Hochschule Karlsruhe
University of
Applied Sciences

Institute for
Energy Efficient Mobility

Attack Path Generation Based on Attack and Penetration Testing Knowledge

Prof. Dr.-Ing. Reiner Kriesten (reiner.kriesten@h-ka.de)
Florian Sommer, M.Sc. (florian.sommer@h-ka.de)

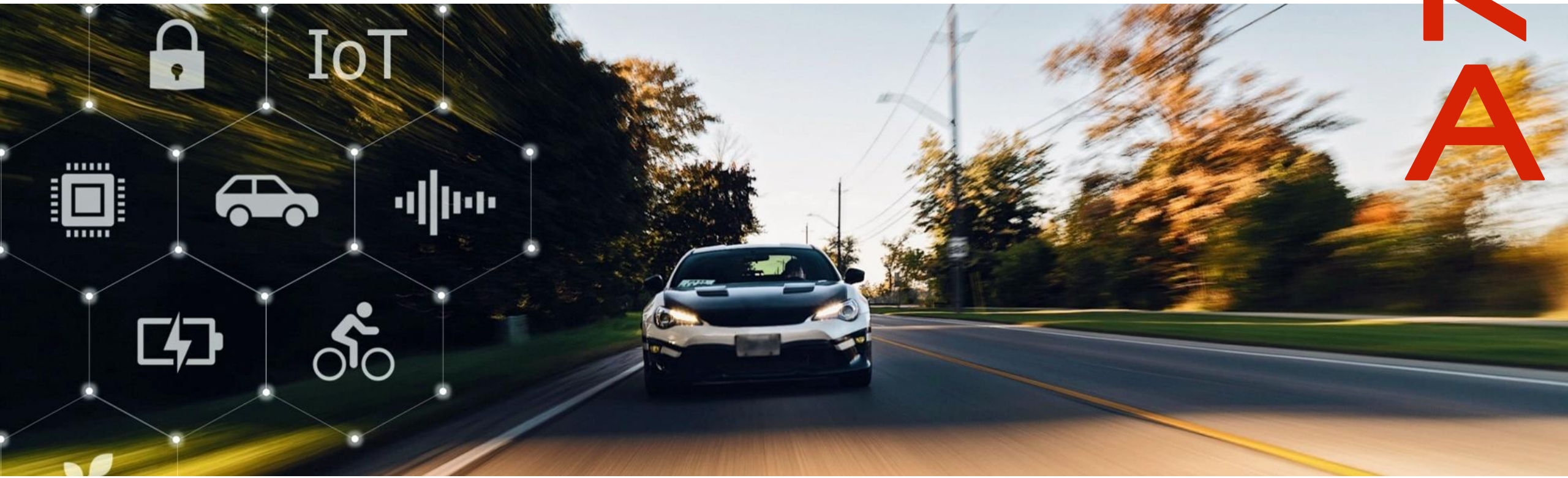


Foto: Qijin Xu / Unsplash

Resume: Reiner Kriesten

- Since 2009: Professor at Karlsruhe University of Applied Sciences
- Since 2012: Chair Institute of Energy Efficient Mobility
- Since 2013: Academic Dean of Master's program Automotive Systems Engineering

University Activities

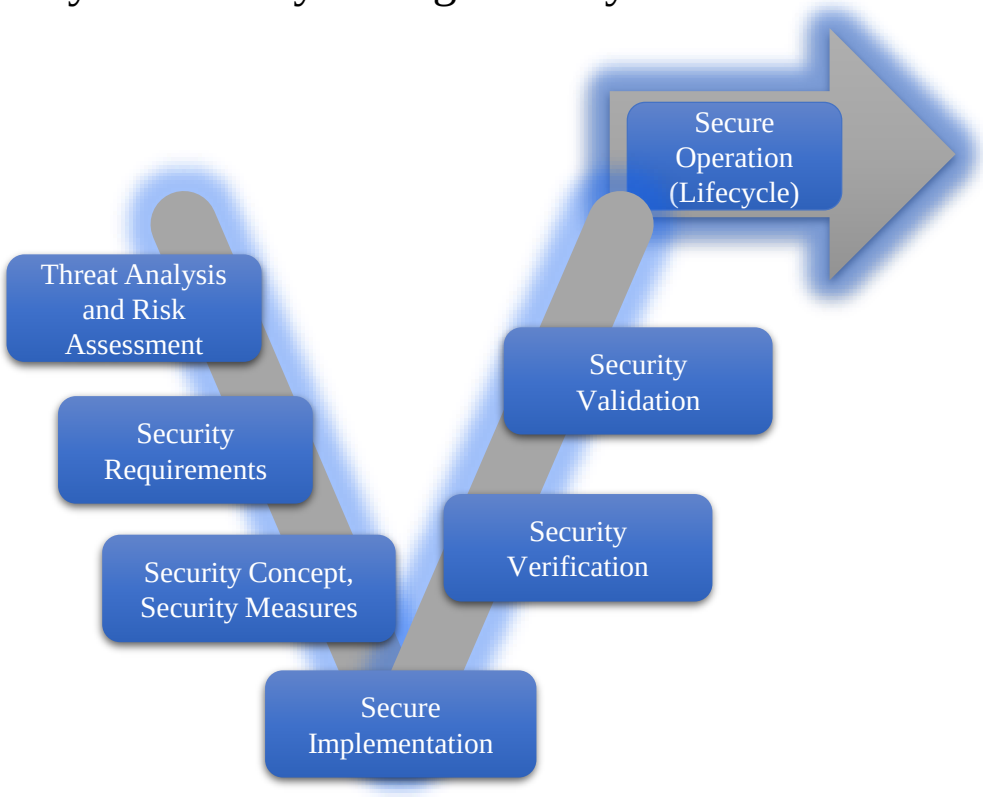
- Lectures
- Supervision of Bachelor and Master Theses
- Supervision of PhD Theses

Research

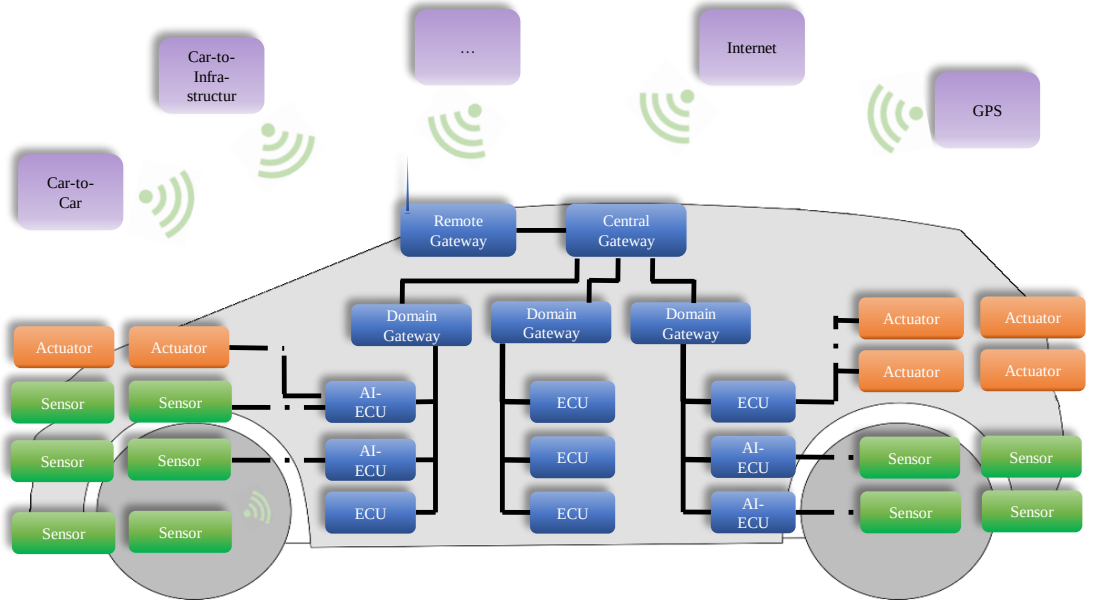
- Systems and software engineering of embedded systems
- Security of Cyber Physical Systems (CPS)

Automotive Security

- ISO/SAE 21434:2021 Road Vehicles – Cybersecurity Engineering
- UN Regulation No. 155 – Cyber security and cyber security management system

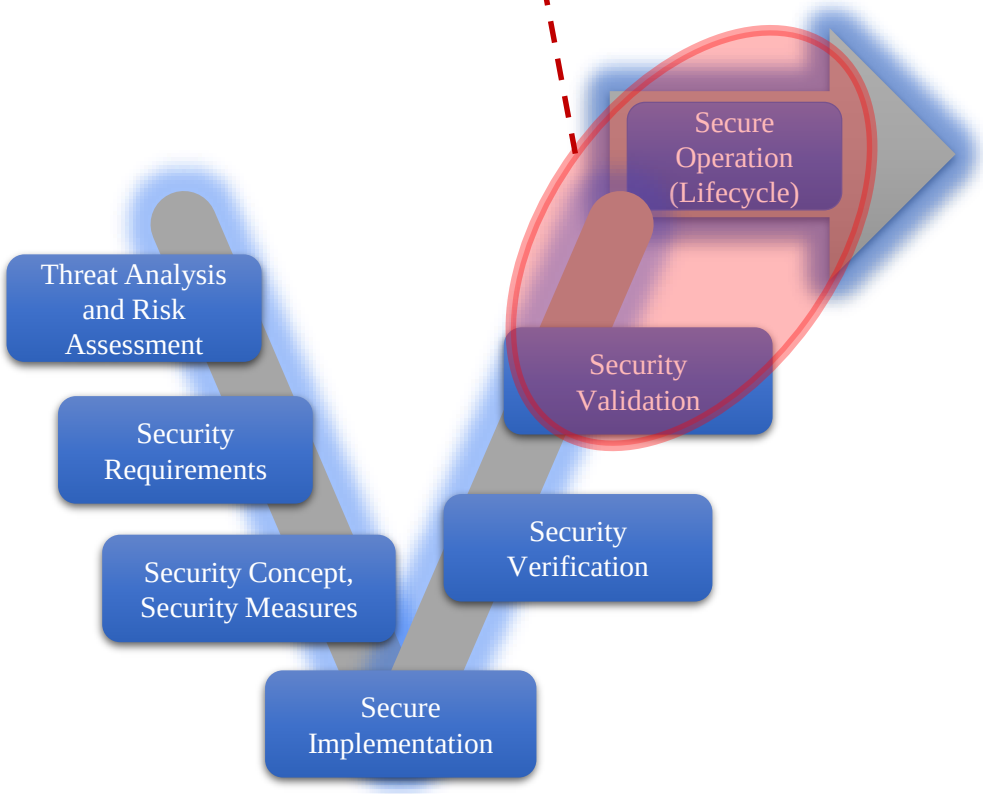


Connected and autonomous vehicles
→Highly complex system of systems



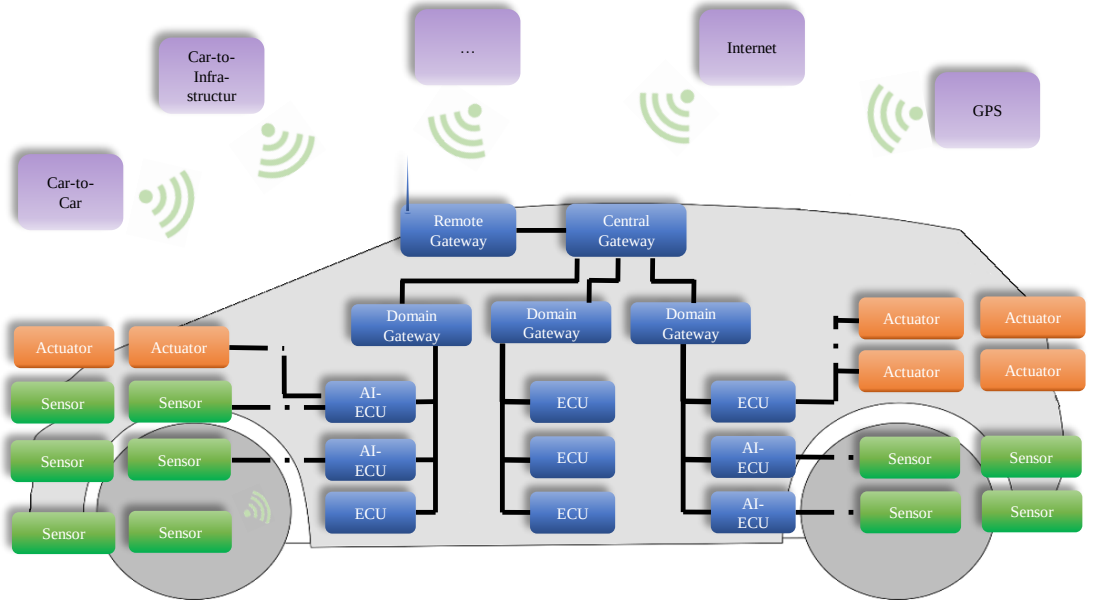
Automotive Security

Security Testing mainly applied at late stages of development



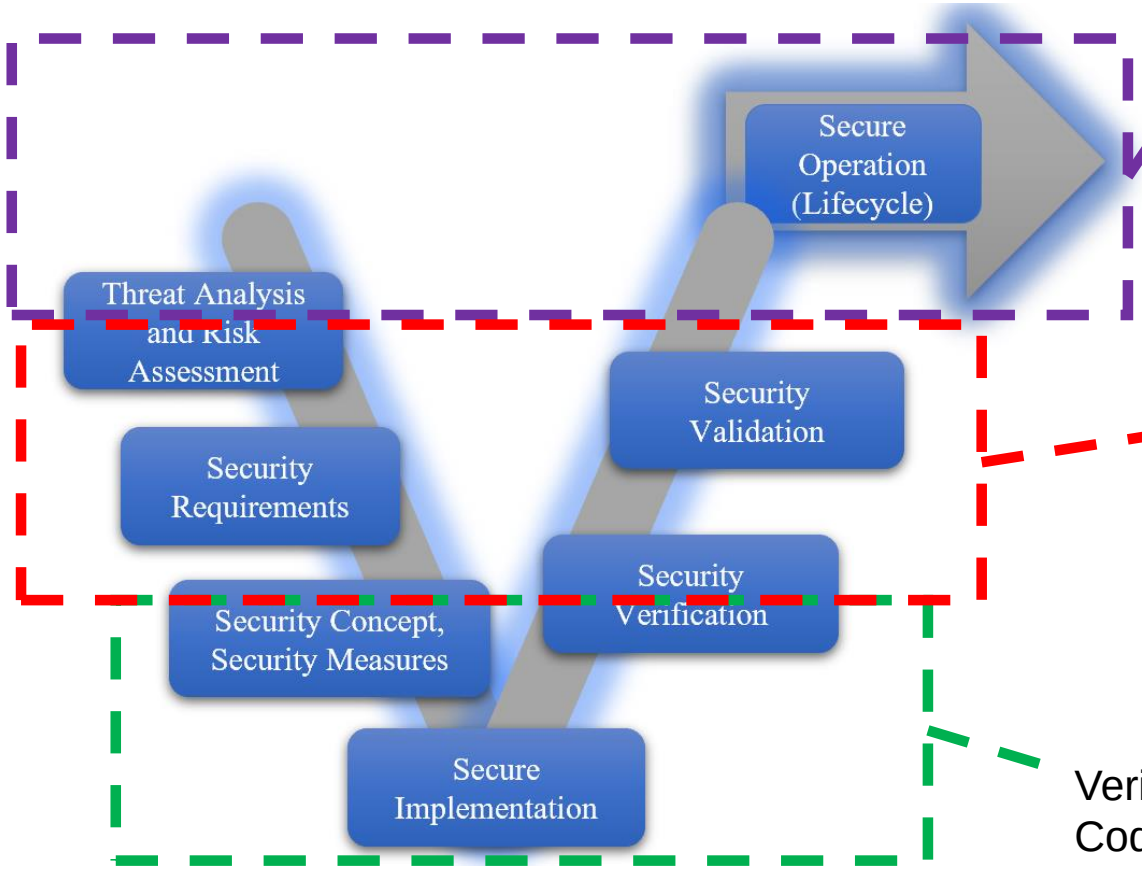
vs.

- High number of components
- High degree of communication
- High degree of data processing



Automotive Security

A deeper look in security testing



Penetration Testing,
Fuzzing,
Vulnerability Scanning

Goal:: Finding of residual vulnerabilities

Goal:: Validation - is the correct system realized ?

Goal:: Verification - is the system correct realized ?

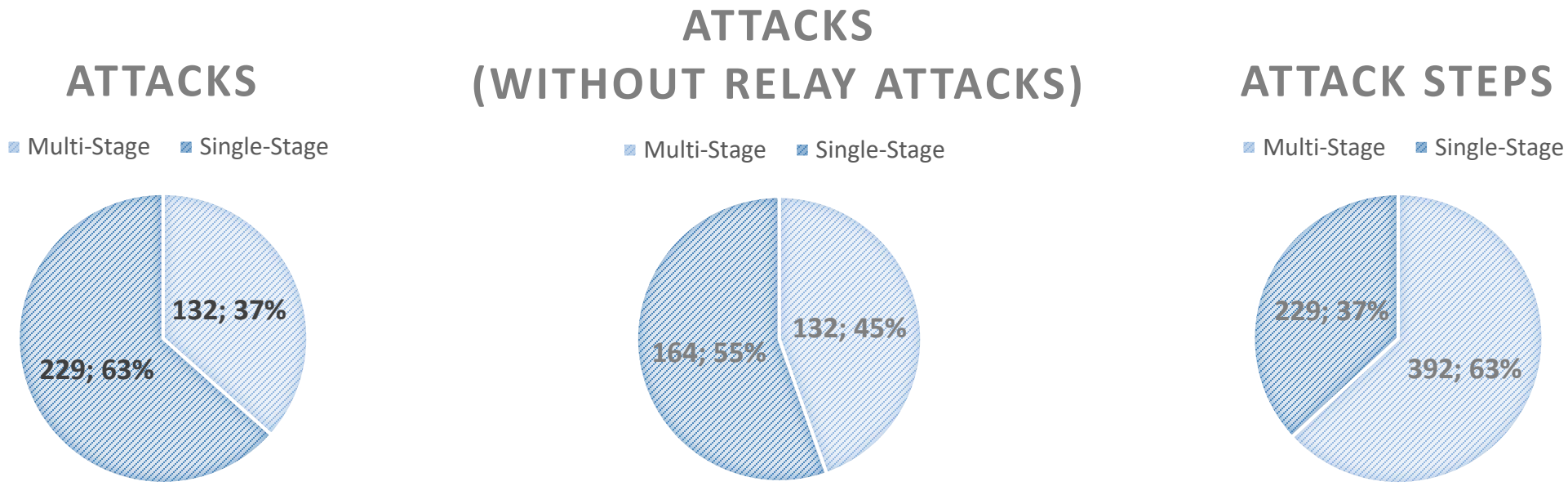
Verifying Security Measures,
Code Analysis

Automotive Security

What about multi-stage attacks?

–“Single functional requirements testing” does not stress out possible “vulnerability chains” which might exist

–Importance of multi-stage attacks?



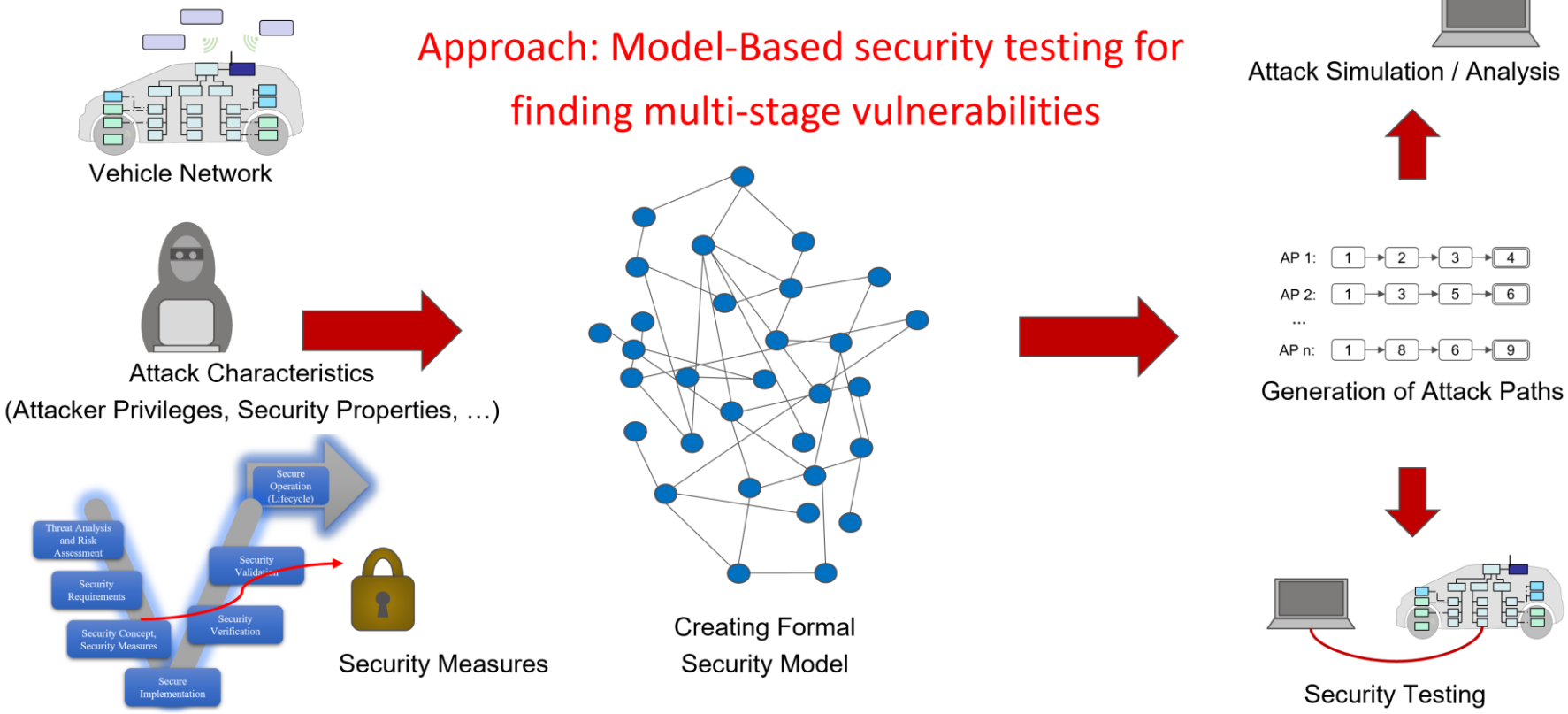
–So: how can we detect vulnerability chains in a system which might be exploited?

–Quality rating of security testing without vulnerability chain analysis?

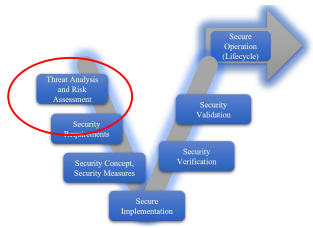
Automotive Security

Approach:

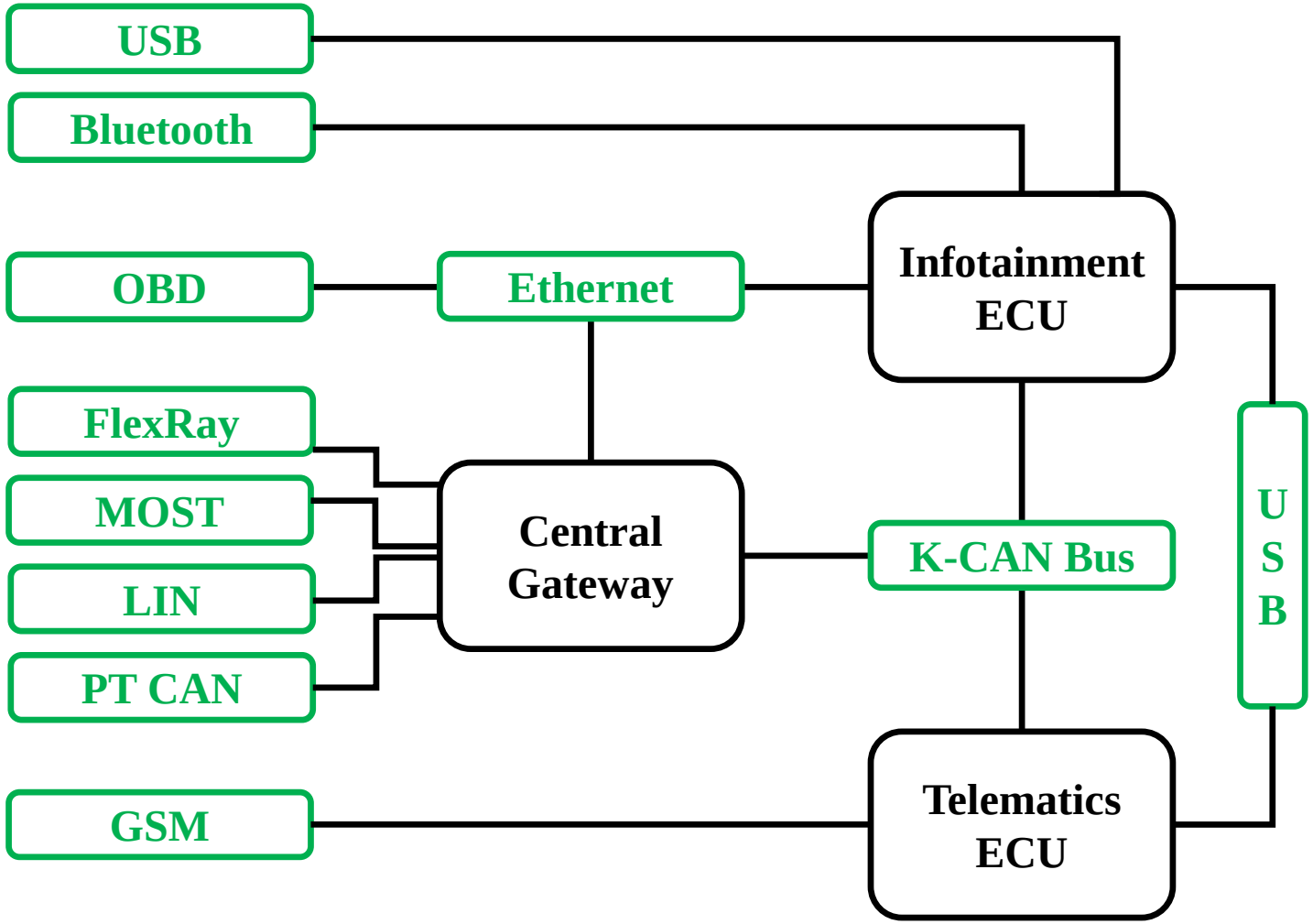
1. Move test activities to left side of V- Model via Model-Based Approach for Security Testing
2. Focus on multi-step attacks, see next slides
3. Find security attack paths automatically based on attack database
4. Fill database with new validated paths / restart



Automotive Security



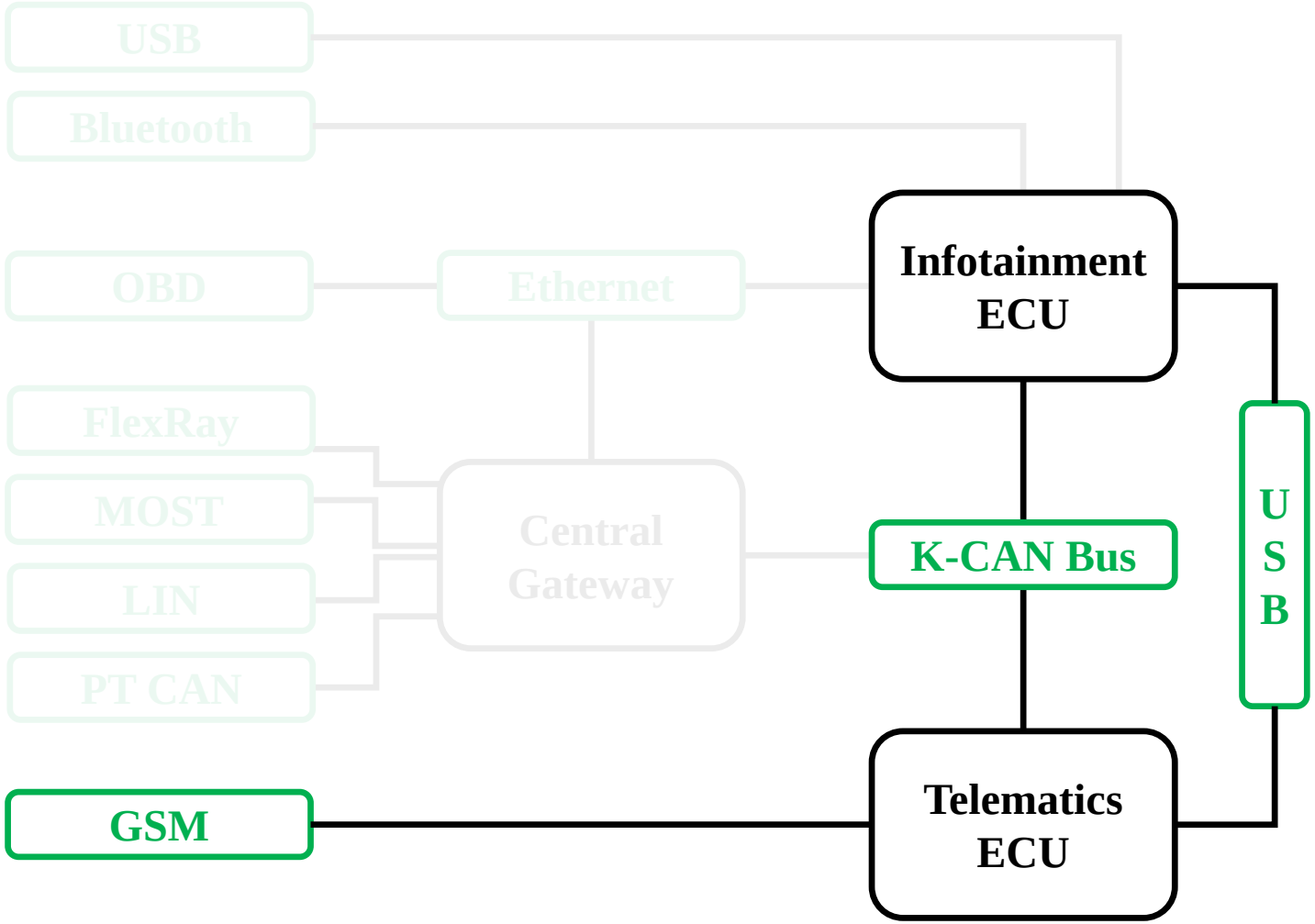
Security Model – Step 1: E/E architecture



Keen Security Lab, “Experimental security assessment of bmw cars: A summary report,” 2017. Available: https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars by_KeenLab.pdf

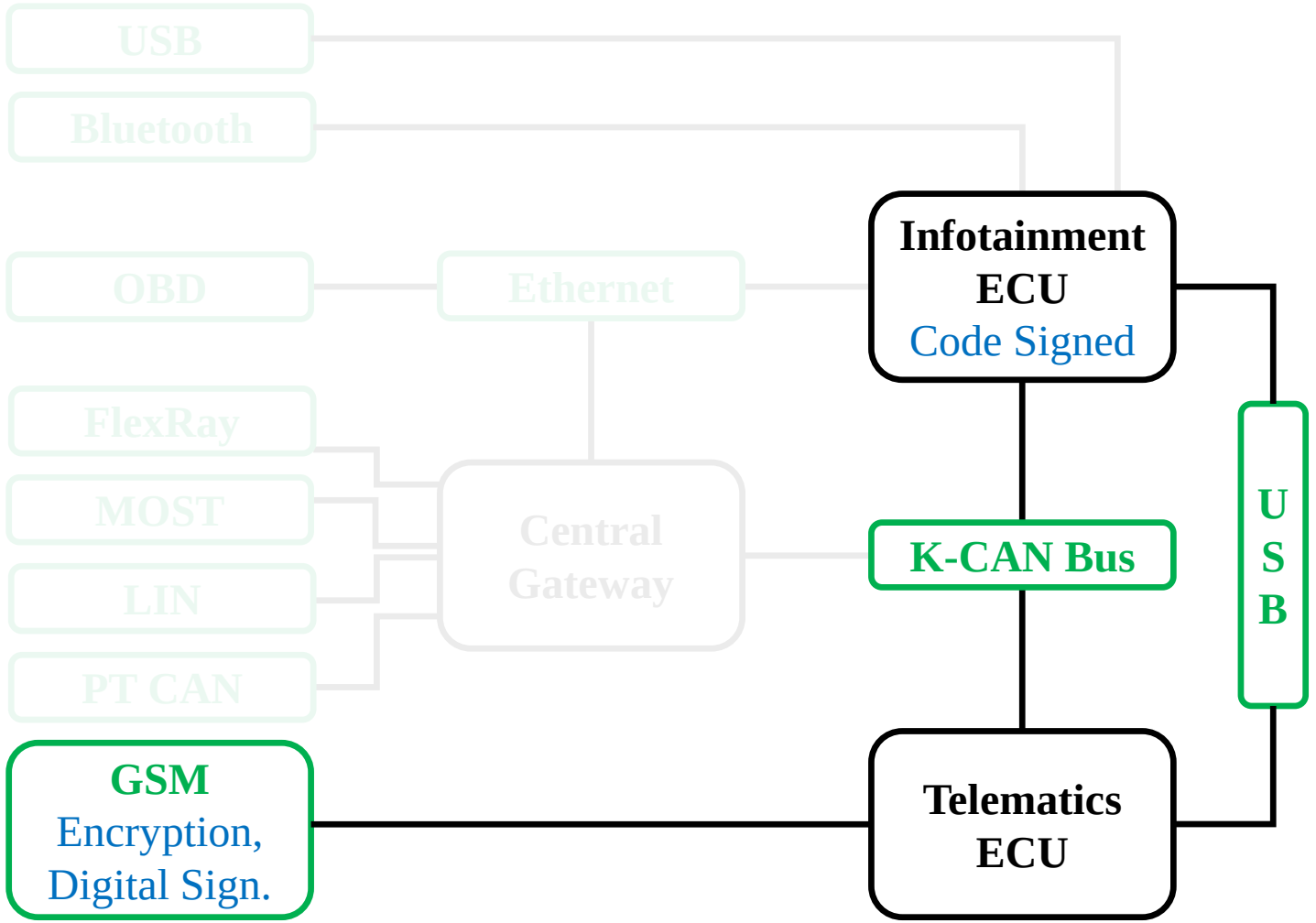
Automotive Security

Security Model – Step 1: E/E architecture



Automotive Security

Security Model – Step 2: Security Measures



Automotive Security

Vul(Step1):

- **Acquired Privilege:** Read/Write
- **Violated Security Property:** Confidentiality and authentication
- **Exploit:** Bypassing encryption/signature algorithms and establishing a GSM network to access remote services offered by the Telematics unit.

Vul(Step2a):

- **Acquired Privilege:** Full Control
- **Violated Security Property:** Authorization
- **Exploit:** No access control implemented on the Telematics ECU, so attackers are authorized users while sending valid GSM messages.

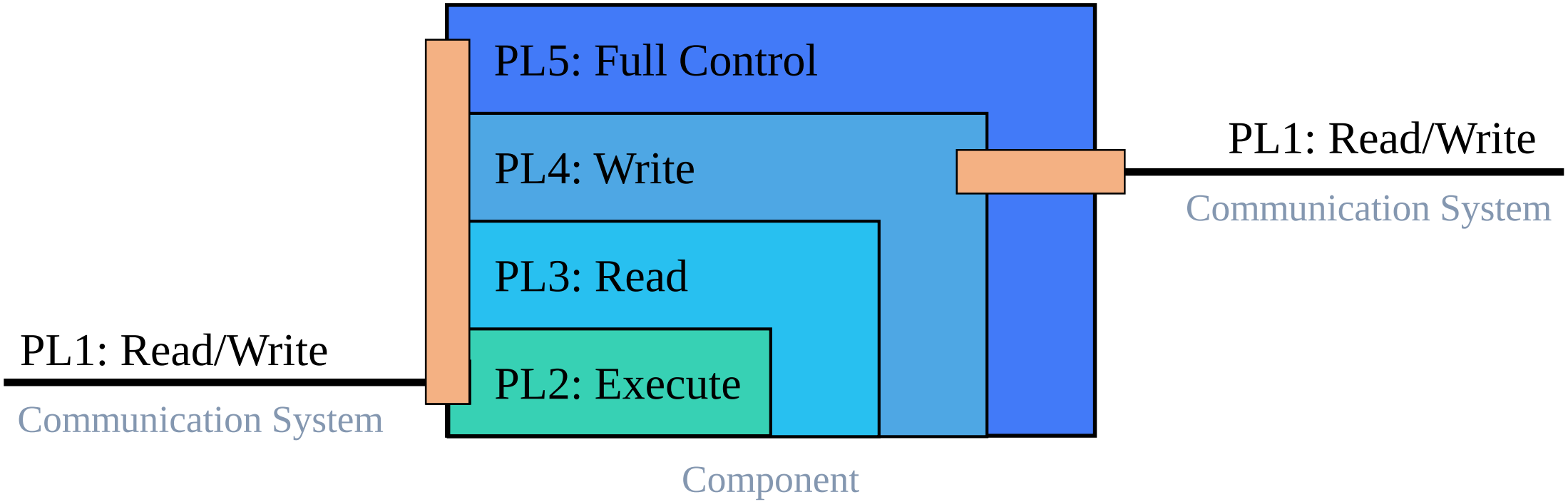
Vul(Step3a):

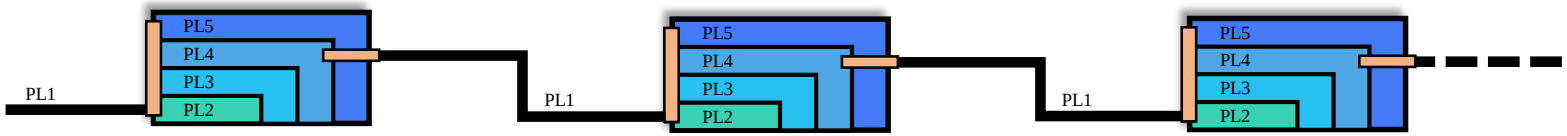
- **Acquired Privilege:** Read/Write
- **Violated Security Property:** Authentication
- **Exploit:** Sending valid messages from Telematics the USB channel.

Vul(Step4a):

- **Acquired Privilege:** Full Control
- **Violated Security Property:** Integrity
- **Exploit:** Exploiting a memory vulnerability in the Infotainment's in-vehicle browser.

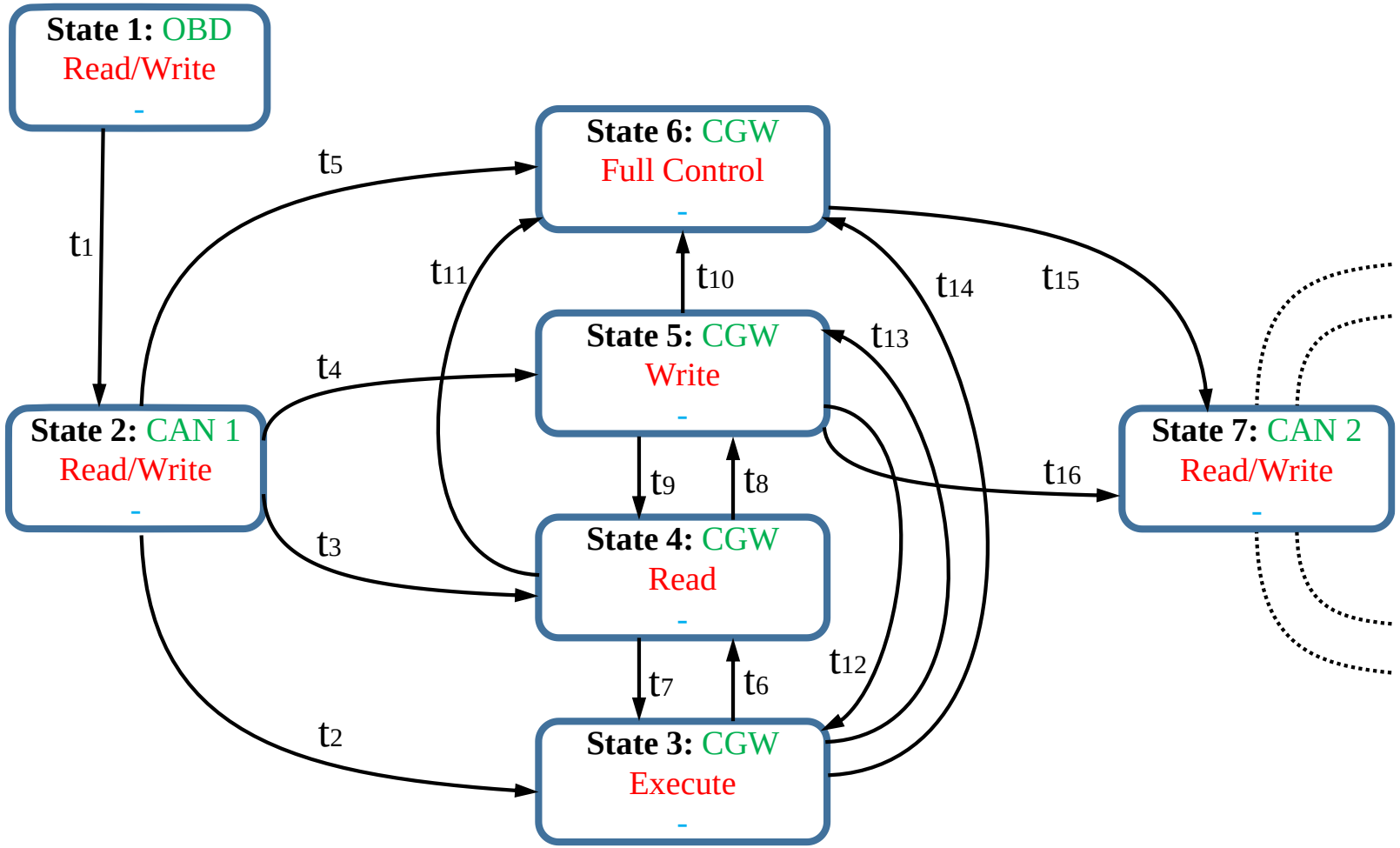
Attacker Privileges





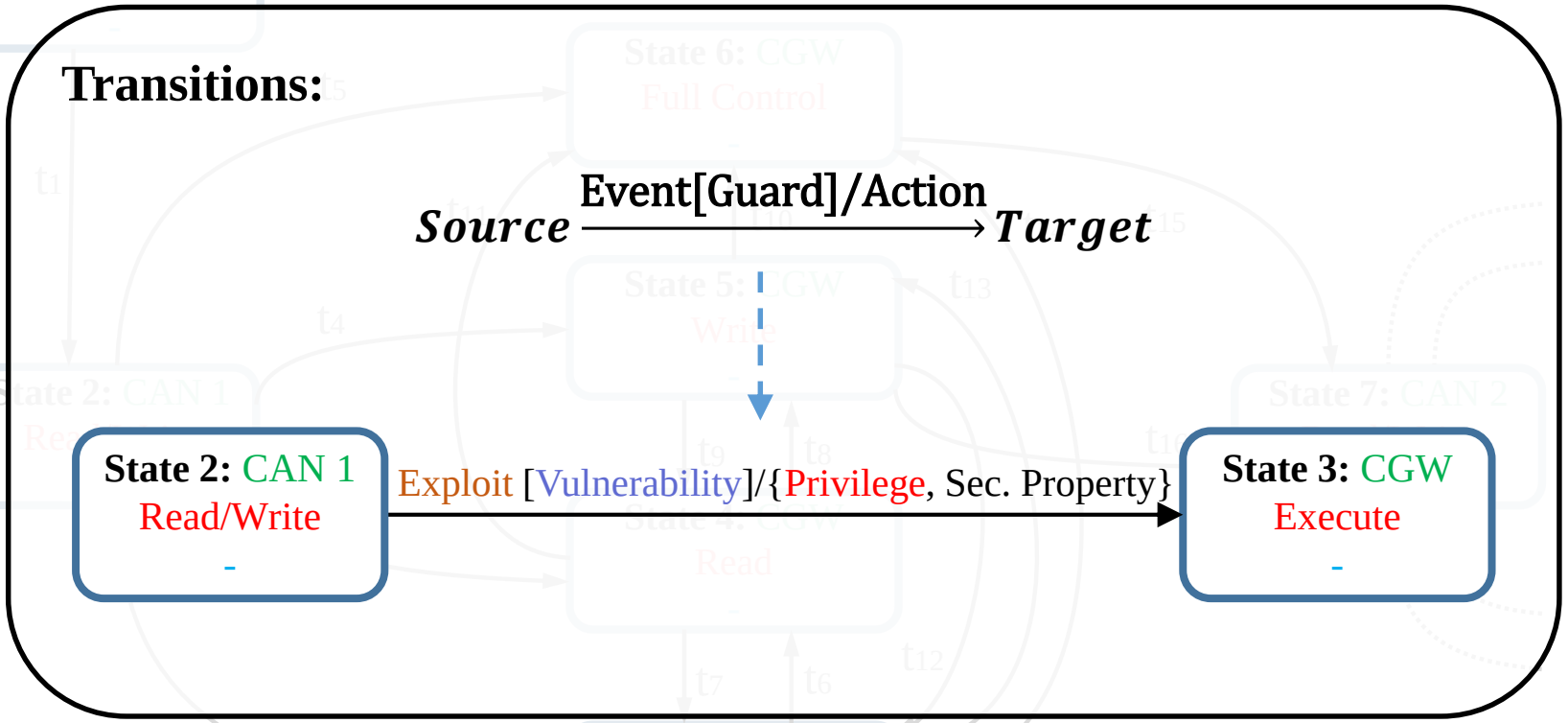
J. Dürrwang, F. Sommer, and R. Kriesten, “Automation in automotive security by using attacker privileges,” Proceedings 19th escar Europe 2021.

Formal Security Model



- Formal Model: Extended Finite State Machine (EFSM)
- States contain E/E architecture components and related attacker privileges
- Transitions contain attacks and exploited vulnerabilities

Formal Security Model



- Events represented by exploits
- Guard condition represented by vulnerabilities
- Actions represented by acquired attack privilege and violated security property

Attack Characteristics

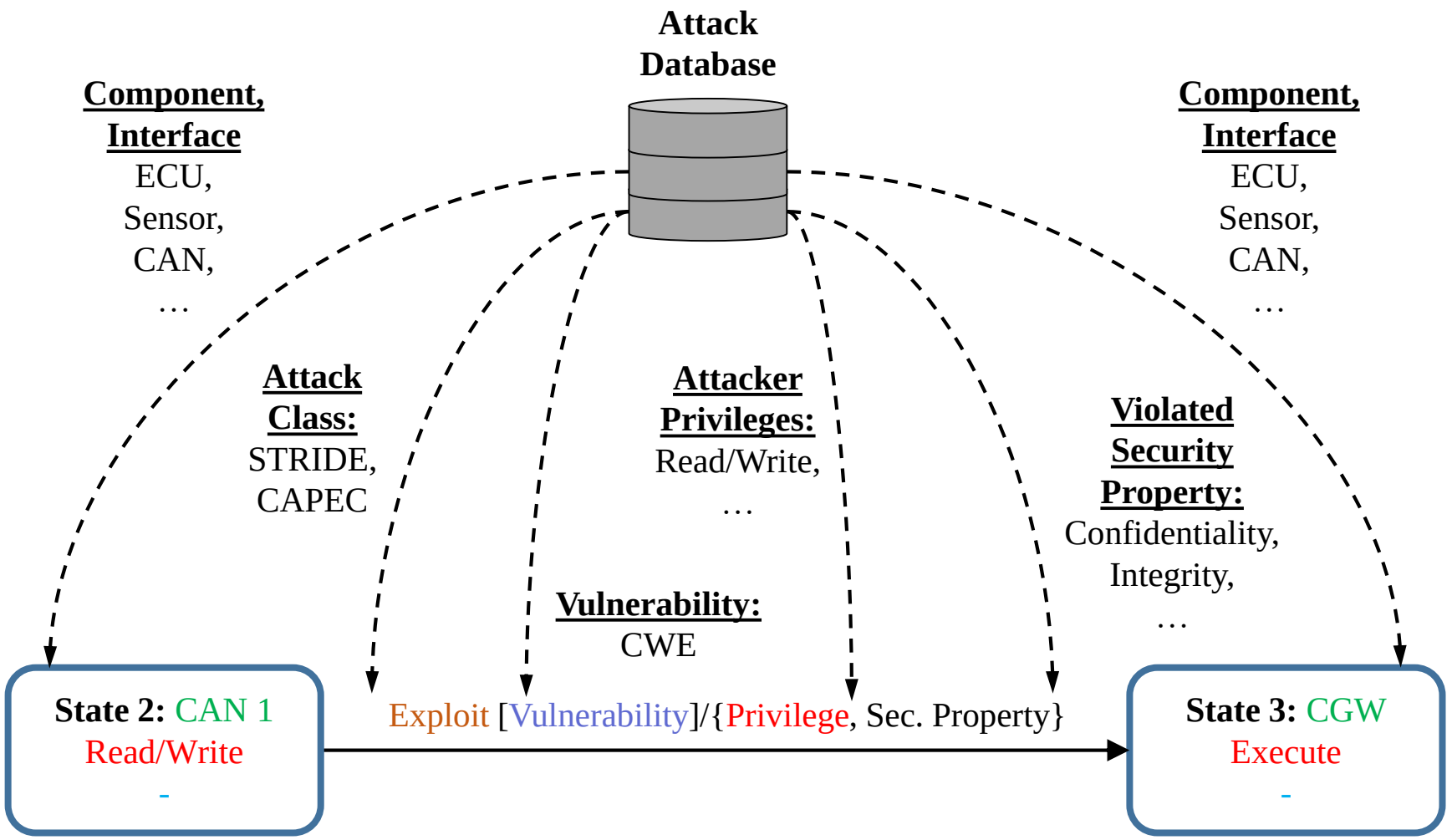
361 published attacks classified by our attack taxonomy and separated into their individual steps (621 steps). (Automotive Attack Database: https://github.com/IEEM-HsKA/AAD)

Category	Level 1	Level 2	Level 3
Description	Unauthorized flashing of malicious code on the engine ECU by using the diagnostic reprogramming routine		
Reference	Adventures in Automotive Networks and Control Units (C. Valasek et al.)		
Year	2013		
Attack Class	Tampering	Firmware Modification	None
Attack Base	Diagnostic Attack		
Attack Type	Real Attack		
Violated Security Property	Integrity		
Affected Asset	Information Security		
Vulnerability	CWE-693: Protection Mechanism Failure	CWE-287: Improper Authentication	Unauthorized reprogramming possible
Interface	OBD		
Consequence	Flashing of malicious code on ECU		
Attack Path	Downloading a new calibration update for ECU from manufacturer and Reverse Engineering of the Toyota Update Calibration Wizard (CUW). Monitoring the update process. Reverse Engineering update algorithm for calibration updates. Modification of calibration update. Reflashing of malicious update.		
Requirement	Required Access/Connection	OBD	None

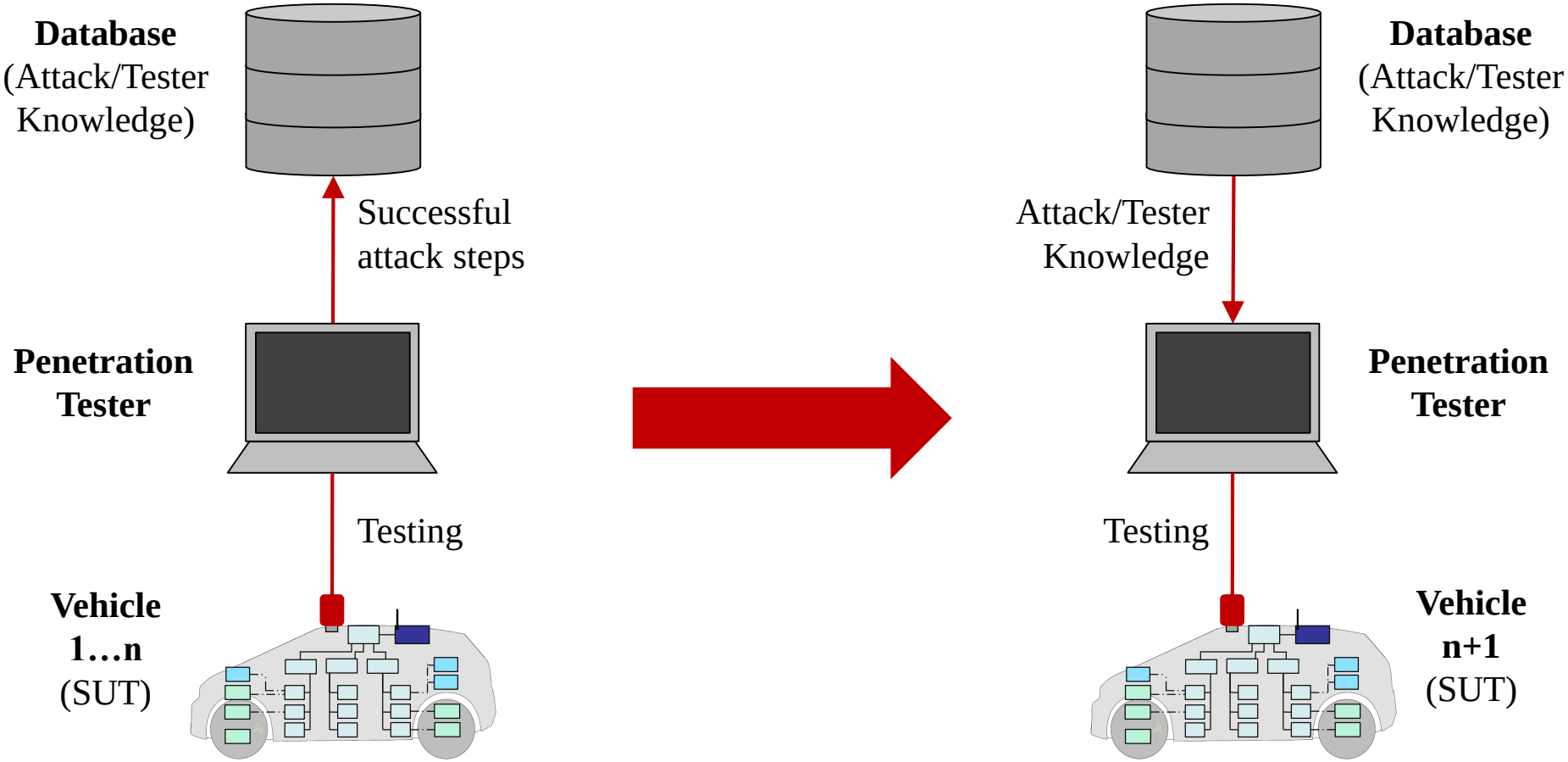
Restriction	Security Feature	Access Control	Security Layer which is tied to the Calibration Version and allows only one time overwriting
Attack Level	Local Network		
Acquired Privileges	Full Control (Functional Component)		
Vehicle	Toyota Prius (Year of Construction: 2010)		
Component	Engine ECU	Engine Control Module	2 CPUs, NEC v850, Renesas M16/C
Tool	Software Tool	Vehicle Diagnostic Software	Toyota Calibration Update Wizard (CUW)
	Hardware Tool	Interface	J2534 PassThru Device (CarDAQPlus)
	Hardware Tool	Interface	ECOM cable
	Hardware Tool	Laptop/PC	Windows PC
	Software Tool	Communication Tool	EcomCat Application
Attack Motivation	Security Evaluation		
Entry in Vulnerability Database	None		
Rating	CVSS: 6,8		
Exploitability	CVSS Exploitability: 1,62		

F. Sommer, J. Dürrwang, R. Kriesten: Survey and Classification of Automotive Security Attacks, MDPI Information, Vol. 10, Issue 4, 2019

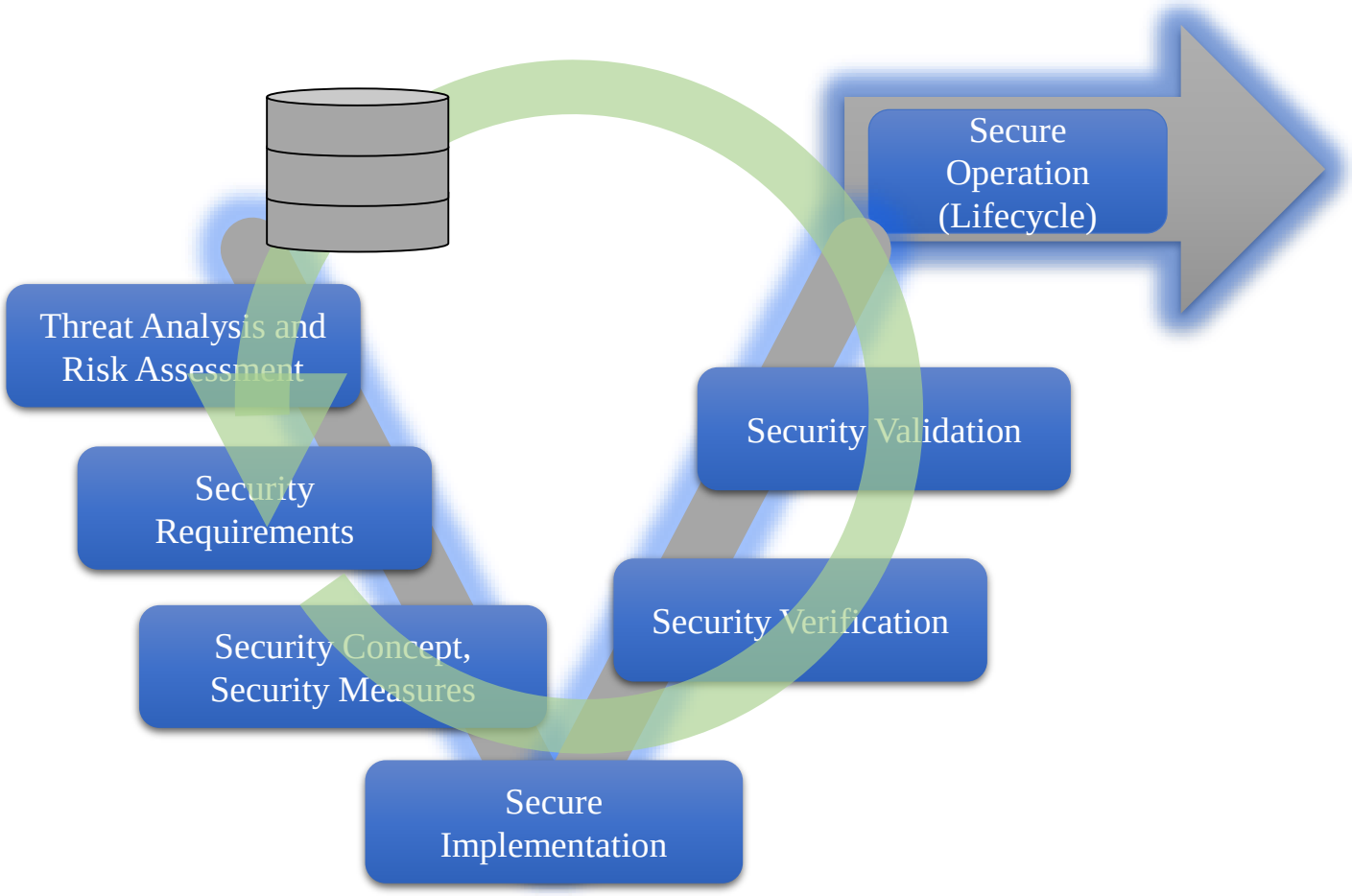
Applying Database to Security Model



Creating and Reusing a Penetration Test Database



Using Attack Path Generation Method in Development



- Knowledge base is created
- Constant refinement and updates of the database
- Early tests possible based on existing penetration tests
- Reusing attacks/tests in security testing and threat modeling
- Mitigations can be aligned with attacks

Bundesministerium für Bildung und Forschung

SecForCARs
security for connected automated cars

Note: Research was performed within the SecForCars project, funded by German „Bundesministerium für Bildung und Forschung“ (BMBF)

Hochschule Karlsruhe
University of
Applied Sciences

Institute for
Energy Efficient Mobility

Reiner Kriesten
Institute for Energy Efficient Mobility
E-Mail: reiner.kriesten@h-ka.de
Web: www.h-ka.de/ieem/profil