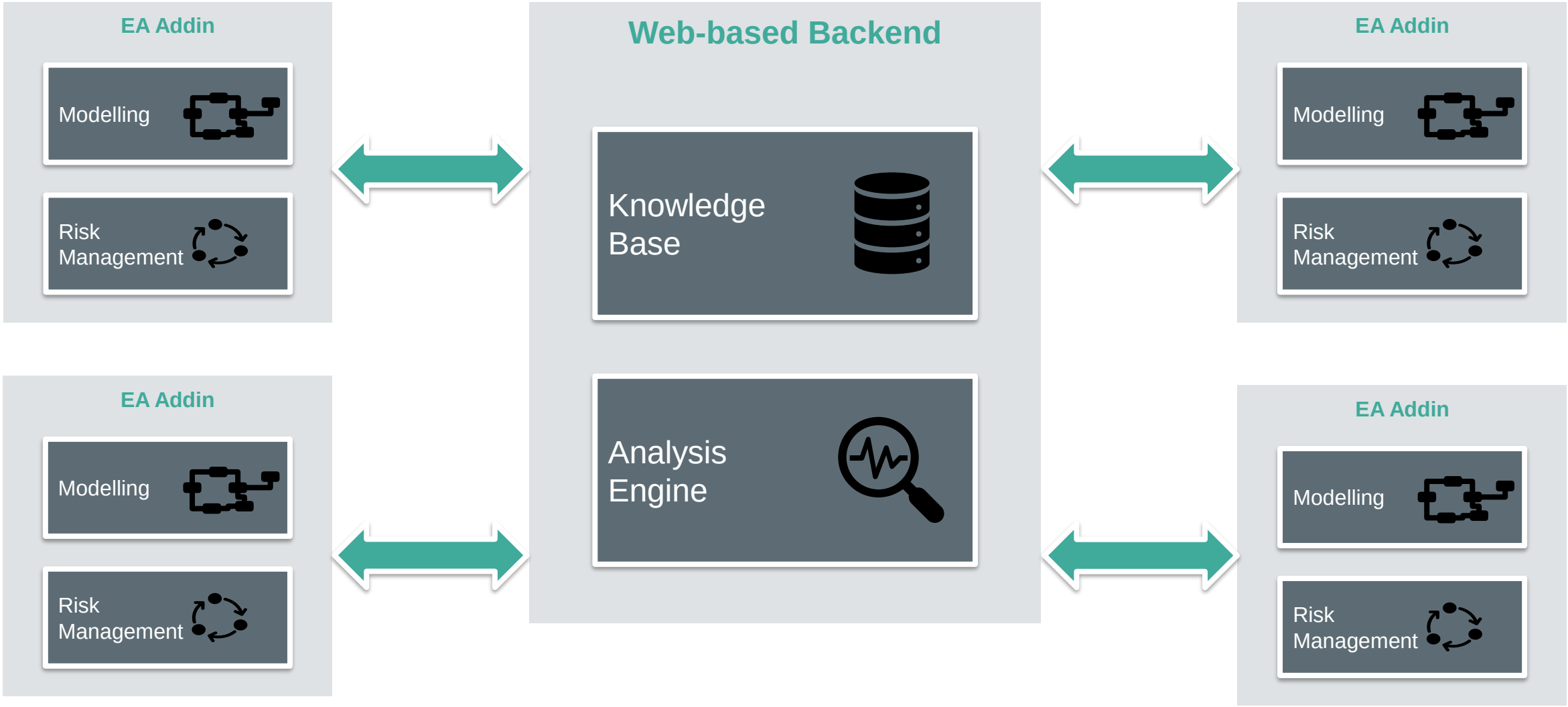
- **For each analysis a snapshot of the model is generated**
- **Snapshot + analysis reports is marked with date and time**
- **Stored in the model**







ARCHITECTURE



AUTOMATED THREAT INTELLIGENCE UPDATES

AUSTRIAN INSTITUTE OF TECHNOLOGY

FuSaCom THE FUNCTIONAL SAFETY COMMUNITY

Web-based Backend

AIT Knowledge Base

User Knowledge Base

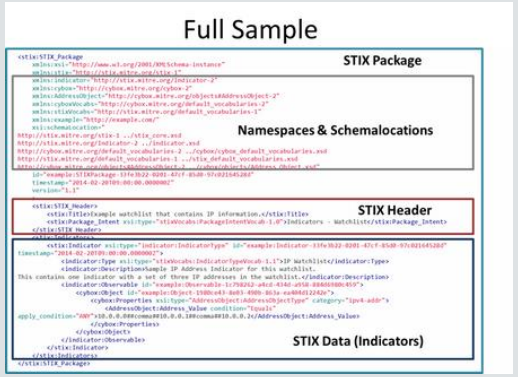
AIT Review and Translation

Threat Intelligence

CVE, Common Vulnerabilities and Exposures

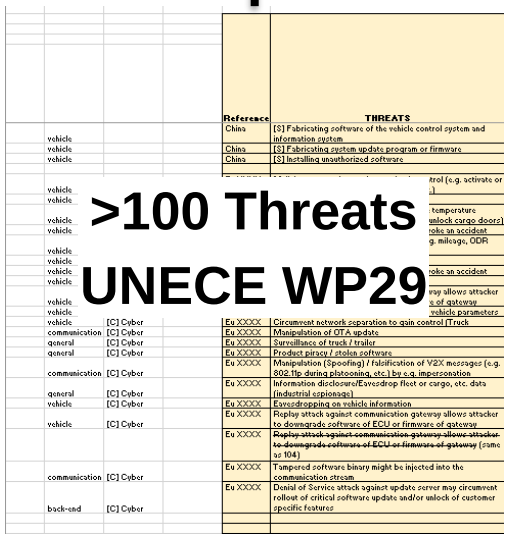
STIX, Structured Threat Information eXpression

…



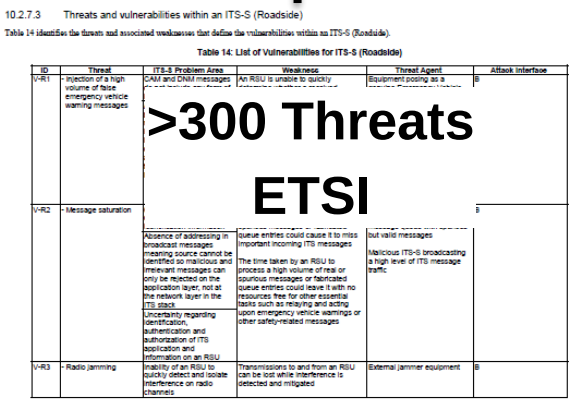
THREAT INTELLIGENCE – AUTOMOTIVE EXAMPLE

AIT Knowledge Base >1400



>100 Threats

UNECE WP29

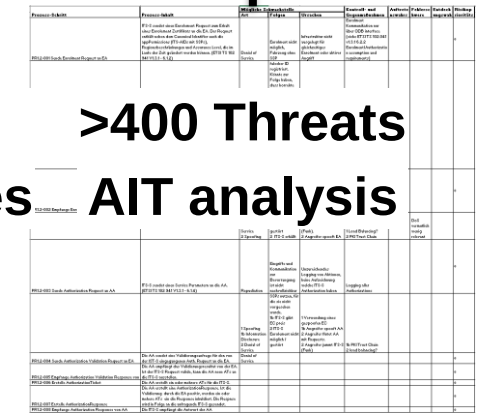


>300 Threats

ETSI

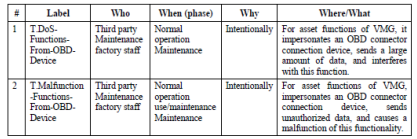
>400 Threats

External sources



>400 Threats

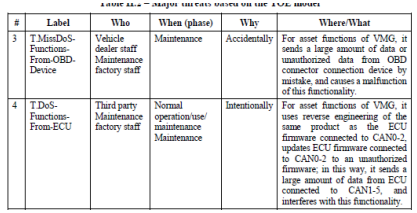
AIT analysis



#	Label	Who	When (phase)	Why	Where/What
1	T.DoS-Functions-From-OBD-Device	Third party Maintenance factory staff	Normal operation Maintenance	Intentionally	For asset functions of VMG, it impersonates an OBD connector connection device, sends a large amount of data, and interferes with this function.
2	T.Malfunction-Functions-From-OBD-Device	Third party Maintenance factory staff	Normal operation use/maintenance Maintenance	Intentionally	For asset functions of VMG, impersonates an OBD connector connection device, sends unauthorized data, and causes a malfunction of this functionality.

>200 Threats

ITU



#	Label	Who	When (phase)	Why	Where/What
3	T.MissDoS-Functions-From-OBD-Device	Vehicle dealer staff Maintenance factory staff	Maintenance	Accidentally	For asset functions of VMG, it sends a large amount of data or unauthorized data from OBD connector connection device by mistake, and causes a malfunction of this functionality.
4	T.DoS-Functions-From-ECU	Third party Maintenance factory staff	Normal operation/use/ maintenance Maintenance	Intentionally	For asset functions of VMG, it uses reverse engineering of the same product as the ECU firmware connected to CAN0-2, updates ECU firmware connected to CAN0-2 to an unauthorized firmware; in this way, it sends a large amount of data from ECU connected to CAN1-5, and interferes with this functionality.

UNECE WP29: World Forum for Harmonization of Vehicle Regulations

ETSI: European Telecommunications Standards Institute (V2X in Europe)

ITU: International Telecommunication Union