How Cyber Security Threat Modeling keeps your Organization Innovative

Secure IoT Design thanks to THREATGET

AGENDA

1. A brief introduction
2. What is ThreatGet?
3. The STRIDE Framework
4. Systems Development
5. IoT-Security Situation
6. Innovation: Security-by Design with ThreatModeling
7. Conclusion

THE SPEAKER

Orsolya Németh

Trainer, Cunsultant and Speaker
Sparx Services CE and LieberLieber

Co-founder: SIG WOMENinICT


THREATGET
Sparx Service
UK
Sparx Service
North America
Sparx Systems
Sparx Services
Central Europe
LieberLieber
Software
LieberLieber
Software
Sparx Systems
China
Sparx Systems
Japan
Sparx Systems
India
Sparx Services
Australia
Sparx Systems
HQ
Sparx Systems
Argentina
Sparx Systems
HQ
Sparx Systems
Sister&Service Companies
LieberLieber Software
AIT
AUSTRIAN INSTITUTE OF TECHNOLOGY
LieberLieber
software gmbh

WHO WE ARE

THREATGET

LieberLieber software gmbh

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY

OUR EXPERTISE

- Model-based Systems Engineering
- Configuration Management for Models
- Integration Enterprise Architect with other Tools

KEY Infrastructure Issues

- Austria‘s largest research and technology organization
- Partner to industry and public institutions

CYBER SECURITY MODELING
WITH METHODOLOGY- THREATGET

THREATGET

- ThreatGet is a tool based on Sparx Systems Enterprise Architect that helps in the design phase of many projects to search for potential threats:

Automotiv

Critical Infrastructure

IIoT Environments

Railway

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY LieberLieber software gmbh

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

THE STRIDE THREAT MODEL

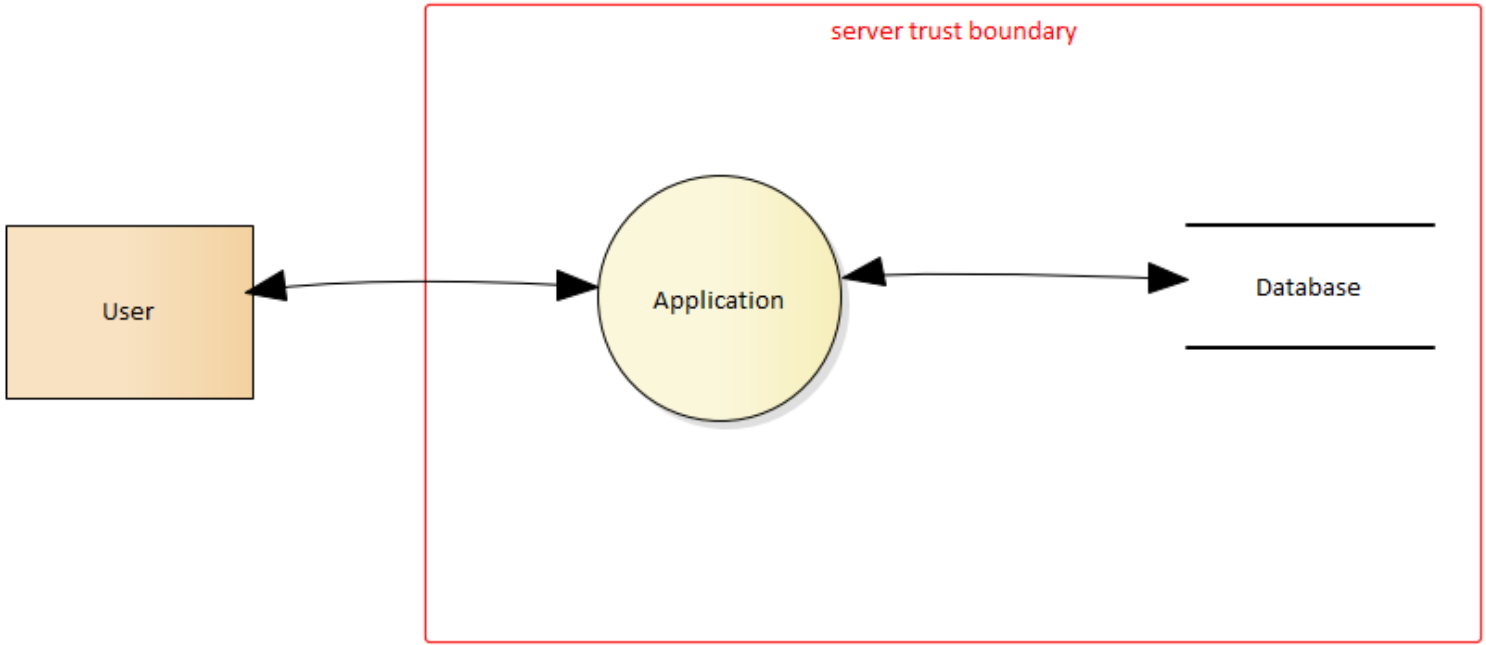
THREATGET

- Is a Framework of security risks developed

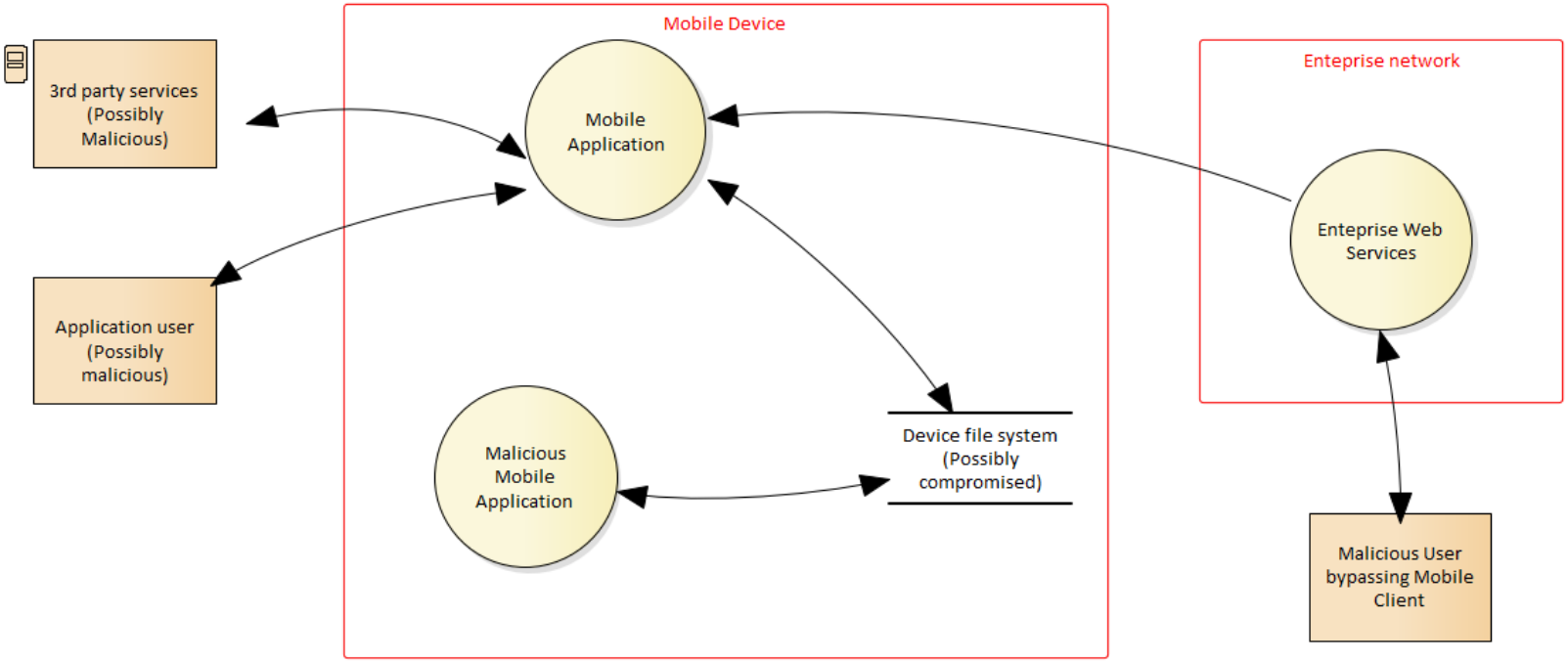
Bedrohung	Betrifft	Definition
S **poofing**	Authentifikation	Vortäuschung falscher Identität, Zugriff auf vertrauliche Informationen und Daten
T **ampering**	Integrität	Manipulation von (presistenten) Daten
R **epudiation**	Zutritt	Nicht beweisbare Aktion eines Angreifers
I **nformation disclosure**	Vertraulichkeit	Angreifer sieht Daten die er nicht sehen soll
D **enial of service**	Verfügbarkeit	Verfügbarkeit einer Anwendung stören
E **levation of privilege**	Autorisierung	Angreifer findet Weg um seine Privilegien zu erhöhen

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY LieberLieber software gmbh

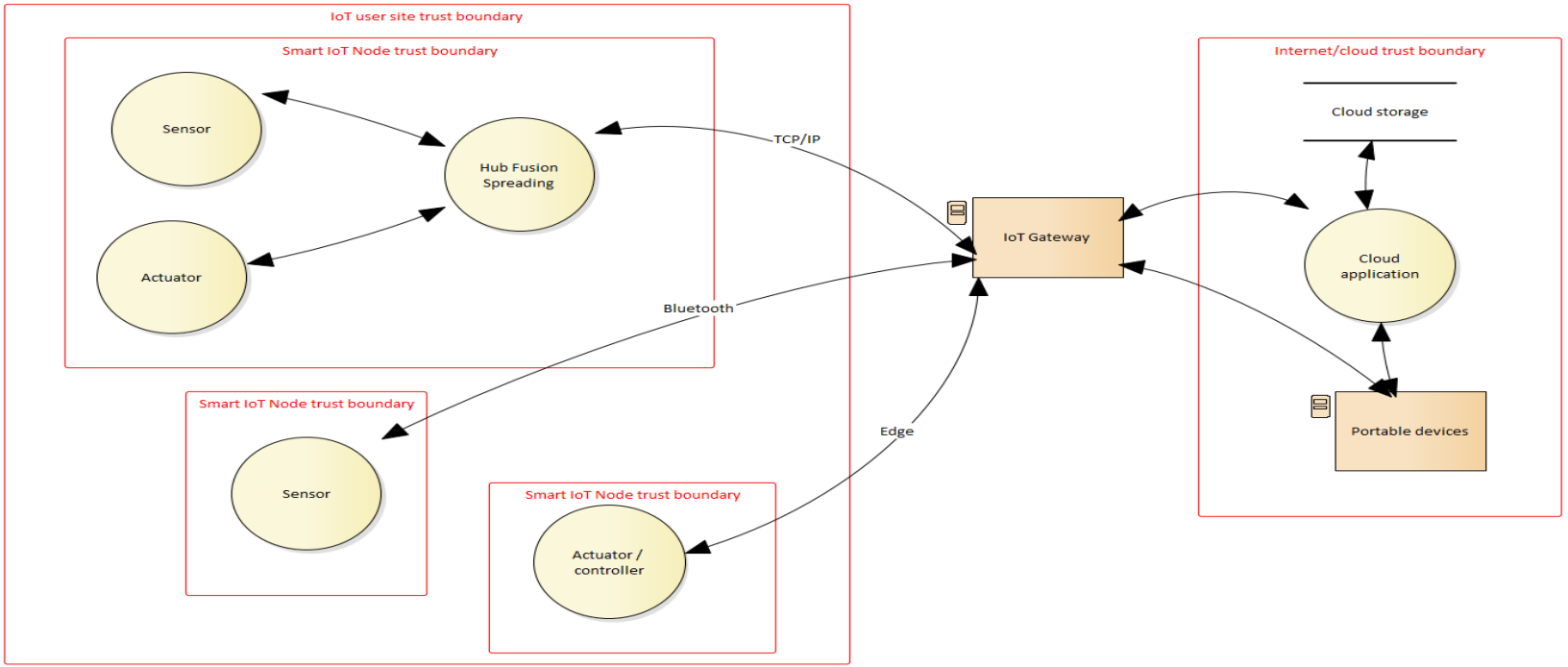
SYSTEM DEVELOPMENT 1/3



SYSTEM DEVELOPMENT 2/3



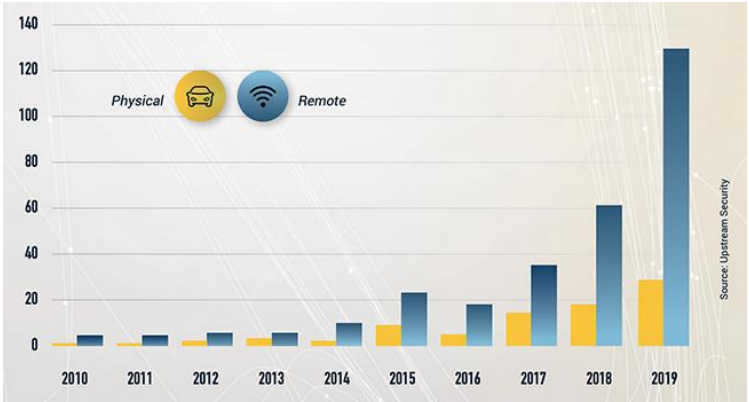
SYSTEM DEVELOPMENT 3/3



IOT

Security Situation

THE CHALLANGES



"In 2020, 54.6% of incidents were attacks by black-hat hackers …"

Quelle: Upstream Security Global Automotive Cybersecurity Report 2021

EXAMPLES FROM 2020

- January
  - *4,118 vehicles were stolen in India with electronic devices r*
  - *A Mobileye 630 PRO hack fooled the ADAS of a Tesla Model X February*
  - 19 security vulnerabilities were found in a Mercedes-Benz E-Class April
  - *Hackers took full control of an OEM's corporate network*
- August
  - *A hacker managed to gain control of Tesla's entire connected car*
  - *More than 300 vulnerabilities found in over 40 ECUs*

Quelle: Upstream Security Global Automotive Cybersecurity Report 2021

LEGAL STANDARDIZATIONS & REGULATIONS

THREATGET

The US

- CCPA (California Consumer Privacy Act) - U.S. state-level privacy law.
- DIGI (Developing and Growing the Internet of Things) Act - National strategy for the IoT.
- NIST (National Institute of Standards and Technology) –Privacy Framework V 1.0.

The UK

- DCMS (Department for Digital, Culture, Media and Sport) - Introduced security requirements for all IoT devices.

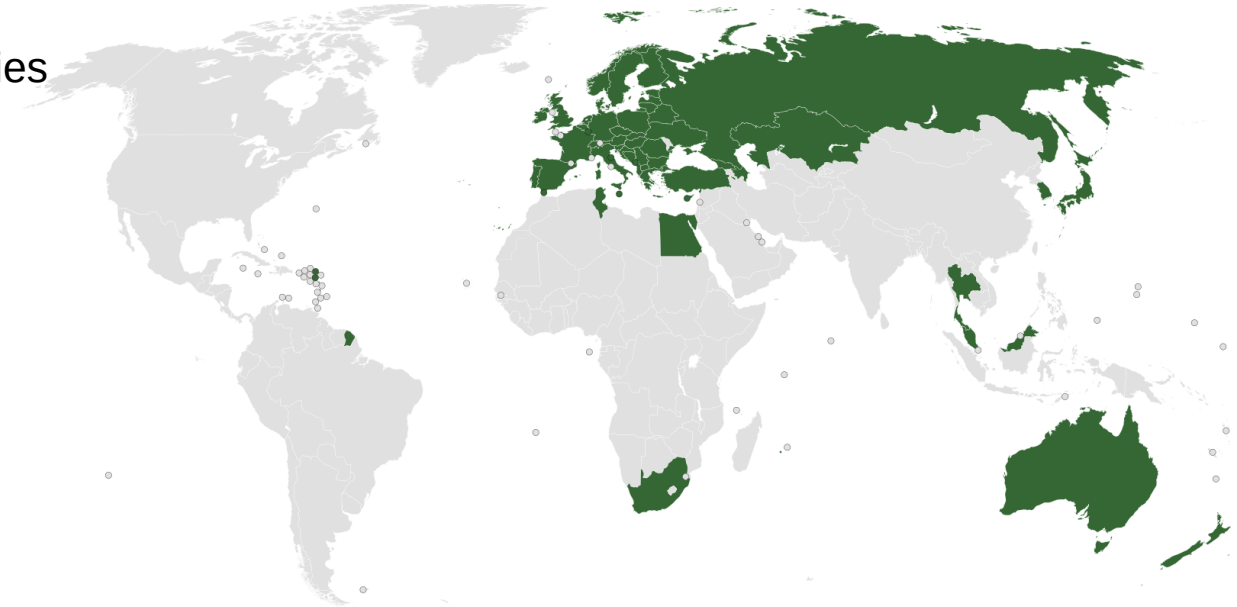
The EU

- ENISA (EU Cybersecurity Agency) study titled: "Essential Security Recommendations for IoT in the Context of Critical Information Infrastructures."

UNECE WORLD FORUM FOR HARMONIZATION OF VEHICLE REGULATIONS

THREATGET

- UNECE WP29 defines requirements for type approval
- Members are:
  - Type approval authorities
  - Certification bodies
  - OEM and Tier 1
- Two new regulations on:
  - **Cybersecurity**
  - Software Updates



AIT Austrian Institute of Technology

LieberLieber software gmbh

UNECE WP 29
REGULATION ON CYBER SECURITY

THREATGET

- **Vehicle manufacturer**, **Supplier** und **Service providers** need a *Cyber Security Management System* (CSMS)

- CSMS covers **Development, Production** und **“Post-Production”**:
  - **Management** of cybersecurity in the **Organisation**
  - **Management** of risks related to the vehicle
  - **Management of new Cyberthreats** and**vulnerabilities**

7.3. Requirements for vehicle types

7.3.1. The manufacturer shall have a valid Certificate of Compliance for the Cyber Security Management System relevant to the vehicle type being approved.

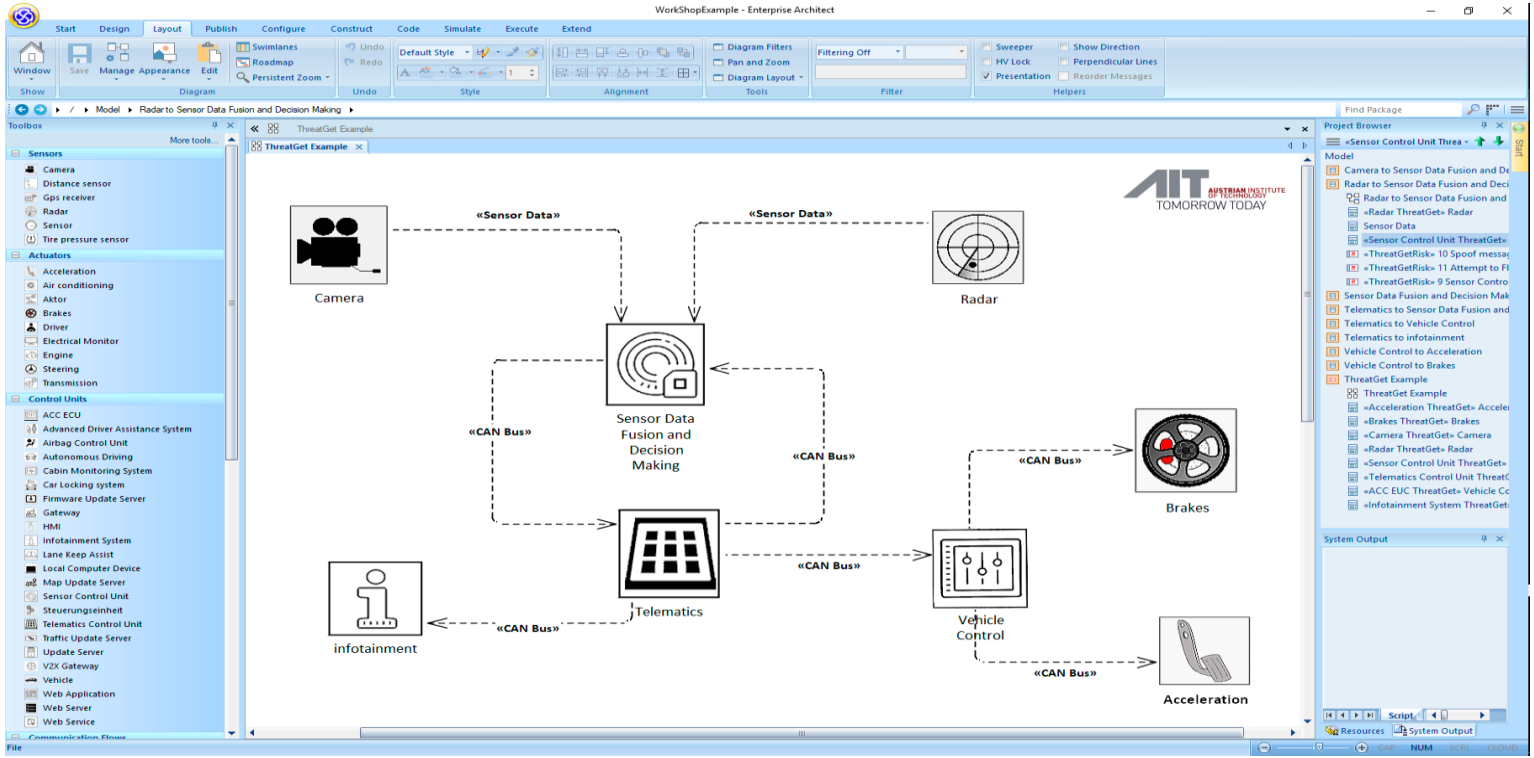
However, for type approvals prior to 1 July 2024, if the vehicle manufacturer can demonstrate that the vehicle type could not be developed in compliance with the CSMS, then the vehicle manufacturer shall demonstrate that cyber security was adequately considered during the development phase of the vehicle type concerned.

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY LieberLieber software gmbh

SECURITY-BY DESIGN

Innovation through Threat Modeling

THREATGET



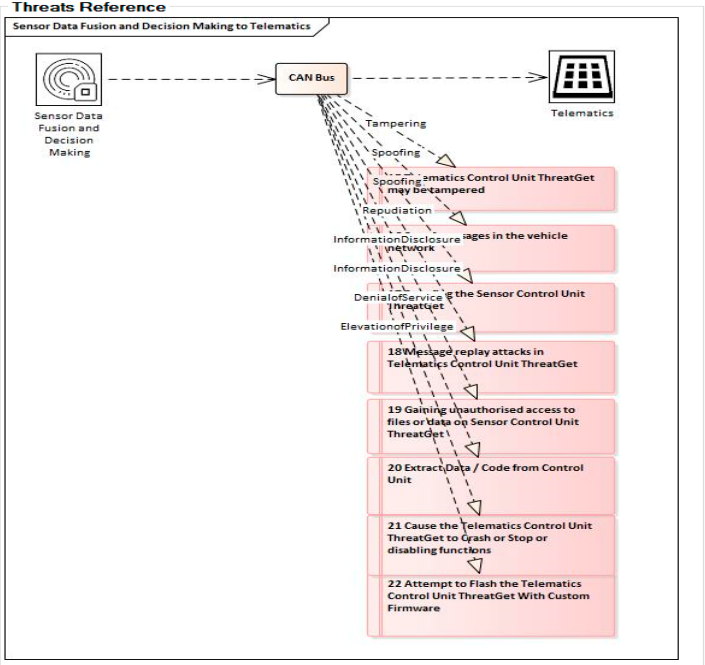
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY LieberLieber software gmbh

THREATGET

Detected Threats

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Threats Reference



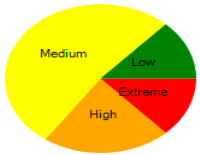
Threats List

	Title	Type	Description	Impact	Likelihood
	16 Spoof me...	Spoofing	Forge or manipulate c...	Major	Likely
▸	17 Spoofing ...	Spoofing	Sensor Control Unit T...	Moder...	Possible
	18 Message ...	Repudiation	Packets or messages...	Major	Likely
	19 Gaining u...	InformationD...	Confidentiality of data...	Moder...	Possible
	20 Extract D...	InformationD...	Accessing data store...	Trivial	Remote
	21 Cause the...	DenialofSer...	DoS on Telematics C...	Critical	Certain
	22 Attempt to...	ElevationofP...	Elevation of privilege...	Moder...	Possible
	23 Sensor C...	Tampering	Sensor Control Unit T...	Moder...	Possible
	24 Spoof me...	Spoofing	Forge or manipulate c...	Major	Likely
	25 Spoofing ...	Spoofing	Telematics Control U...	Moder...	Possible
	26 Message ...	Repudiation	Packets or messages...	Major	Likely
	27 Gaining u...	InformationD...	Confidentiality of data...	Moder...	Possible
	28 Extract D...	InformationD...	Accessing data store...	Trivial	Remote
	29 Cause the...	DenialofSer...	DoS on Sensor Contr...	Critical	Certain
	30 Attempt to...	ElevationofP...	Elevation of privilege...	Moder...	Possible

46 Threats Cyber Security Risk Assessment

Risk Evaluation

Threat Severity



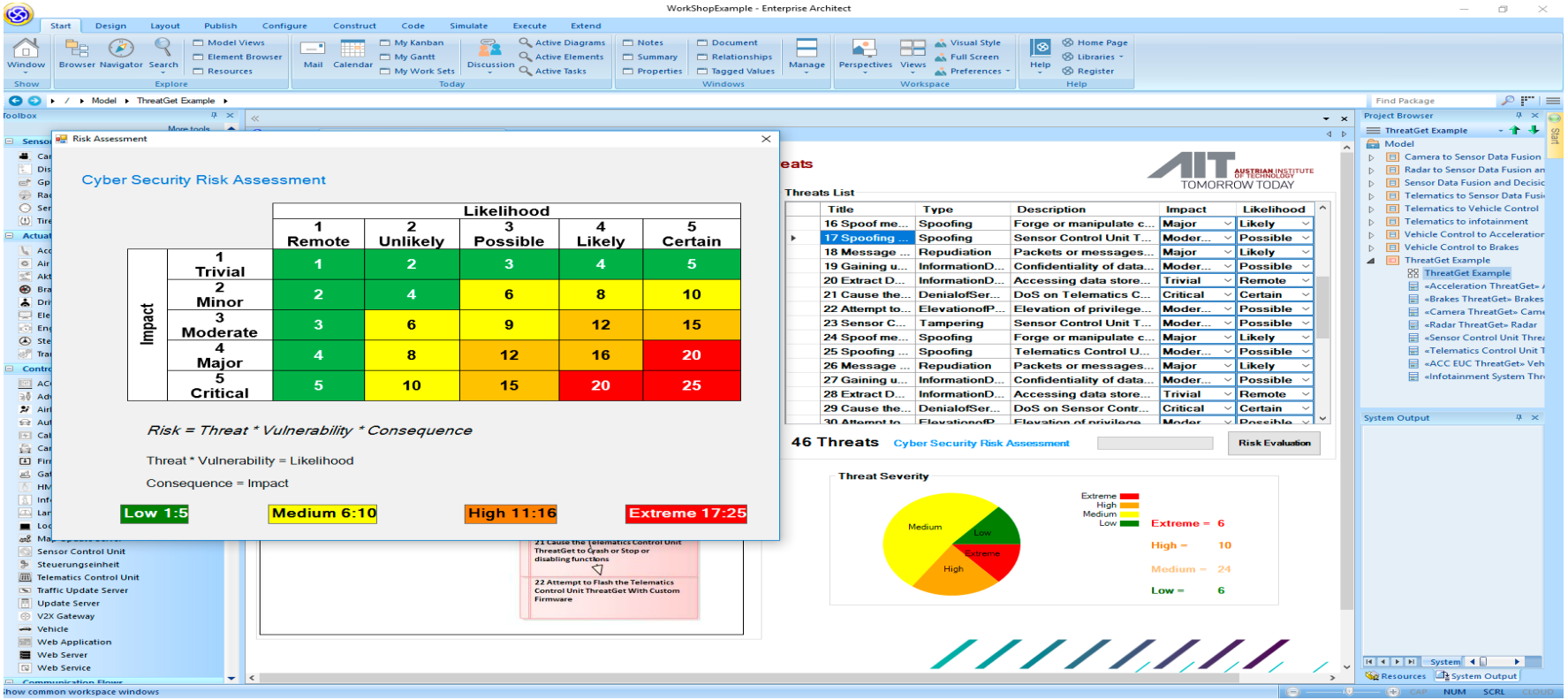
Extreme
High
Medium
Low

Extreme = 6
High = 10
Medium = 24
Low = 6

AUSTRIAN INSTITUTE OF TECHNOLOGY
LieberLieber software gmbh

THREATGET

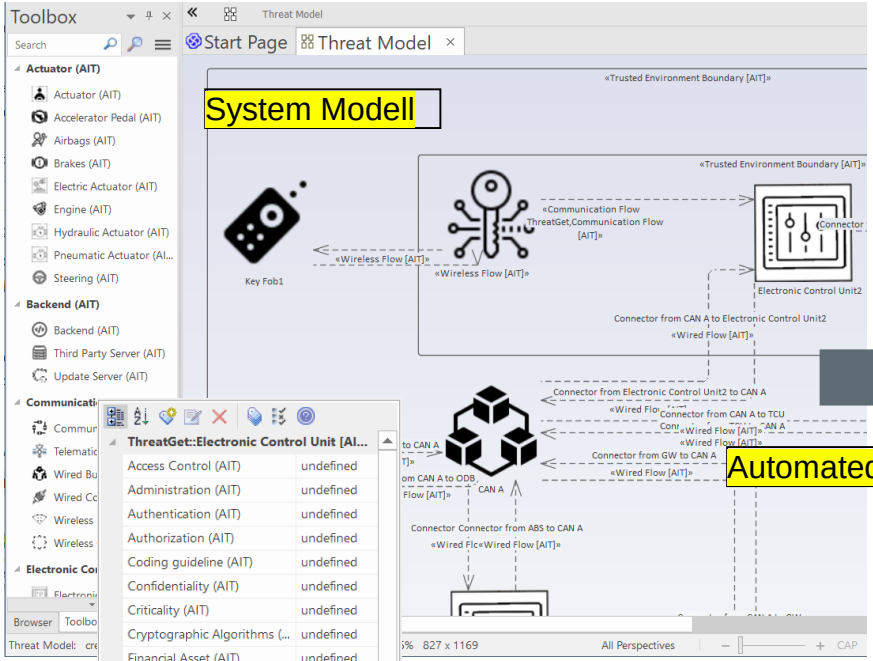
THREATGET



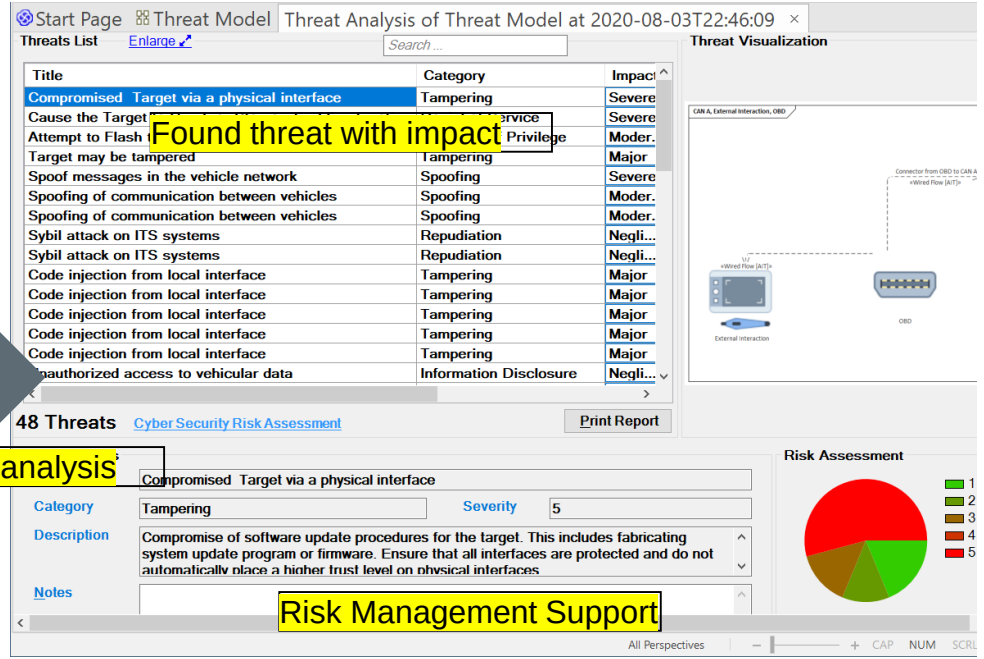
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY LieberLieber software gmbh

THREAT MODELLING WITH THREATGET

THREATGET



Security propertiesn



AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

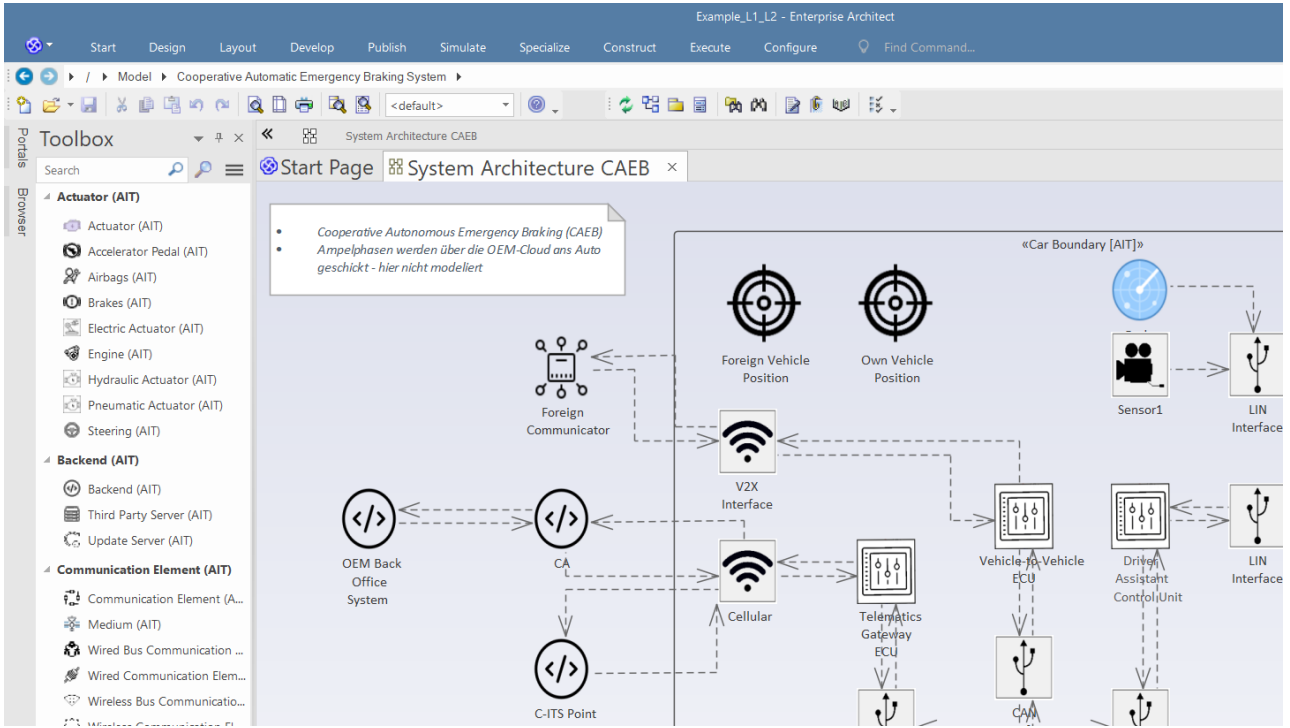
LieberLieber software gmbh

CONCLUSION

THREATGET FOR AUTOMOTIVE (ISO/SAE 21434, UNECE)

THREATGET

- Threat Catalog
  - UNECE
  - ETSI, ITU, ISO/SAE
  - AIT Analyses
  - Cont. Updates
- ISO/SAE compatible Workflow
  - Risik analysis
  - Reporting
- Extensible by user



AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
LieberLieber software gmbh

- Automated cybersecurity analysis of design
  - ✓ Avoidance of vulnerabilities and insecure architecture
- Supports system design and risk analysis according to ISO/SAE 21434
  - ✓ Complience with ISO/SAE 21434 becomes mandatory
- Knows current and future threats: Threat database updates
  - ✓ Easy verification of system already on the market

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY LieberLieber software gmbh

THANK YOU!

Contact us: orsolya.nemeth@sparxservices.eu