Security & Safety by Model-based Requirements Engineering

28th IEEE International Requirements Engineering Conference, 2020, Zurich, Switzerland

Sergej Japs, M.Sc.

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer
IEM

About Me

Sergej Japs

Fraunhofer Research Institute for
Mechatronic Systems Design IEM
Zukunftsmeile 1
33102 Paderborn (Germany)
sergej.japs@iem.fraunhofer.de

Research Associate &
PhD Candidate (Since 1,5 Years)

Experience in Systems Engineering &
Requirements Engineering (Since 7,5 Years)

M.Sc. in Computer Science
from University of Paderborn (Germany)

Twitter: @MBSEGuy

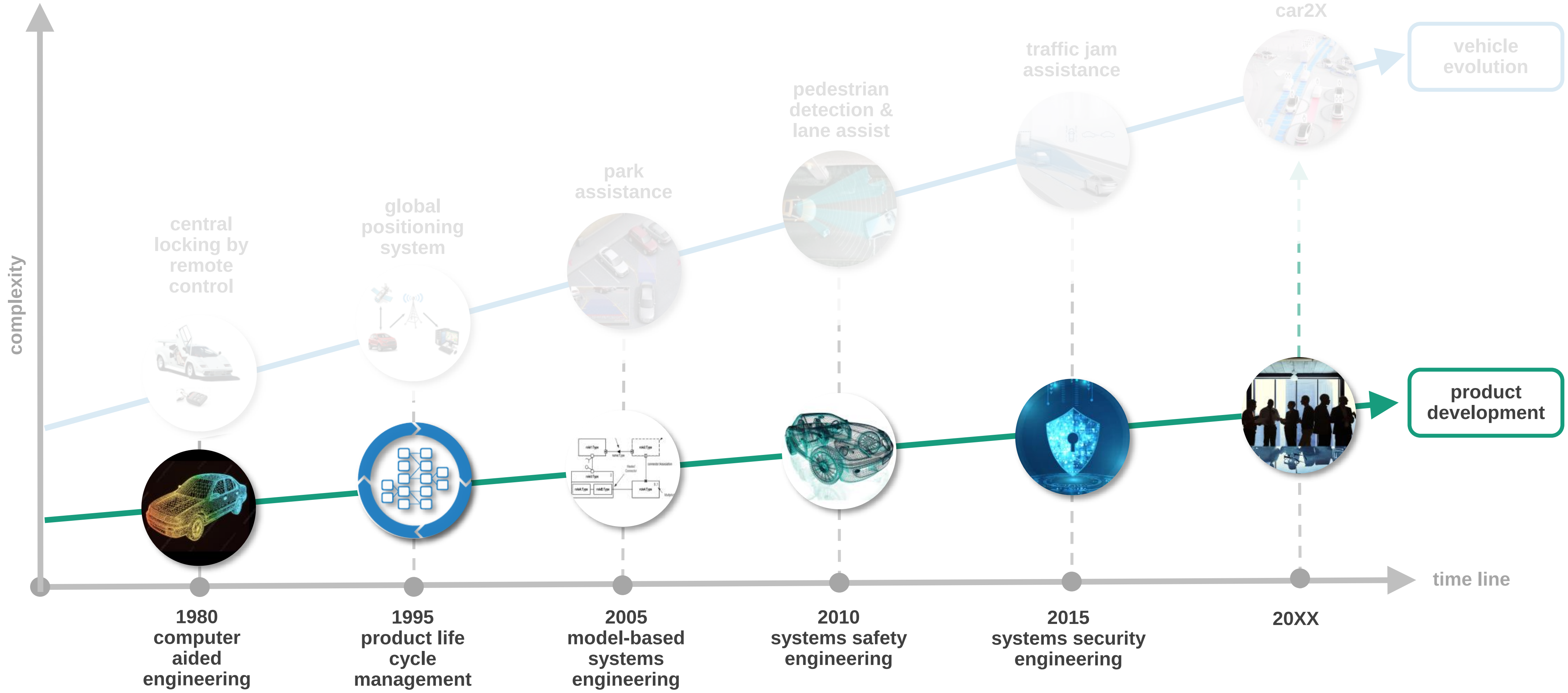
LinkedIn

Xing

Research Gate

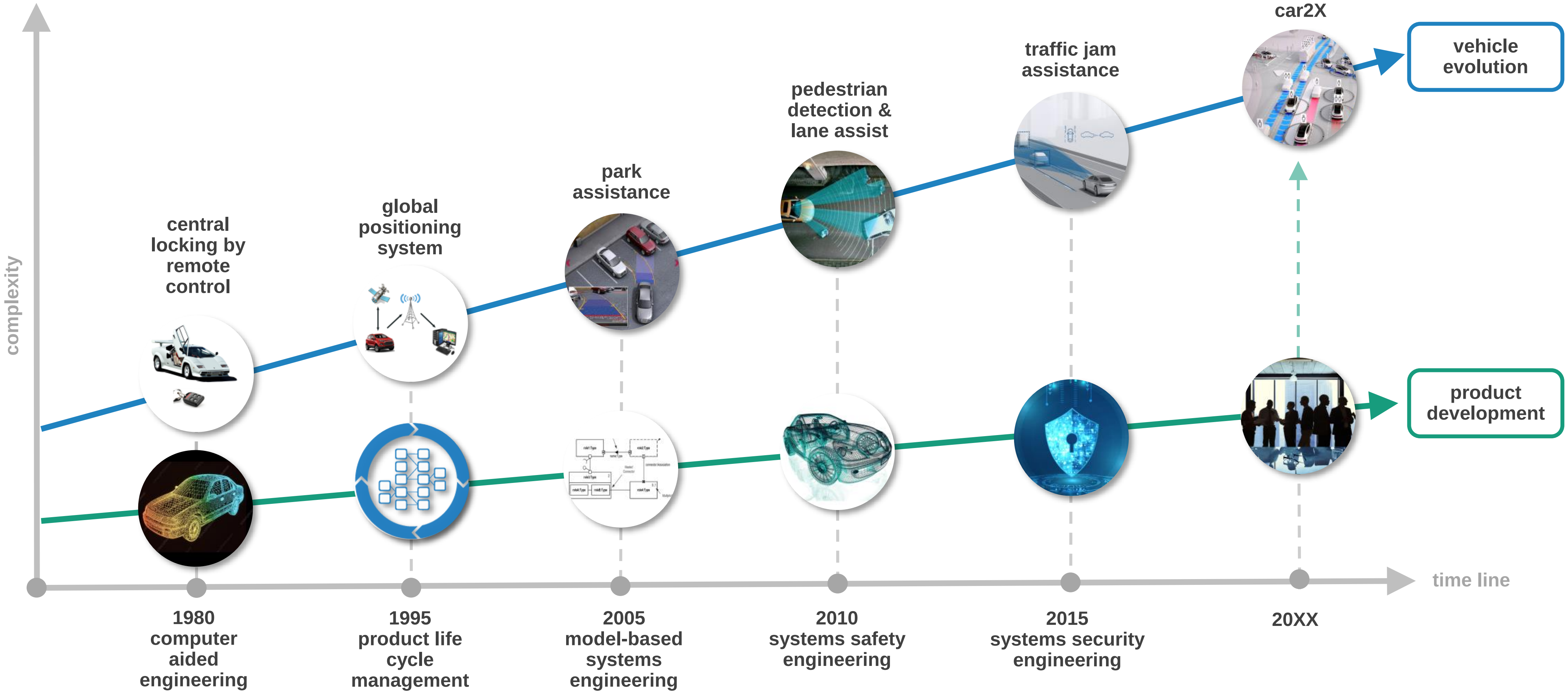
Motivation

Product Development vs. Increasing Vehicle Complexity


complexity
central locking by remote control
global positioning system
park assistance
pedestrian detection & lane assist
traffic jam assistance
car2X
vehicle evolution
product development
time line
1980
computer aided engineering
1995
product life cycle management
2005
model-based systems engineering
2010
systems safety engineering
2015
systems security engineering
20XX

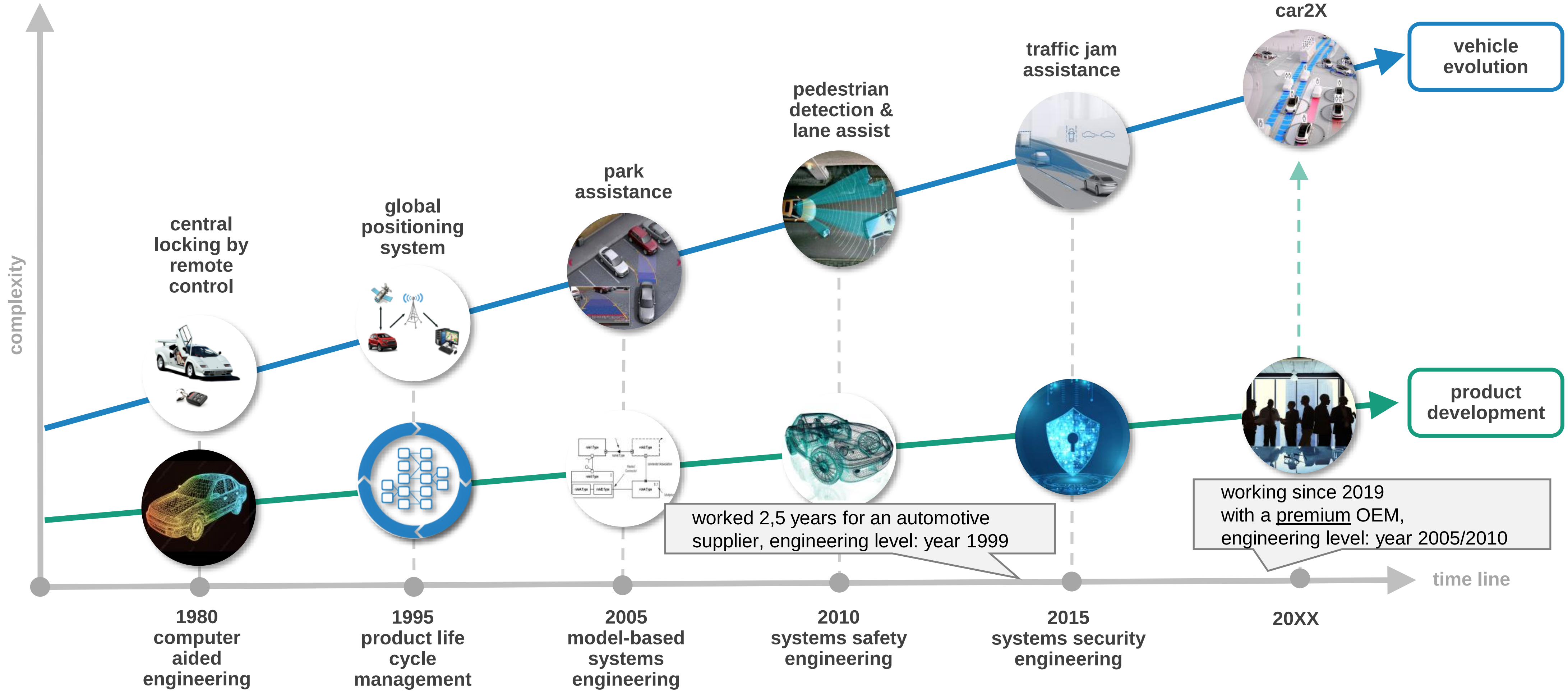
Motivation

Product Development vs. Increasing Vehicle Complexity


complexity
car2X
vehicle evolution
traffic jam assistance
pedestrian detection & lane assist
park assistance
global positioning system
central locking by remote control
product development
time line
1980 computer aided engineering
1995 product life cycle management
2005 model-based systems engineering
2010 systems safety engineering
2015 systems security engineering
20XX

Motivation

Product Development vs. Increasing Vehicle Complexity



complexity

central locking by remote control

global positioning system

park assistance

pedestrian detection & lane assist

traffic jam assistance

car2X

vehicle evolution

product development

worked 2,5 years for an automotive supplier, engineering level: year 1999

working since 2019 with a premium OEM, engineering level: year 2005/2010

time line

1980 computer aided engineering

1995 product life cycle management

2005 model-based systems engineering

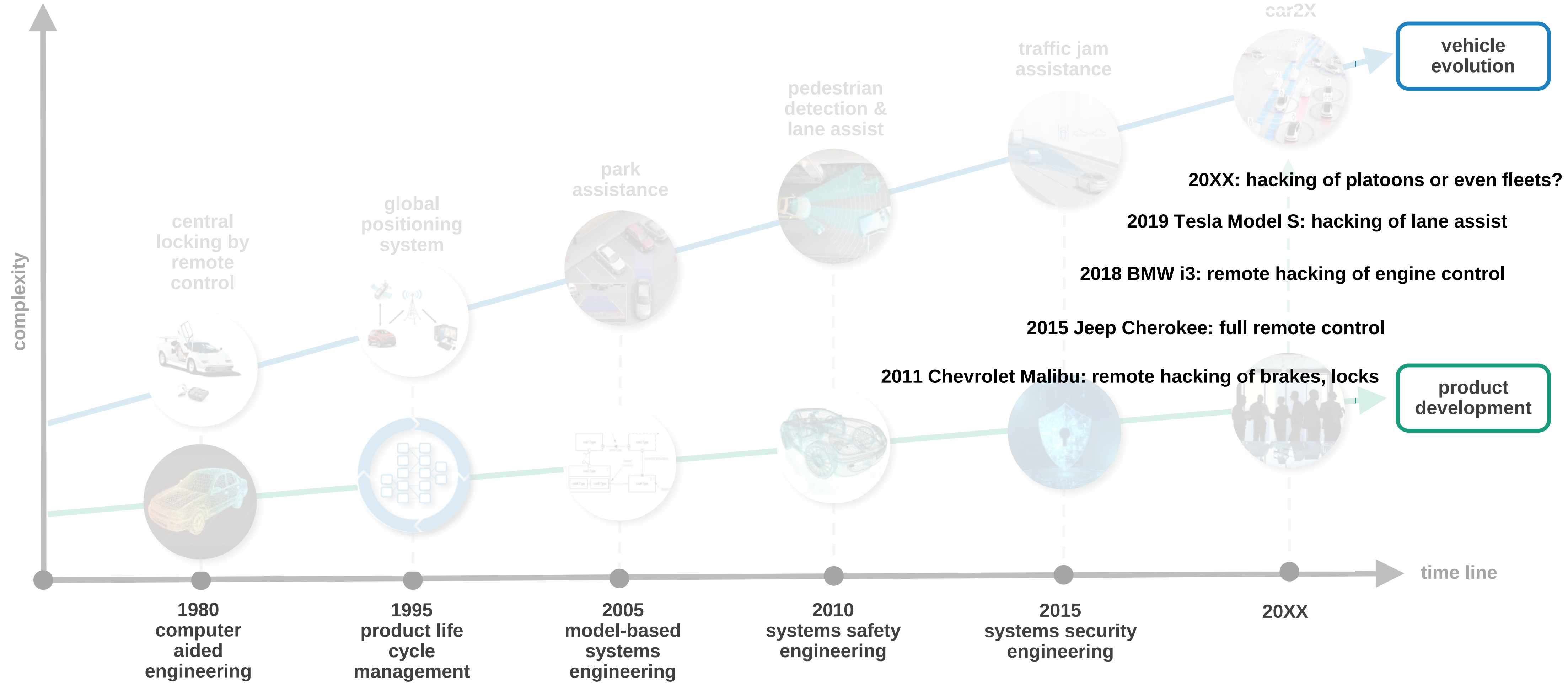
2010 systems safety engineering

2015 systems security engineering

20XX

Motivation

Product Development vs. Increasing Vehicle Complexity vs. Hacking



complexity

central locking by remote control

global positioning system

park assistance

pedestrian detection & lane assist

traffic jam assistance

car2X

vehicle evolution

20XX: hacking of platoons or even fleets?

2019 Tesla Model S: hacking of lane assist

2018 BMW i3: remote hacking of engine control

2015 Jeep Cherokee: full remote control

2011 Chevrolet Malibu: remote hacking of brakes, locks

product development

time line

1980 computer aided engineering

1995 product life cycle management

2005 model-based systems engineering

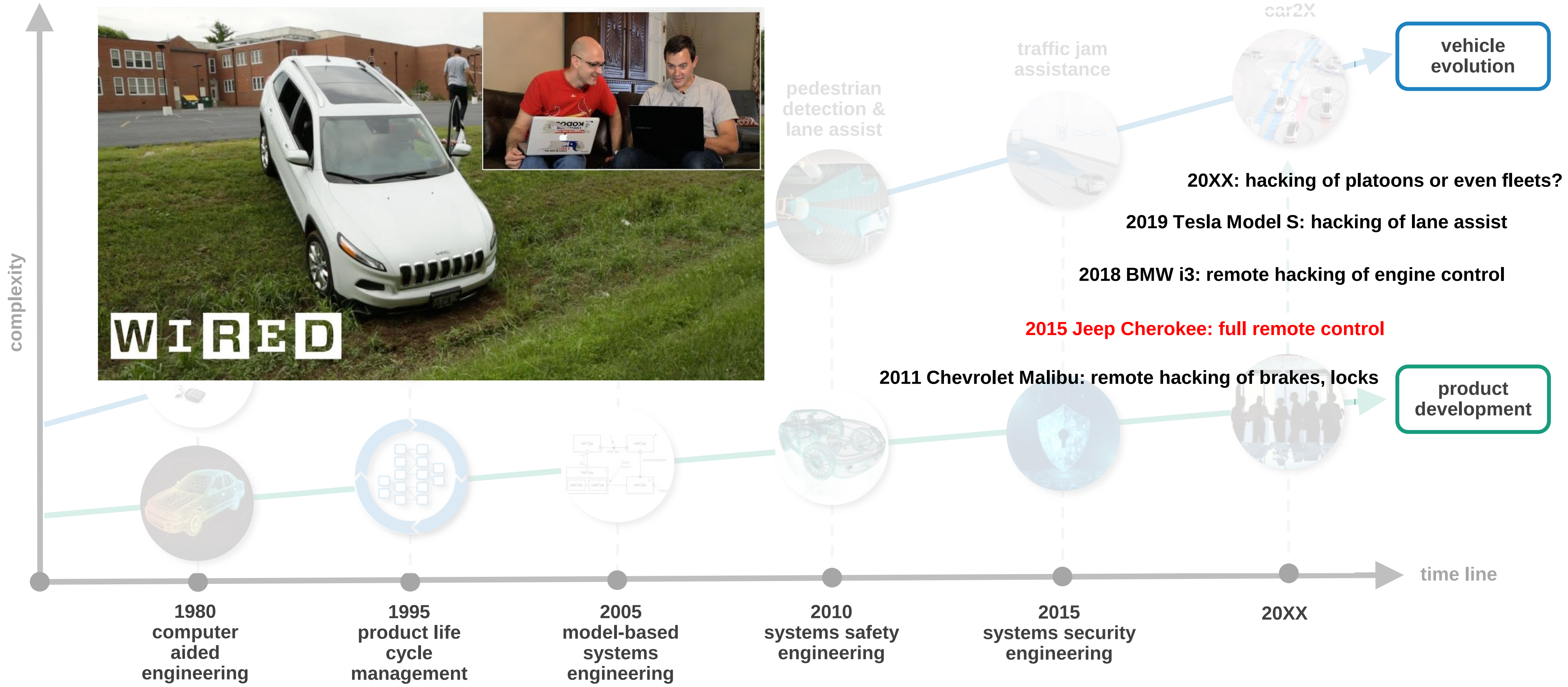
2010 systems safety engineering

2015 systems security engineering

20XX

Motivation

Product Development vs. Increasing Vehicle Complexity vs. Hacking



20XX: hacking of platoons or even fleets?

2019 Tesla Model S: hacking of lane assist

2018 BMW i3: remote hacking of engine control

2015 Jeep Cherokee: full remote control

2011 Chevrolet Malibu: remote hacking of brakes, locks

1980 computer aided engineering

1995 product life cycle management

2005 model-based systems engineering

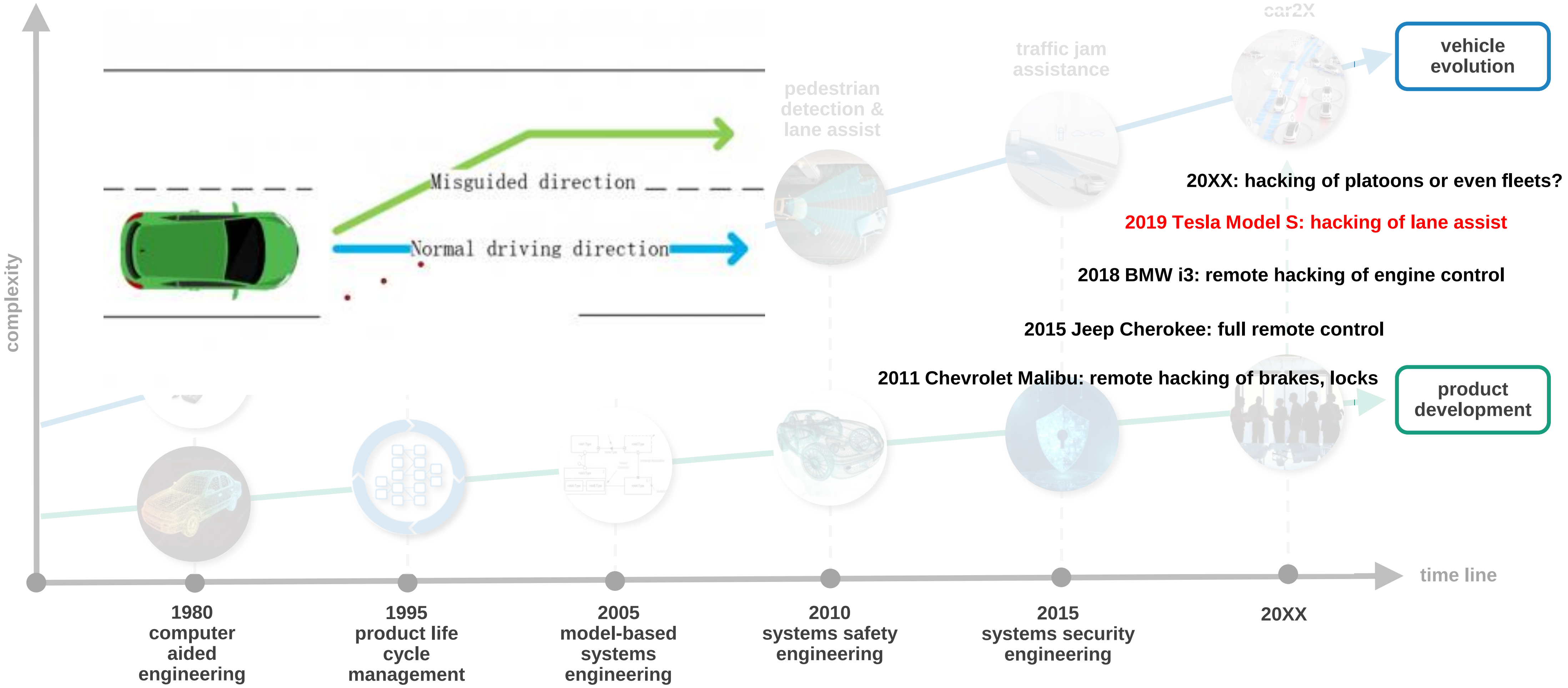
2010 systems safety engineering

2015 systems security engineering

20XX

Motivation

Product Development vs. Increasing Vehicle Complexity vs. Hacking



20XX: hacking of platoons or even fleets?

2019 Tesla Model S: hacking of lane assist

2018 BMW i3: remote hacking of engine control

2015 Jeep Cherokee: full remote control

2011 Chevrolet Malibu: remote hacking of brakes, locks

1980 computer aided engineering

1995 product life cycle management

2005 model-based systems engineering

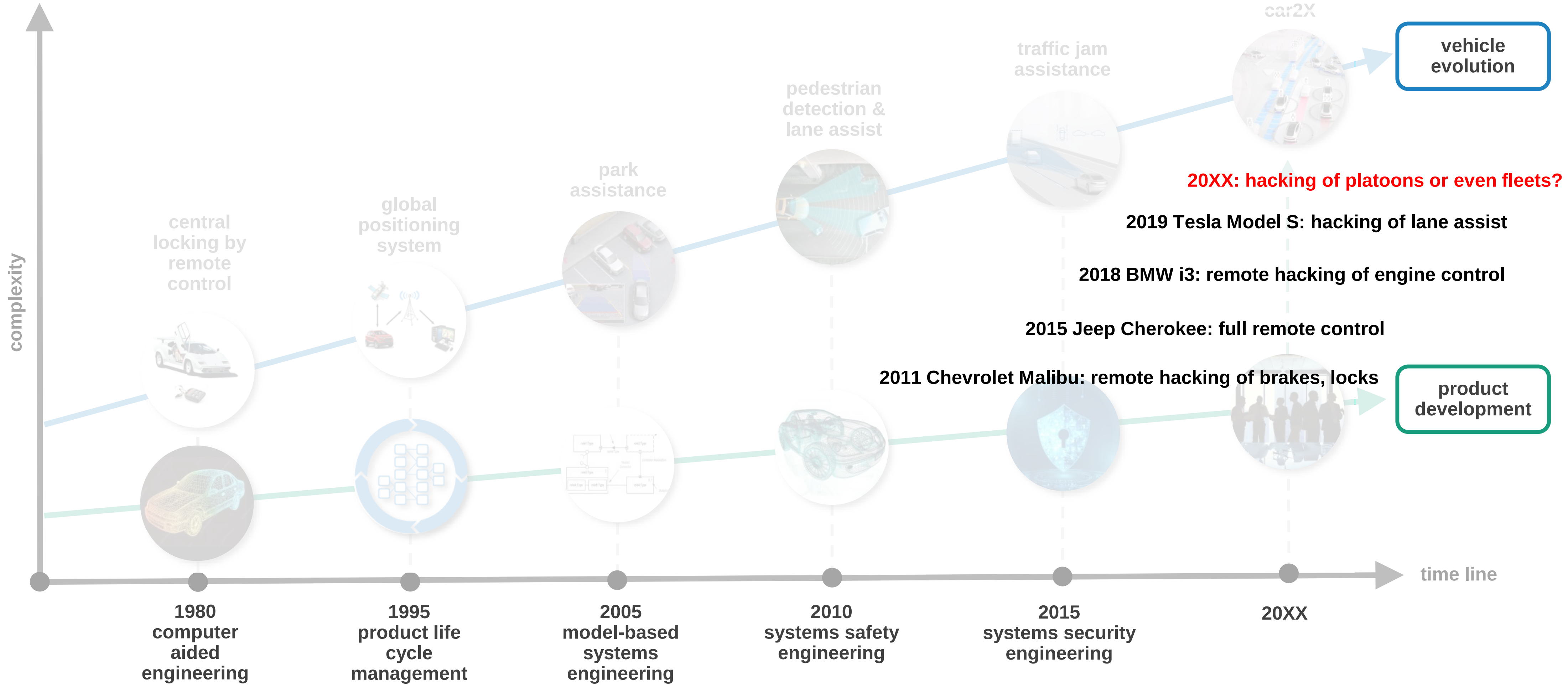
2010 systems safety engineering

2015 systems security engineering

20XX

Motivation

Product Development vs. Increasing Vehicle Complexity vs. Hacking



complexity

central locking by remote control

global positioning system

park assistance

pedestrian detection & lane assist

traffic jam assistance

car2X

vehicle evolution

20XX: hacking of platoons or even fleets?

2019 Tesla Model S: hacking of lane assist

2018 BMW i3: remote hacking of engine control

2015 Jeep Cherokee: full remote control

2011 Chevrolet Malibu: remote hacking of brakes, locks

product development

time line

1980 computer aided engineering

1995 product life cycle management

2005 model-based systems engineering

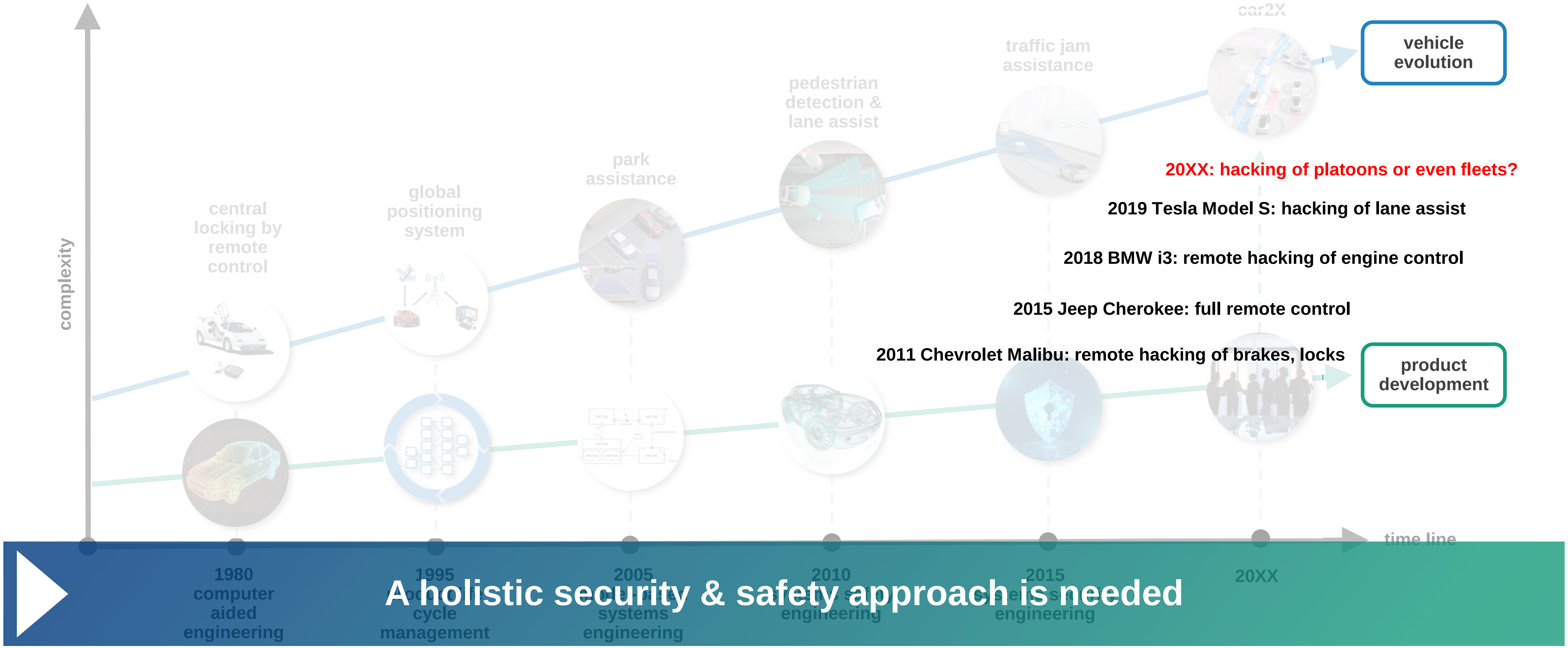
2010 systems safety engineering

2015 systems security engineering

20XX

Motivation

Product Development vs. Increasing Vehicle Complexity vs. Hacking



20XX: hacking of platoons or even fleets?

2019 Tesla Model S: hacking of lane assist

2018 BMW i3: remote hacking of engine control

2015 Jeep Cherokee: full remote control

2011 Chevrolet Malibu: remote hacking of brakes, locks

A holistic security & safety approach is needed

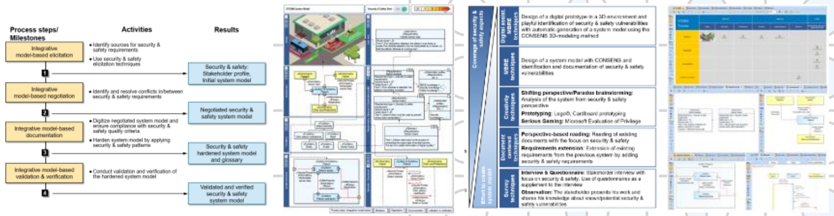
Holistic Security & Safety Approach

Criteria & Literature Analysis

● = satisfied ◐ = parially satisfied ○ = not satisfied

	C1	C2	C3-C4	C5	C6-C8
01 Cheng et al.: 2019	●	◐	●	◐	◐
02 Amorim et al.: 2017	●	◐	●	◐	◐
03 SAE J3061: 2016	●	◐	●	◐	○
04 SAHARA: 2015	●	◐	◐	◐	○
05 PBSE: 2020	●	◐	○	●	●
06 SREP FOR CPS: 2018	●	◐	●	○	○
07 ISO 26262-9:2018	●	◐	◐	◐	○
08 POHL: 2016					○
09 ISO/IEC/IEEE 15288: 2015					○
10 Rupp et al: 2014					○
11 Heisel et al: 2019					◐
12 FERNANDES: 2013					◐
13 CORAS: 2020					○
14 Microsoft SDL: 2016					◐
15 SQUARE: 2005	○	◐	◐	○	○

The holistic approach (identify & fix threats) is based on my initial approach (identify threats):
STORM - Security & safety driven model-based requirements engineering process, 2020, (currently under review)



Process steps/ Milestones
Activities
Results
Integrative model-based elicitation
Integrative model-based negotiation
Integrative model-based documentation
Integrative model-based validation & verification
Security & safety: Stakeholder profile, Initial system model
Negotiated security & safety system model
Security & safety hardened system model and glossary
Validated and verified security & safety system model

Criteria

C1	Applicability at system level
C2	Coverage of the requirements engineering process steps (elicitation & negotiation, documentation, validation)
C3 - C4	Consideration of security & safety
C5	Capability (Validation) for use with models
C6-C8	Reduction of engineering effort (model generation & analysis, design patterns)

Holistic Security & Safety Approach

Criteria & Literature Analysis

STORM - Security & safety driven model-based requirements engineering process, 2020, (currently under review)

Criteria

C1	Applicability at system level
C2	Coverage of the requirements engineering process steps (elicitation & negotiation, documentation, validation)
C3 - C4	Consideration of security & safety
C5	Capability (Validation) for use with models
C6-C8	Reduction of engineering effort (model generation & analysis, design patterns)

Not every approach can be (directly) used on system level

● = satisfied ◐ = parially satisfied ○ = not satisfied

	C1	C2	C3-C4	C5	C6-C8
01 Cheng et al.: 2019	●	◐	●	◐	◐
02 Amorim et al.: 2017	●	◐	●	◐	◐
03 SAE J3061: 2016	●	◐	●	◐	○
04 SAHARA: 2015	●	◐	◐	◐	○
05 PBSE: 2020	●	◐	○	●	●
06 SREP FOR CPS: 2018	●	◐	●	○	○
07 ISO 26262-9:2018	●	◐	◐	◐	○
08 POHL: 2016	●	●	◐	◐	○
09 ISO/IEC/IEEE 15288: 2015	●	◐	○	○	○
10 Rupp et al: 2014	●	●	◐	◐	○
11 Heisel et al: 2019	○	◐	●	●	◐
12 FERNANDES: 2013	○	◐	◐	●	◐
13 CORAS: 2020	○	◐	◐	◐	○
14 Microsoft SDL: 2016	○	◐	◐	●	◐
15 SQUARE: 2005	○	◐	◐	○	○

Holistic Security & Safety Approach

Criteria & Literature Analysis

STORM - Security & safety driven model-based requirements engineering process, 2020, (currently under review)

Criteria

C1	Applicability at system level
C2	Coverage of the requirements engineering process steps (elicitation & negotiation, documentation, validation)
C3 - C4	Consideration of security & safety
C5	Capability (Validation) for use with models
C6-C8	Reduction of engineering effort (model generation & analysis, design patterns)

The most approaches only partially cover the requirements engineering process steps

● = satisfied ◐ = parially satisfied ○ = not satisfied

	C1	C2	C3-C4	C5	C6-C8
01 Cheng et al.: 2019	●	◐	●	◐	◐
02 Amorim et al.: 2017	●	◐	●	◐	◐
03 SAE J3061: 2016	●	◐	●	◐	○
04 SAHARA: 2015	●	◐	◐	◐	○
05 PBSE: 2020	●	◐	○	●	●
06 SREP for CPS: 2018	●	◐	●	○	○
07 ISO 26262-9:2018	●	◐	◐	◐	○
08 Pohl: 2016	●	●	◐	◐	○
09 ISO/IEC/IEEE 15288: 2015	●	◐	○	○	○
10 Rupp et al: 2014	●	●	◐	◐	○
11 Heisel et al: 2019	○	◐	●	●	◐
12 Fernandes: 2013	○	◐	◐	●	◐
13 CORAS: 2020	○	◐	◐	◐	○
14 Microsoft SDL: 2016	○	◐	◐	●	◐
15 SQUARE: 2005	○	◐	◐	○	○

Holistic Security & Safety Approach

Criteria & Literature Analysis

STORM - Security & safety driven model-based requirements engineering process, 2020, (currently under review)

Criteria

C1	Applicability at system level
C2	Coverage of the requirements engineering process steps (elicitation & negotiation, documentation, validation)
C3 - C4	Consideration of security & safety
C5	Capability (Validation) for use with models
C6-C8	Reduction of engineering effort (model generation & analysis, design patterns)

The analyzed appraoches cover either security or safety, or they cover security & safety together, but superficially

● = satisfied ◐ = parially satisfied ○ = not satisfied

	C1	C2	C3-C4	C5	C6-C8
01 Cheng et al.: 2019	●	◐	●	◐	◐
02 Amorim et al.: 2017	●	◐	●	◐	◐
03 SAE J3061: 2016	●	◐	●	◐	○
04 SAHARA: 2015	●	◐	◐	◐	○
05 PBSE: 2020	●	◐	○	●	●
06 SREP for CPS: 2018	●	◐	●	○	○
07 ISO 26262-9:2018	●	◐	◐	◐	○
08 Pohl: 2016	●	●	◐	◐	○
09 ISO/IEC/IEEE 15288: 2015	●	◐	○	○	○
10 Rupp et al: 2014	●	●	◐	◐	○
11 Heisel et al: 2019	○	◐	●	●	◐
12 Fernandes: 2013	○	◐	◐	●	◐
13 CORAS: 2020	○	◐	◐	◐	○
14 Microsoft SDL: 2016	○	◐	◐	●	◐
15 SQUARE: 2005	○	◐	◐	○	○

Holistic Security & Safety Approach

Criteria & Literature Analysis

STORM - Security & safety driven model-based requirements engineering process, 2020, (currently under review)

Criteria

C1	Applicability at system level
C2	Coverage of the requirements engineering process steps (elicitation & negotiation, documentation, validation)
C3 - C4	Consideration of security & safety
C5	Capability (Validation) for use with models
C6-C8	Reduction of engineering effort (model generation & analysis, design patterns)

The most approaches which used models, are not understandable by non discipline specific experts

● = satisfied ◐ = parially satisfied ○ = not satisfied

	C1	C2	C3-C4	C5	C6-C8
01 Cheng et al.: 2019	●	◐	●	◐	◐
02 Amorim et al.: 2017	●	◐	●	◐	◐
03 SAE J3061: 2016	●	◐	●	◐	○
04 SAHARA: 2015	●	◐	◐	◐	○
05 PBSE: 2020	●	◐	○	●	●
06 SREP FOR CPS: 2018	●	◐	●	○	○
07 ISO 26262-9:2018	●	◐	◐	◐	○
08 POHL: 2016	●	●	◐	◐	○
09 ISO/IEC/IEEE 15288: 2015	●	◐	○	○	○
10 Rupp et al: 2014	●	●	◐	◐	○
11 Heisel et al: 2019	○	◐	●	●	◐
12 FERNANDES: 2013	○	◐	◐	●	◐
13 CORAS: 2020	○	◐	◐	◐	○
14 Microsoft SDL: 2016	○	◐	◐	●	◐
15 SQUARE: 2005	○	◐	◐	○	○

Holistic Security & Safety Approach

Criteria & Literature Analysis

STORM - Security & safety driven model-based requirements engineering process, 2020, (currently under review)

Criteria

C1	Applicability at system level
C2	Coverage of the requirements engineering process steps (elicitation & negotiation, documentation, validation)
C3 - C4	Consideration of security & safety
C5	Capability (Validation) for use with models
C6-C8	Reduction of engineering effort (model generation & analysis, design patterns)

Only some approaches care about reduction of engineering effort, but do not cover all sub-criteria

● = satisfied ◐ = parially satisfied ○ = not satisfied

	C1	C2	C3-C4	C5	C6-C8
01 Cheng et al.: 2019	●	◐	●	◐	◐
02 Amorim et al.: 2017	●	◐	●	◐	◐
03 SAE J3061: 2016	●	◐	●	◐	○
04 SAHARA: 2015	●	◐	◐	◐	○
05 PBSE: 2020	●	◐	○	●	●
06 SREP for CPS: 2018	●	◐	●	○	○
07 ISO 26262-9:2018	●	◐	◐	◐	○
08 Pohl: 2016	●	●	◐	◐	○
09 ISO/IEC/IEEE 15288: 2015	●	◐	○	○	○
10 Rupp et al: 2014	●	●	◐	◐	○
11 Heisel et al: 2019	○	◐	●	●	◐
12 Fernandes: 2013	○	◐	◐	●	◐
13 CORAS: 2020	○	◐	◐	◐	○
14 Microsoft SDL: 2016	○	◐	◐	●	◐
15 SQUARE: 2005	○	◐	◐	○	○

Holistic Security & Safety Approach

Criteria & Literature Analysis

STORM - Security & safety driven model-based requirements engineering process, 2020, (currently under review)

Criteria

C1	Applicability at system level
C2	Coverage of the requirements engineering process steps (elicitation & negotiation, documentation, validation)
C3 - C4	Consideration of security & safety
C5	Capability (Validation) for use with models
C6-C8	Reduction of engineering effort (model generation & analysis, design patterns)

Only some approaches care about reduction of engineering effort, but do not cover all s criteria

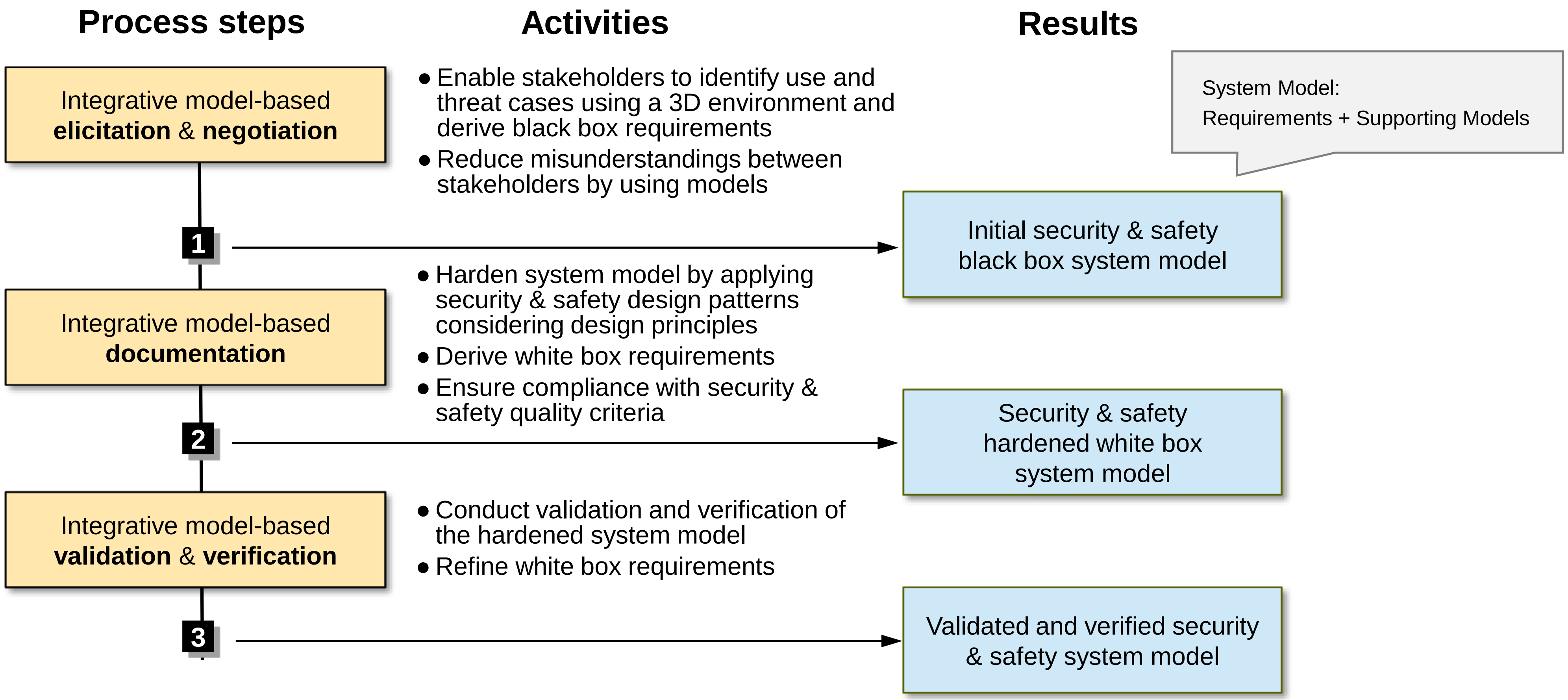
● = satisfied ◐ = parially satisfied ○ = not satisfied

	C1	C2	C3-C4	C5	C6-C8
01 Cheng et al.: 2019	●	◐	●	◐	◐
02 Amorim et al.: 2017	●	◐	●	◐	◐
03 SAE J3061: 2016	●	◐	●	◐	○
04 SAHARA: 2015	●	◐	◐	◐	○
05 PBSE: 2020	●	◐	○	●	●
06 SREP FOR CPS: 2018	●	◐	●	○	○
07 ISO 26262-9:2018	●	◐	◐	◐	○
08 POHL: 2016	●	●	◐	◐	○
09 ISO/IEC/IEEE 15288: 2015	●	◐	○	○	○
10 Rupp et al: 2014	●	●	◐	◐	○
11 Heisel et al: 2019	○	◐	●	●	◐
12 FERNANDES: 2013	○	◐	◐	●	◐
13 CORAS: 2020	○	◐	◐	◐	○
14 Microsoft SDL: 2016	○	◐	◐	●	◐
15 SQUARE: 2005	○	◐	◐	○	○

None of the analysed approaches fulfill all criteria

Holistic Security & Safety Approach

Process Model



Process steps

Activities

Results

System Model:
Requirements + Supporting Models

Integrative model-based **elicitation** & **negotiation**

- Enable stakeholders to identify use and threat cases using a 3D environment and derive black box requirements
- Reduce misunderstandings between stakeholders by using models

1 → Initial security & safety black box system model

Integrative model-based **documentation**

- Harden system model by applying security & safety design patterns considering design principles
- Derive white box requirements
- Ensure compliance with security & safety quality criteria

2 → Security & safety hardened white box system model

Integrative model-based **validation** & **verification**

- Conduct validation and verification of the hardened system model
- Refine white box requirements

3 → Validated and verified security & safety system model

STORM - Security & safety driven model-based requirements engineering process, 2020, (currently under review)

Integrative Model-Based Elicitation & Negotiation

Reduce Misunderstandings Between Stakeholders by Using Models

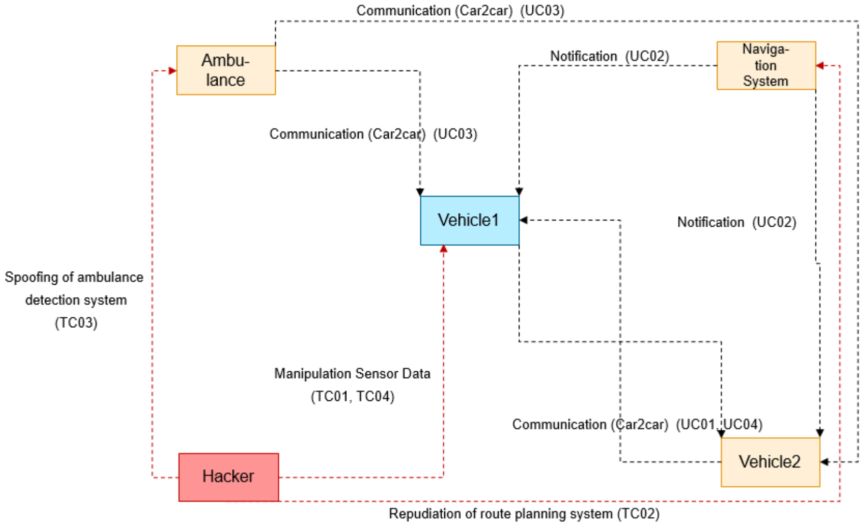
How to consider security & safety in early engineering?

1. Form **interdisciplinary team** of stakeholders
2. **Identify** & **fix** threats using models
3. **Derive** requirements

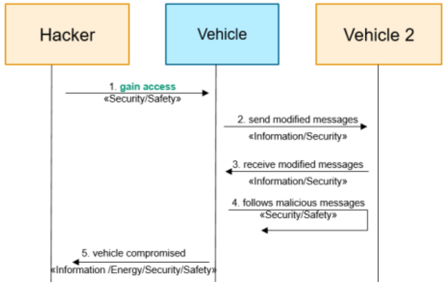
I prepared and moderated **8 workshops** with overall **84 participants** from industry which were not familiar with security

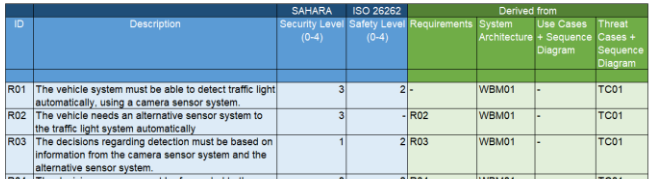
Lessons learned:

1. Early **identification of threats** generally **works** with non security experts
2. For a **better common understanding** of use and threat cases the stakeholders **require tools**
3. Non security experts need additional tools to **fix** identified threats



Communication (Car2car) (UC03)
Ambu-lance
Notification (UC02)
Naviga-tion System
Communication (Car2car) (UC03)
Vehicle1
Notification (UC02)
Spoofing of ambulance detection system (TC03)
Manipulation Sensor Data (TC01, TC04)
Communication (Car2car) (UC01, UC04)
Vehicle2
Hacker
Repudiation of route planning system (TC02)





		SAHARA	ISO 26262	Derived from			
ID	Description	Security Level (0-4)	Safety Level (0-4)	Requirements	System Architecture	Use Cases + Sequence Diagram	Threat Cases + Sequence Diagram
R01	The vehicle system must be able to detect traffic light automatically, using a camera sensor system.	3	2	-	WBM01	-	TC01
R02	The vehicle needs an alternative sensor system to the traffic light system automatically	3	-	R02	WBM01	-	TC01
R03	The decisions regarding detection must be based on information from the camera sensor system and the alternative sensor system.	1	2	R03	WBM01	-	TC01

Participant area	No. of workshops	Ø-Partic.	Application purpose	Consideration of safety & security aspects
Farming	5	7	Development of a sensor system	Focus on security aspects
Management consultancy	2	12	Introduction to MBRE using the example of a CPS	Given in the task definition
Mechanical and plant engineering	1	25		

Integrative Model-Based Elicitation & Negotiation

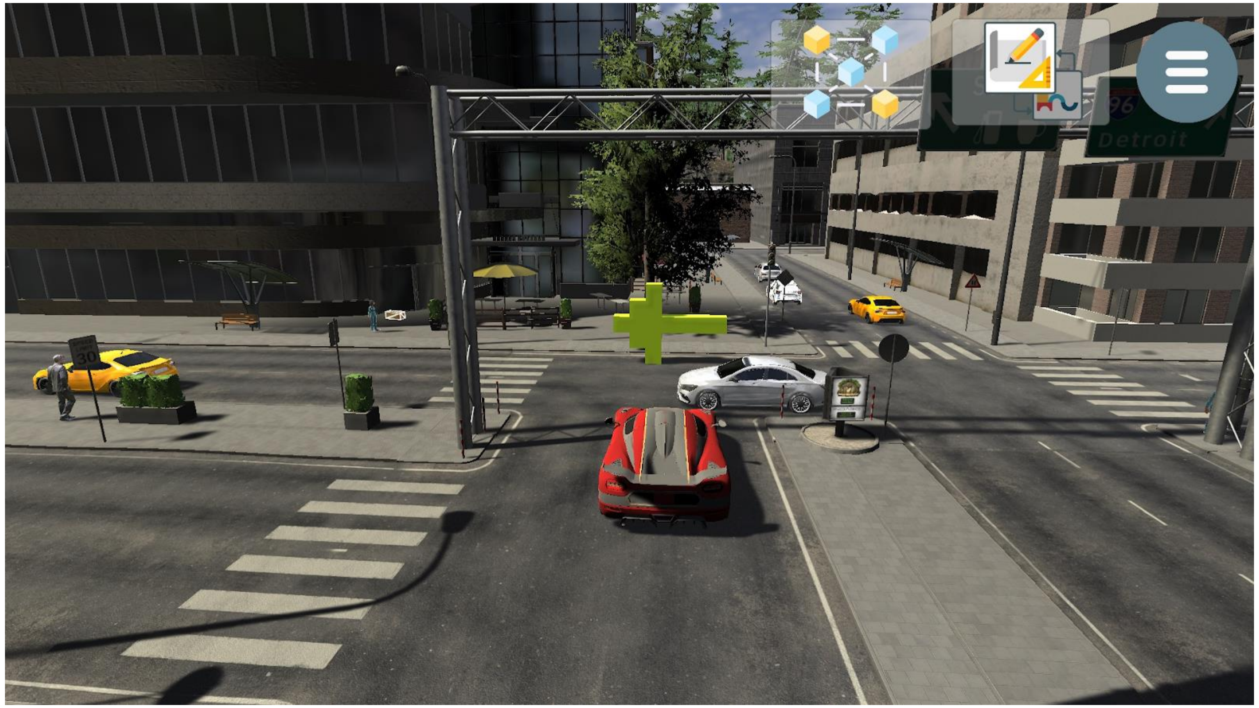
Enable Stakeholders to Identify Use and Threat Cases Using a 3D Environment

How can stakeholders from different disciplines communicate with each other and identify use and threat cases on system of systems level?

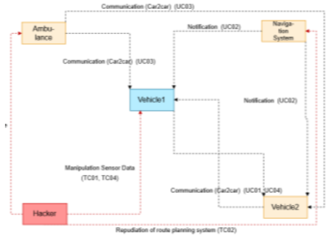
Analyzed approaches either only helped with visualization and not with model based engineering or were only applicable to one specific technical system -> do both

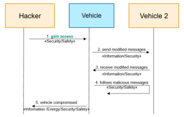
3D Engineer

1. **Initiation of the project and project lead since 1.5 years with currently 7 student developers**
2. **Currently A/B Testing: Review of the effectiveness of the use of the 3D environment in a 40h project with 130 interdisciplinary master students.**
   -> Will the approach improve the overall quality of the derived black box requirements?
3. **Planned: Adjustment of the method and tool usability and review with participants from industry**



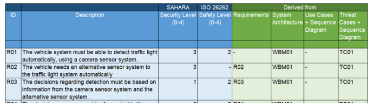
1. Identify use and threat cases using the 3D environment and derive user stories


Communication (Car2car) (UC03)
Ambu-lance
Notification (UC02)
Naviga-tion System
Communication (Car2car) (UC03)
Vehicle1
Notification (UC02)
Manipulation Sensor Data (TC01, TC04)
Communication (Car2car) (UC01, UC04)
Hacker
Vehicle2
Repudiation of route planning system (TC02)


Hacker
Vehicle
Vehicle 2
1. gain access «Security/Safety»
2. send modified messages «Information/Security»
3. receive modified messages «Information/Security»
4. follows malicious messages «Security/Safety»
5. vehicle compromised «Information /Energy/Security/Safety»

2. Generate models automatically

3. Refine models



		SAHARA	ISO 26262	Derived from			
ID	Description	Security Level (0-4)	Safety Level (0-4)	Requirements	System Architecture	Use Cases + Sequence Diagram	Threat Cases + Sequence Diagram
R01	The vehicle system must be able to detect traffic light automatically, using a camera sensor system.	3	2	-	WBM01	-	TC01
R02	The vehicle needs an alternative sensor system to the traffic light system automatically	3	-	R02	WBM01	-	TC01
R03	The decisions regarding detection must be based on information from the camera sensor system and the alternative sensor system.	1	2	R03	WBM01	-	TC01

4. Derive black box requirements

Download paper at: https://doi.org/10.1017/dsd.2020.41

Download prototype at: https://gitlab.cc-asp.fraunhofer.de/mbseguy/3d_engineer

Integrative Model-Based Elicitation & Negotiation

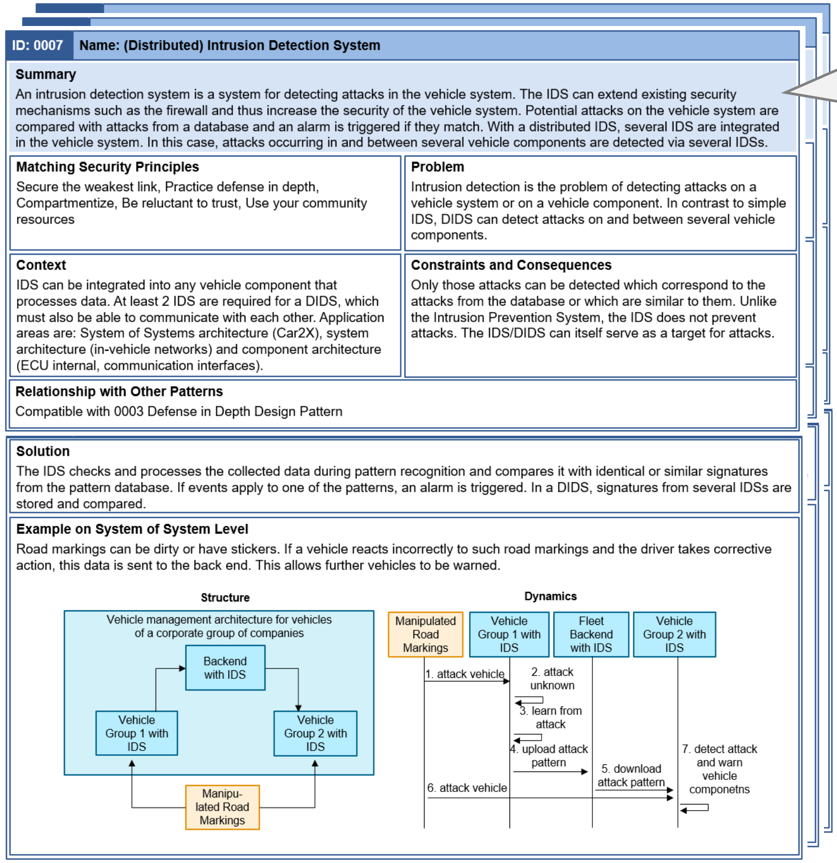
Harden System Model by Applying Security & Safety Design Patterns

So we have managed to identify threats, but how to actually fix these threats?

Literature research: Some good methodical work exists, but without security reference. Many pattern catalogues exist, but only for security experts.
-> consider security, make design patterns understandable for an interdisciplinary team of non security experts

1. Currently A/B Testing: Review of the effectiveness of the use of the security & safety design patterns in an additional 40h project with 130 interdisciplinary master students.
   -> Will the approach improve the overall quality of the derived white box requirements?

2. Planned: Adjustment of the method, increase of design pattern pool and review of the method with participants from industry



ID: 0007 | **Name: (Distributed) Intrusion Detection System**

Summary
An intrusion detection system is a system for detecting attacks in the vehicle system. The IDS can extend existing security mechanisms such as the firewall and thus increase the security of the vehicle system. Potential attacks on the vehicle system are compared with attacks from a database and an alarm is triggered if they match. With a distributed IDS, several IDS are integrated in the vehicle system. In this case, attacks occurring in and between several vehicle components are detected via several IDSs.

Matching Security Principles
Secure the weakest link, Practice defense in depth, Compartmentize, Be reluctant to trust, Use your community resources

Problem
Intrusion detection is the problem of detecting attacks on a vehicle system or on a vehicle component. In contrast to simple IDS, DIDS can detect attacks on and between several vehicle components.

Context
IDS can be integrated into any vehicle component that processes data. At least 2 IDS are required for a DIDS, which must also be able to communicate with each other. Application areas are: System of Systems architecture (Car2X), system architecture (in-vehicle networks) and component architecture (ECU internal, communication interfaces).

Constraints and Consequences
Only those attacks can be detected which correspond to the attacks from the database or which are similar to them. Unlike the Intrusion Prevention System, the IDS does not prevent attacks. The IDS/DIDS can itself serve as a target for attacks.

Relationship with Other Patterns
Compatible with 0003 Defense in Depth Design Pattern

Solution
The IDS checks and processes the collected data during pattern recognition and compares it with identical or similar signatures from the pattern database. If events apply to one of the patterns, an alarm is triggered. In a DIDS, signatures from several IDSs are stored and compared.

Example on System of System Level
Road markings can be dirty or have stickers. If a vehicle reacts incorrectly to such road markings and the driver takes corrective action, this data is sent to the back end. This allows further vehicles to be warned.

Own created design patterns were reviewed by experts from industry & research

1. Derive white box system model

2. Mark threats in white box system model, do risk management

3. Apply design patterns considering security principles, derive white box requirements

Integrative Model-Based Elicitation & Negotiation

Planned: Conduct Validation and Verification of the Hardened System Model

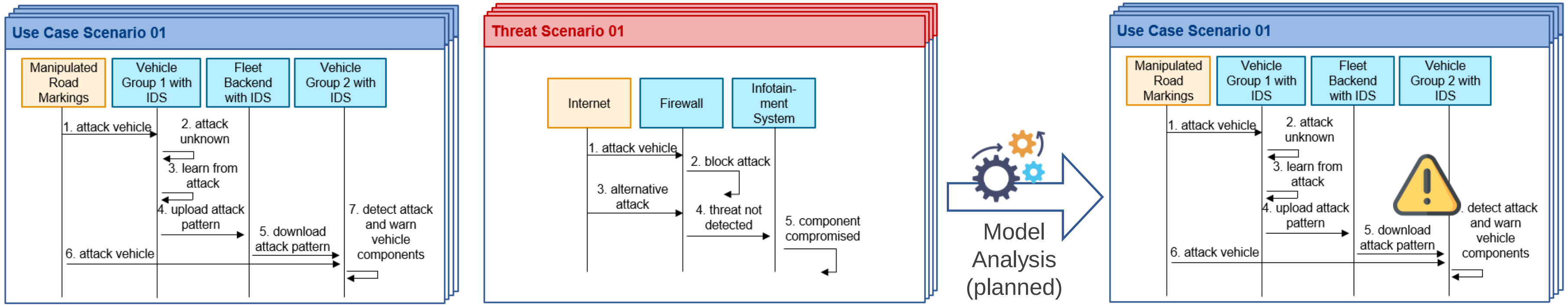
Are we done yet? No, the models & requirements still have to be reviewed. How can we reduce the effort for this?

Lessons learned from workshops with industry participants
-> even simple sequences of system behaviour are not manageable without software tool support

How can the occurrence of already defined threat cases be automatically checked taking into account the already defined use cases?

Literature Research -> Adapt existing approaches/software tools so that they can be used by industry

Idea



Own preliminary work: https://www.google.de/books/edition/Tag_des_Systems_Engineering/Phu4DwAAQBAJ?hl=de&gbpv=0

1. Perform model analysis

2. Fix white box system model

3. Refine white box requirements

THANK YOU

Security & Safety by Model-based Requirements Engineering

28th IEEE International Requirements Engineering Conference, 2020, Zurich, Switzerland

Sergej Japs, M.Sc.

Fraunhofer Research Institute for Mechatronic Systems Design IEM

Paderborn, Germany

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer
IEM