Threat Modeling for Automotive Security Analysis

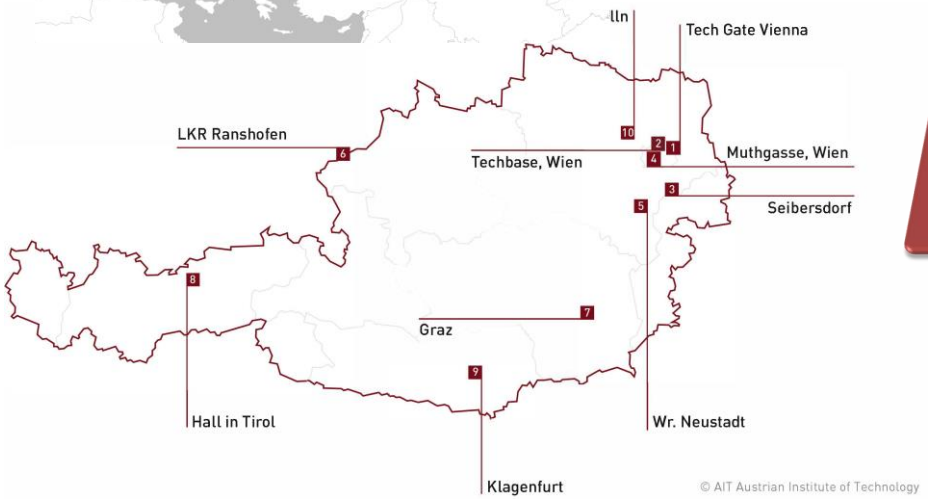
SecTech 2016, Jeju Island, Korea

Zhendong Ma and Christoph Schmittner

AIT Austrian Institute of Technology

Outline

- Security of modern vehicle/automotive CPS
- Automotive threat modeling
- PoC implementation
- Conclusion

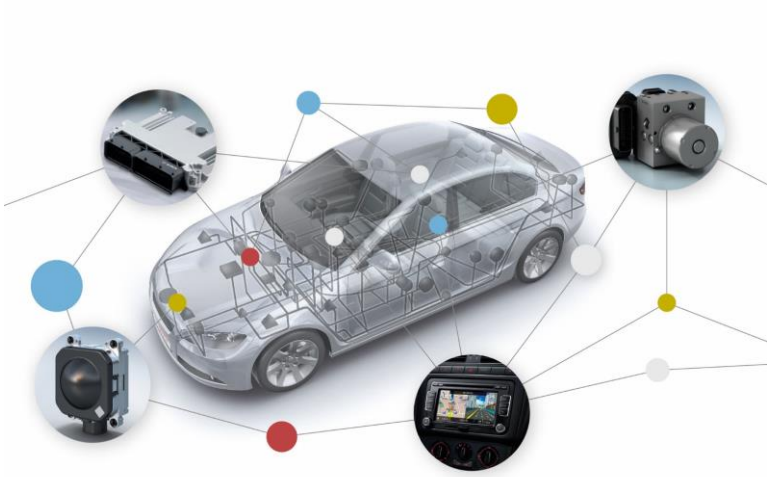

Tech Gate Vienna
LKR Ranshofen
Techbase, Wien
Muthgasse, Wien
Seibersdorf
Graz
Hall in Tirol
Wr. Neustadt
Klagenfurt
© AIT Austrian Institute of Technology

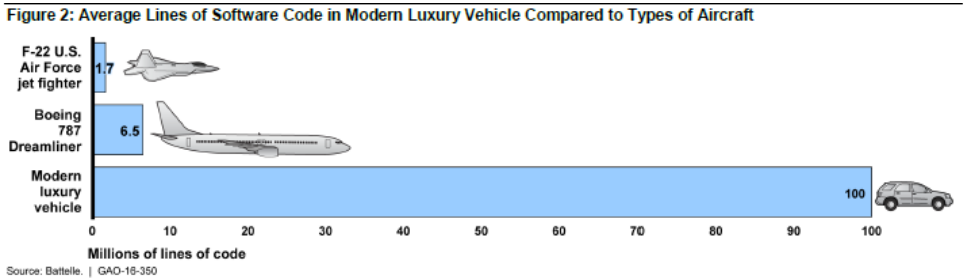

AIT Austrian Institute of Technology
Seibersdorf Labor GmbH
Nuclear Engineering Seibersdorf GmbH
Energy
Mobility
Digital Safety & Security
Health & Environment
Foresight & Policy Development


TECH GATE

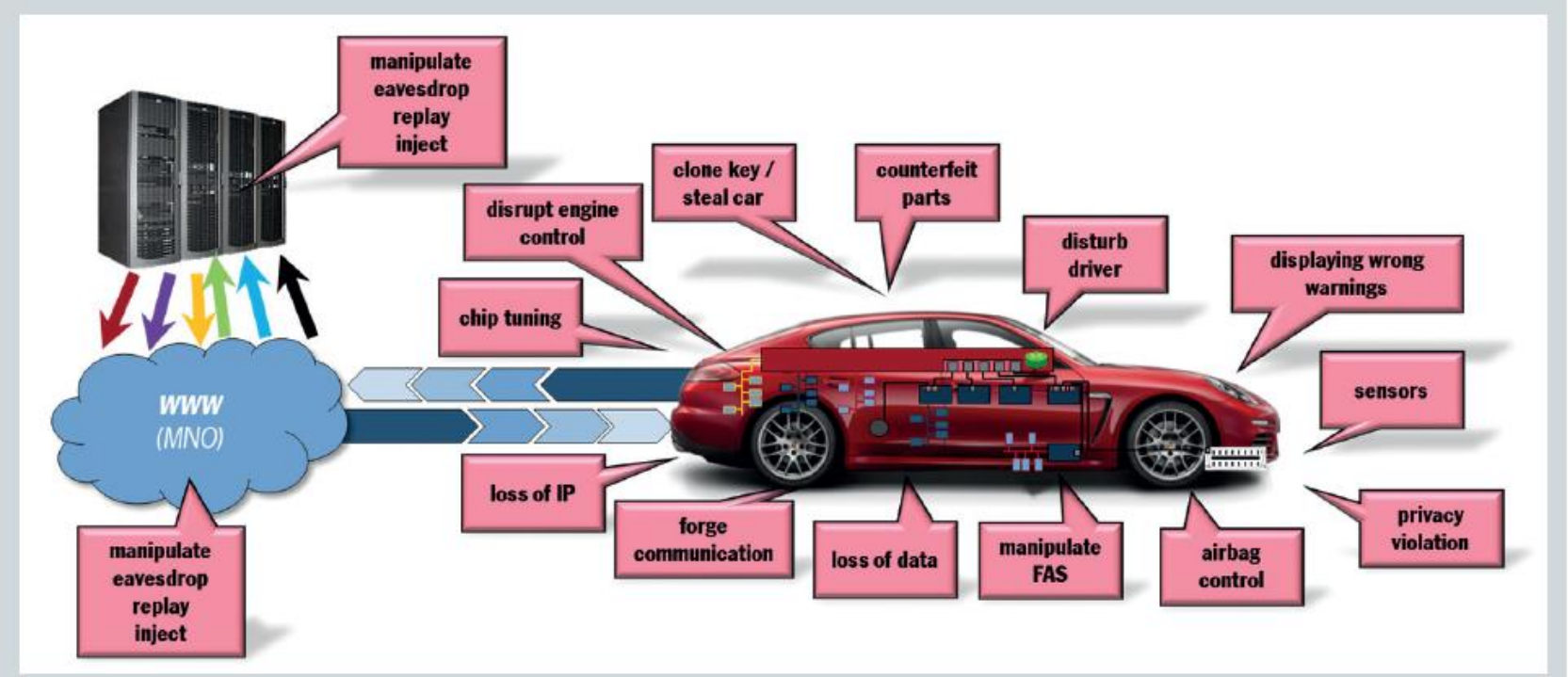
Security of automotive systems

- Vehicle systems are increasingly **open** and **connected** to user devices
- Critical vehicle functions getting **automated** and the driver is outside of the control loop
- **Cooperative** driving functions depend on trustworthiness of external data
- Security is a concern for safety
  - Adds new causes to existing hazards
  - Adds new hazards
- Privacy concerns

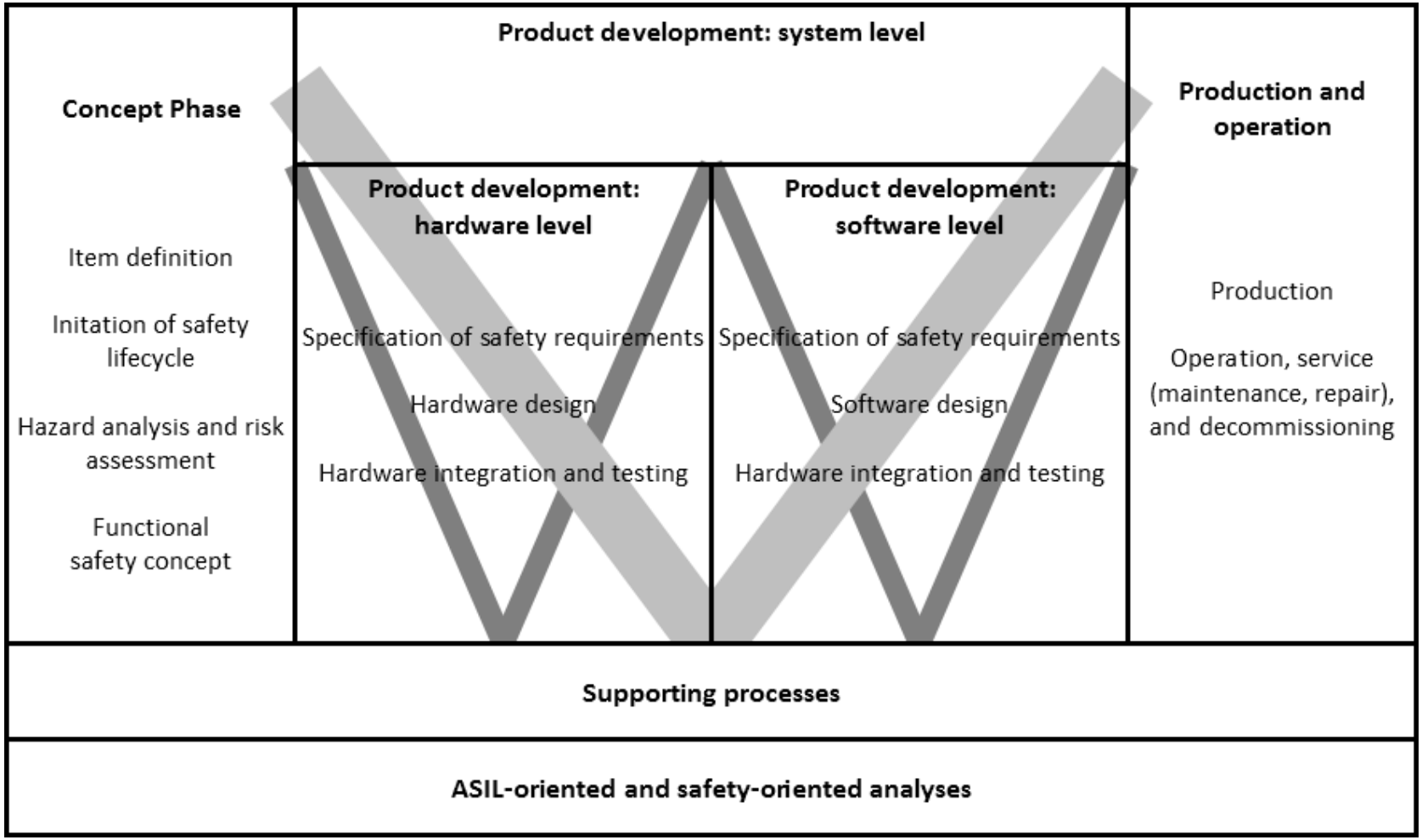




Automotive attack surface



ISO 26262 Road vehicles - Functional safety



SAE J3061Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

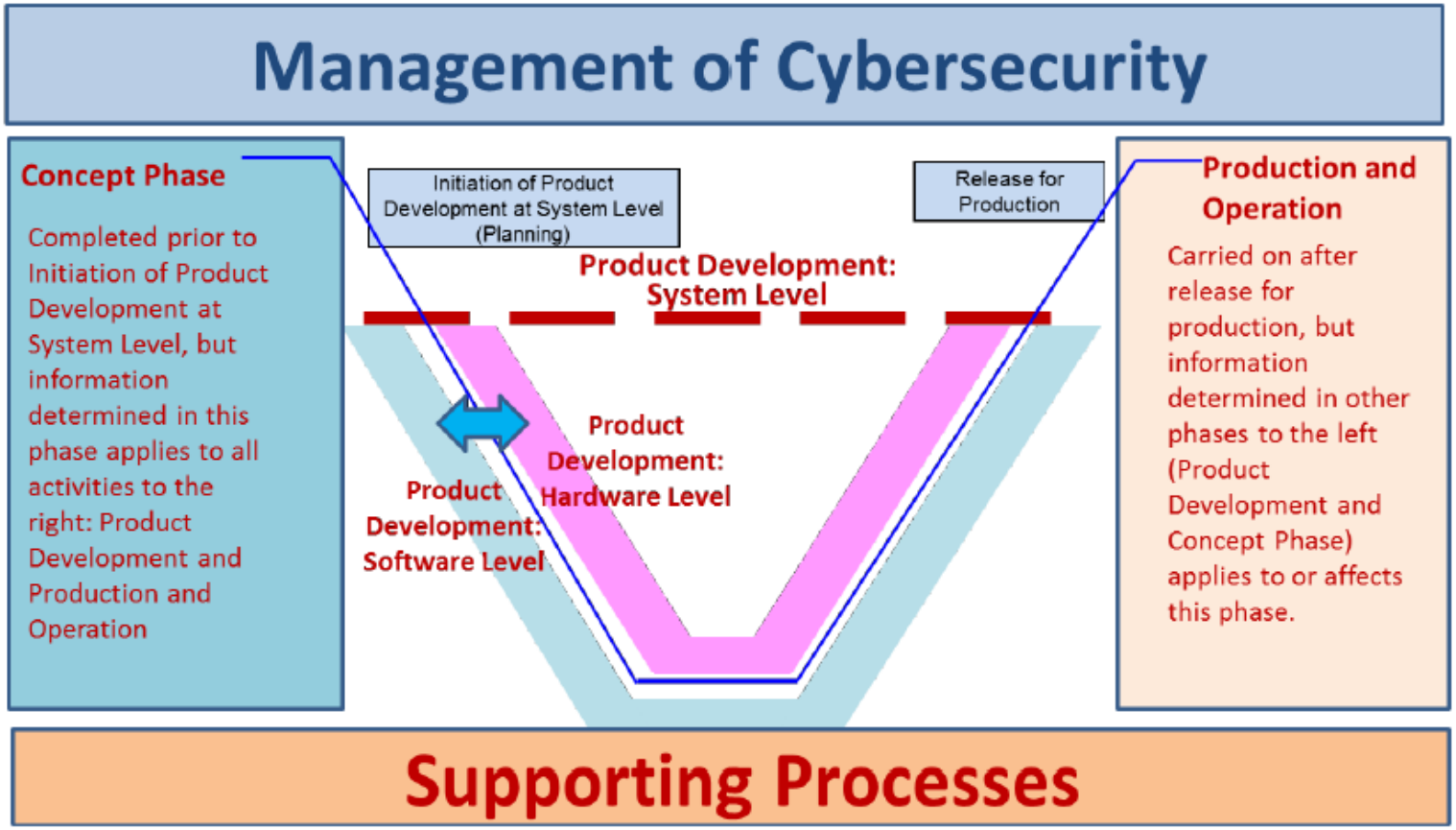


Figure 3 - Overall Cybersecurity process framework

TARA

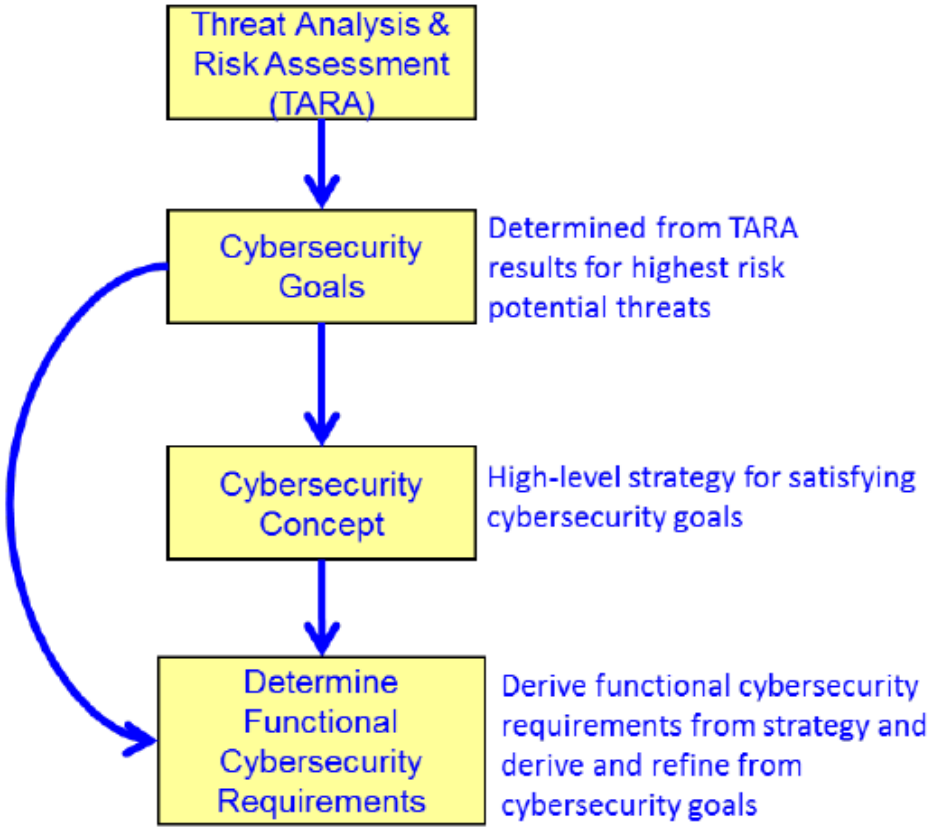
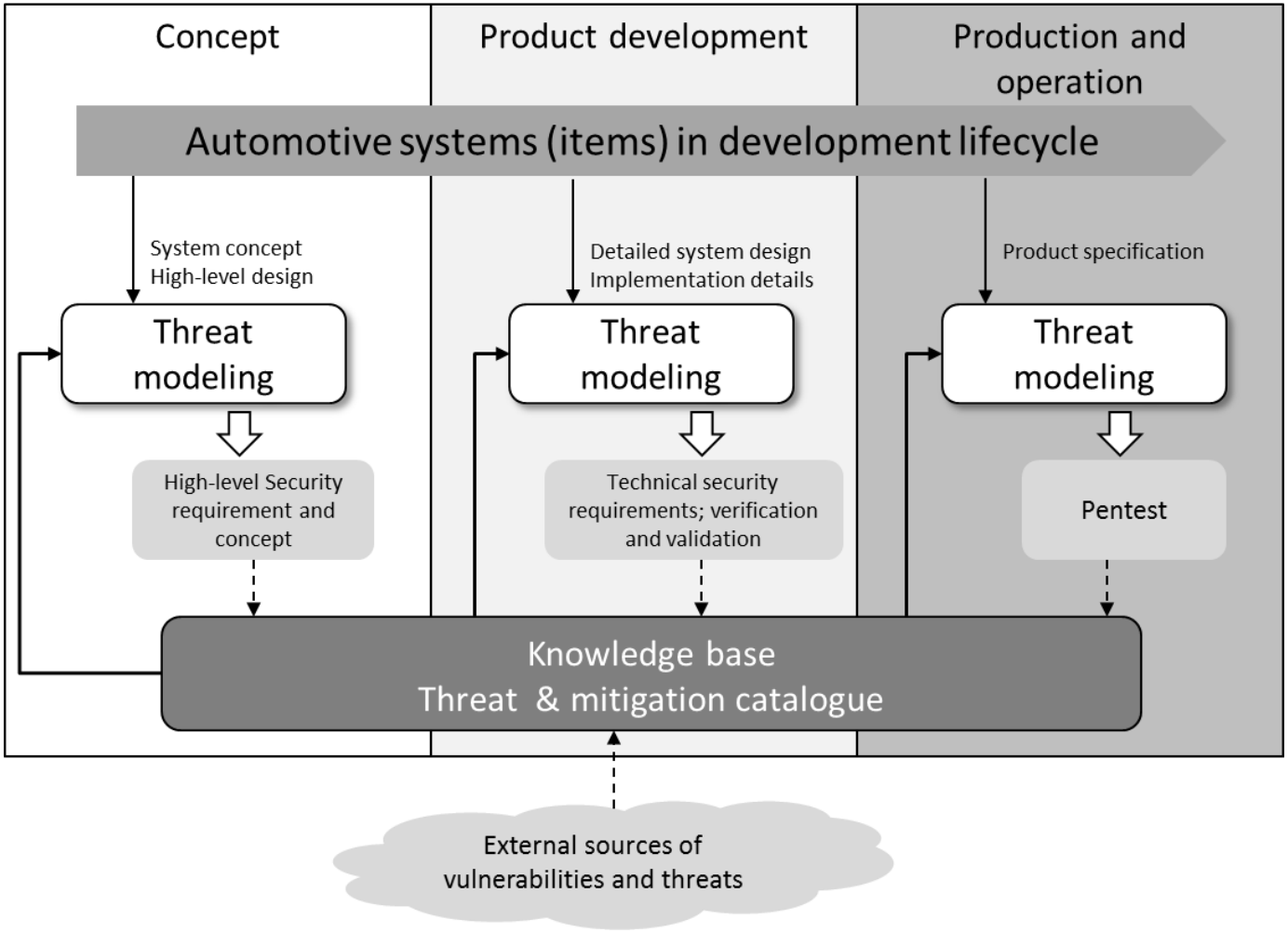


Figure 18 - Determining functional Cybersecurity requirements

Threat modeling

- Threat modeling: defining a theoretical model of perceived threats to a system.
  - Theoretical model should be as close as possible to the practical implementation to capture the significant attack vectors.
- How to model a system and its trust assumptions?
- How to model an adversary that captures its motivations, capabilities, and actions including its tactics, techniques, and procedures (TTP)?

Our proposal

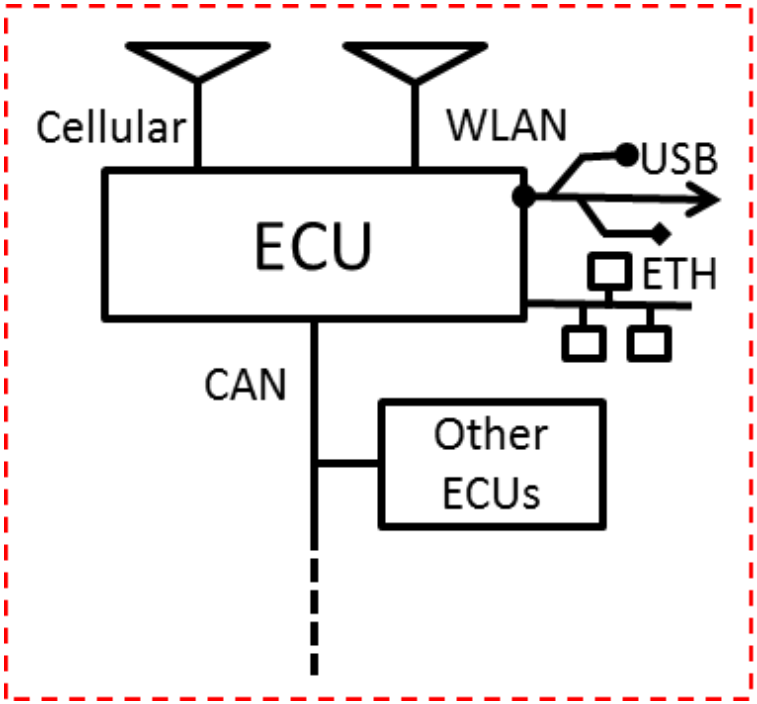


4 steps to automotive threat modeling

- Model a system by drawing the system architecture in Data-flow Diagram (DFD), adding system details to the elements in the DFD, and draw the trust boundaries.
- Identify threats stemmed from data flows by using a threat identification methodology such as STRIDE. An assessment of the severity of the threats can be added.
- Address each threat by redesigning the system, adding mitigation, or ignoring it if the risk is acceptable.
- Validate the threat modeling diagram against actual system and all identified threats are addressed.

Implementation

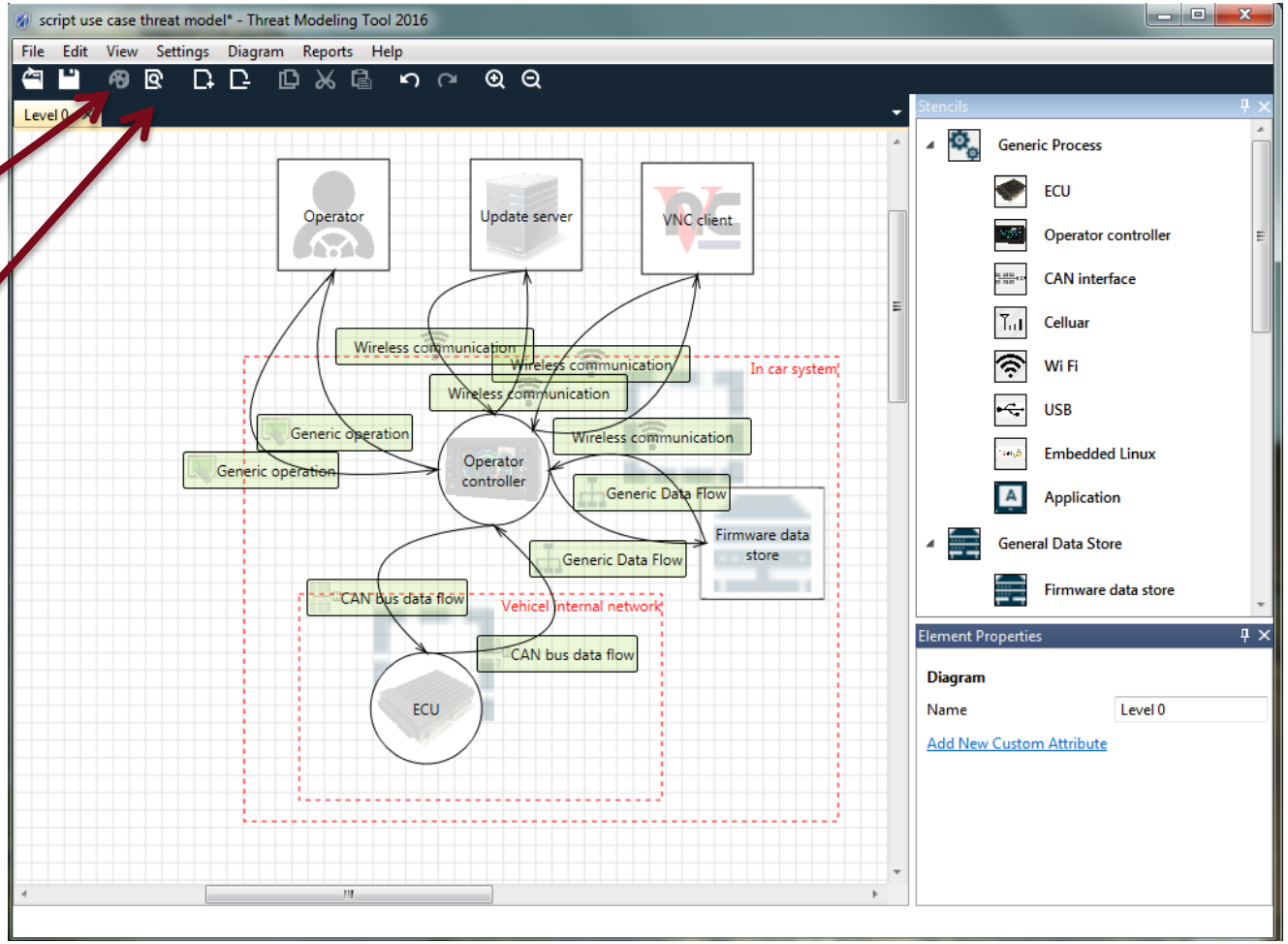
- Automotive ECU as a communication gateway
- Applications
  - Remote maintenance
  - Remote control similar as in cockpit
  - Over-the-Air update
- Based on an existing HMI module, which is extended with remote connectivity
- Used for off-road and duty vehicles
- Configuration of ECU may impact safety (different equipment limits depending on model)
- Configuration and software are important Intellectual Property
- Remote connection can influence operation



DFD

DFD view

Threat analysis view



Threats generated

Threat List

ID	Title	Category	Short Description	De	Interaction	Priority	Attack method	Attack motivation	Attack capability
6	Modify or tamper application program or datat on Operator controller	Integrity	Attack on Integrity		Wireless communication	High	Gain physical access to Operator controller	Manipulation of application...	Hackers with automotive expertise
7	Exploit known vulnerabilities in OS or applications remotely	Integrity	Attack on Integrity		Wireless communication	High		Compromise the device rem...	Well-organized and financed team with expe
8	MITM attack on communication between VNC client and Operator controller	Integrity	Attack on Integrity		Wireless communication	Medium		Tampering transmitted data	Hackers with automotive expertise
9	Tamper configuration data	Integrity	Attack on Integrity		Wireless communication	Low		Unintended sending of confi...	Hackers without automotive expertise
10	Sending bogus data which overload CPU resources for checking the updates	Availability	Attacks on availability		Wireless communication	Medium		Temporarily disabling the no...	Hackers without automotive expertise
11	MITM attack on communication between Operator controller and VNC client	Integrity	Attack on Integrity		Wireless communication	Medium		Tampering transmitted data	Hackers with automotive expertise
12	Modify or tamper application program or datat on Operator controller	Integrity	Attack on Integrity		Generic Data Flow	High	Gain physical access to Operator controller	Manipulation of application...	Hackers with automotive expertise
13	Exploit known vulnerabilities in OS or applications remotely	Integrity	Attack on Integrity		Generic Data Flow	H		Compromise the device rem...	Well-organized and financed team with expe
14	Sending bogus data which overload CPU resources for checking the updates	Availability	Attacks on availability		Generic Data Flow	Medium		Temporarily disabling the no...	Hackers without automotive expertise
15	Dumping software from Firmware data store	Confidentiality	Attack on confidentiality		Generic Data Flow	Low	gain physical access	Copy of propriety data (OS, c...	Hackers without automotive expertise
16	Sniff update transmitted in wireless network	Confidentiality	Attack on confidentiality		Wireless communication	High		Copy of propriety Data (OS, c...	Hackers without automotive expertise
17	Modify or tamper application program or datat on Operator controller	Integrity	Attack on Integrity		Wireless communication	High	Gain physical access to Operator controller	Manipulation of application...	Hackers with automotive expertise
18	Exploit known vulnerabilities in OS or applications remotely	Integrity	Attack on Integrity		Wireless communication	High		Compromise the device rem...	Well-organized and financed team with expe
19	Compromise update server	Integrity	Attack on Integrity		Wireless communication	Medium	Compromise the call		Hackers with automotive expertise
20	MITM attack on communication between Update server and Operator controller	Integrity	Attack on Integrity		Wireless communication	Medium		Tampering transmitted data	Hackers with automotive expertise
21	Sending bogus data which overload CPU resources for checking the updates	Availability	Attacks on availability		Wireless communication	Medium		Temporarily disabling the no...	Hackers without automotive expertise
22	MITM attack on communication between Operator controller and Update server	Integrity	Attack on Integrity		Wireless communication	Medium		Tampering transmitted data	Hackers with automotive expertise
23	Modify or tamper application program or datat on Operator controller	Integrity	Attack on Integrity		CAN bus data flow	High	Gain physical access to Operator controller	Manipulation of application...	Hackers with automotive expertise
24	Exploit known vulnerabilities in OS or applications remotely	Integrity	Attack on Integrity		CAN bus data flow	High		Compromise the device rem...	Well-organized and financed team with expe
25	Sending bogus data which overload CPU resources for checking the updates	Availability	Attacks on availability		CAN bus data flow	Medium		Temporarily disabling the no...	Hackers without automotive expertise

20 Threats Displayed, 20 Total

TARA: threat analysis

Integrity

Availability

Confidentiality

Confidentiality

Confidentiality

Integrity

Attack scenario	Threat	Effect	Attack prob.	Severity	Risks
Asset: Software/Applications					
Exploit known vulnerabilities in OS or applications remotely	Install rootkit, Trojan	Take control of system ECU operations, change parameters, and access data	9 (2+1+3+3)	4	High
Exploit known vulnerabilities in OS or applications remotely	Delete software component	Reduce functionality of ECU	9 (2+1+3+3)	2	Medium
Asset: Remote control functions					
Man-in-the-middle attack on communication	Eavesdropping password used for remote connection	Hijack established connection and disturb normal operation	8 (1+1+3+3)	2	Medium
Brute force or guess remote connection password	Reveal password	Exploit remote connectivity to disturb normal operation	7 (1+2+2+2)	2	Medium
Asset: Remote maintenance functions					
Compromise and control a device in the communication link between ECU and Web server	Eavesdrop communication to intercept maintenance data	Intercept sensitive configuration and maintenance data	7 (1+2+2+2)	3	Medium
Man-in-the-middle attack on communication	Send manipulated maintenance data to Web server	Cause unnecessary maintenance actions by sending crafted maintenance data	8 (1+1+3+3)	1	Low

Conclusion

- Threat modeling – an effective and practical tool for security analys in automotive development lifecycle
- Efficiency, accuracy, and repeatability
- Future work
  - Build up threat database
  - Connect DFD with SysML

AIT Austrian Institute of Technology

your ingenious partner

Zhendong Ma
Zhendong.ma(at)ait.ac.at