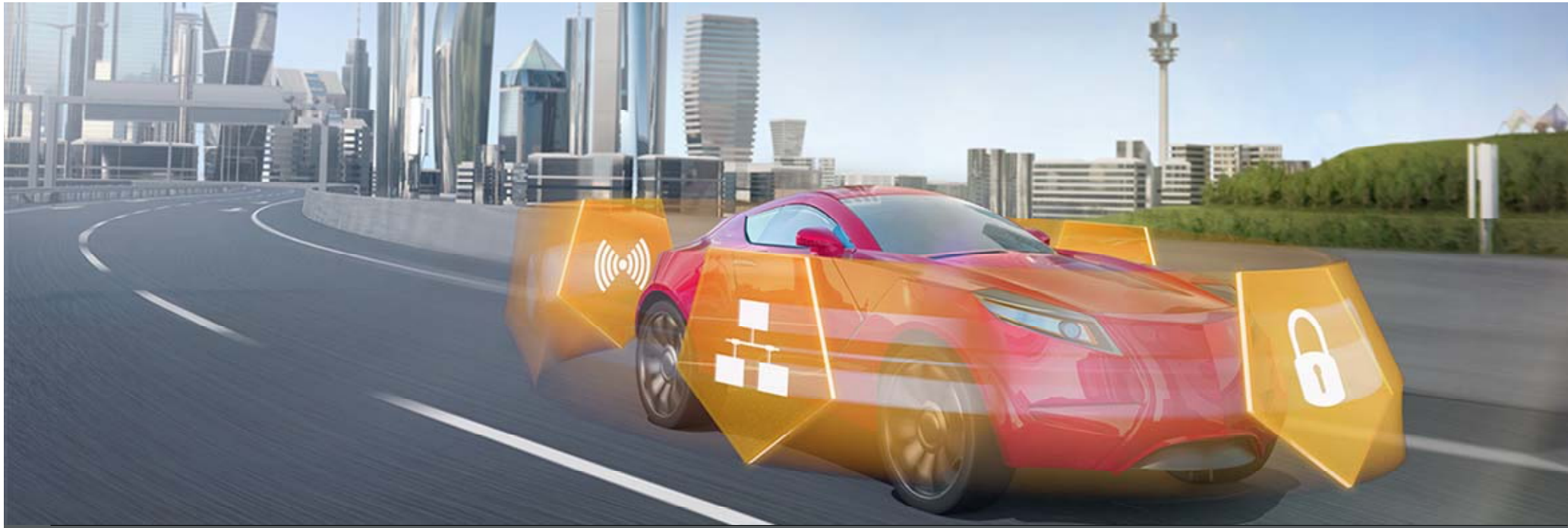
VECTOR



Functional Safety and Cyber-Security – Experiences and Trends

Dr. Christof Ebert, Vector Consulting Services

V1.1 | 2017-10-25

Vector Consulting Services

- Experts for product development, product strategy and IT in critical systems
- Interim support, such as virtual security and safety officers and interim management
- Global presence
- Trainings on Agile, Requirements, Security, Safety, CMMI/SPICE etc.
- Part of Vector Group with over 1800 employees

www.vector.com/consulting

Automotive

Aerospace

IT & Finance

Digital Transformation

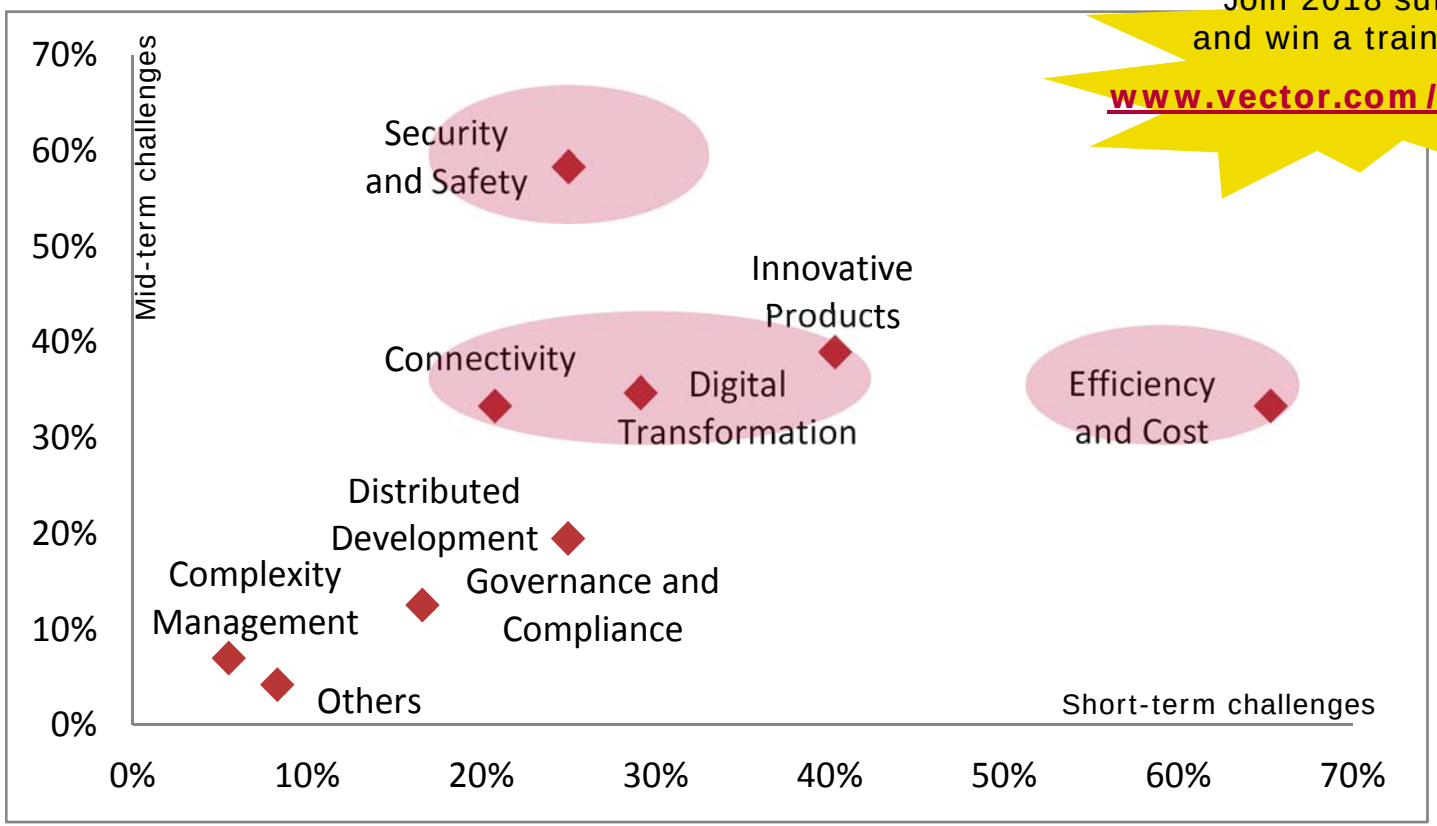
Medical

Railway

Vector Client Survey: Security and Safety are Major Challenges

Join 2018 survey now
and win a training or book

www.vector.com/trends-survey



Vector Client Survey 2017. Details: www.vector.com/trends. Horizontal axis shows short-term challenges; vertical axis shows mid-term challenges. Sum > 100% due to 3 answers per question. Strong validity with >4% response rate of 1500 recipients from different industries worldwide.

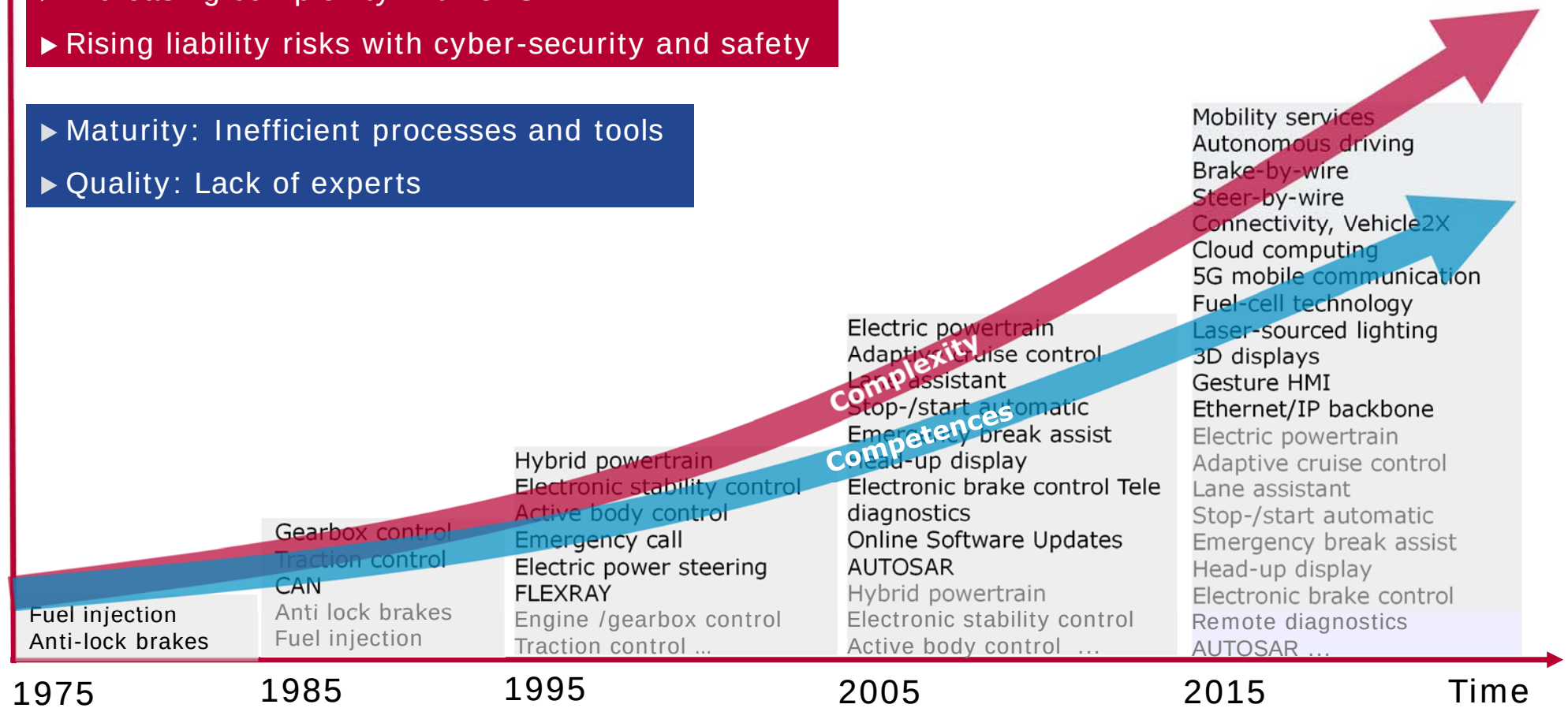
Safety and **security** paired with **efficient engineering** are major challenge.

Agenda

Challenge: Security and Safety

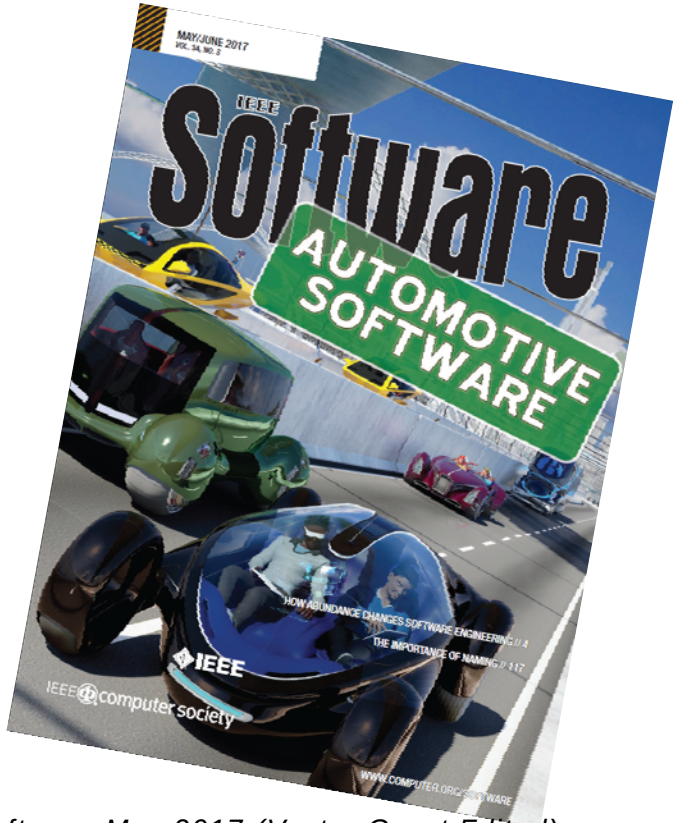
- Increasing complexity with CASE
- Rising liability risks with cyber-security and safety

- Maturity: Inefficient processes and tools
- Quality: Lack of experts



Automotive E/E Trends: CASE and more

- **Mobility**: From driving to multi-modal mobility services and sharing culture
- **Business Models**: From incumbent tiered supply-chain to flexible new players from IT industry
- **E/E architecture**: From distributed electronic controllers to standardized three-tier architecture
- **IT architecture**: From proprietary building blocks to open IT systems with off-the-shelf components and adaptive SOA.
- **Development lifecycle**: From the classic V model with rather heavy release cycles to agile DevOps-like approach.
- **Governance**: From encapsulated safety-critical functions to interwoven quality assurance for liability, safety, cyber-security, privacy.
- **Culture**: From R&D vs. IT separation to convergence.
- **Competences**: From automotive embedded electronics to IT as a core competence of all engineers.



Source: IEEE Software May 2017 (Vector Guest Edited)
www.vector.com/consulting-mediacenter

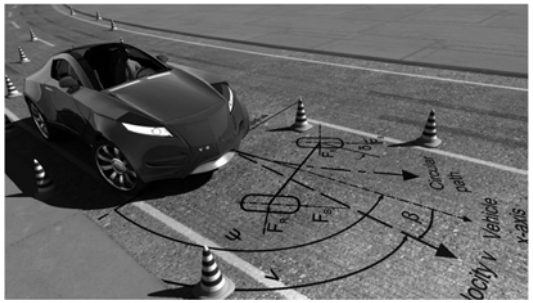
Fast evolution along all technology dimensions – and all needs to be safe and secure

Automotive Trends Impact Safety and Security

1. Powertrain

→ Energy efficiency

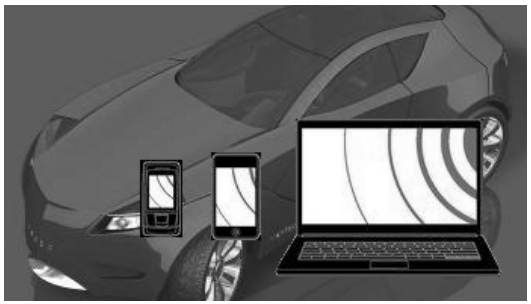
→ **Unintended speed change**



2. Driver Assistance

→ Autonomous driving

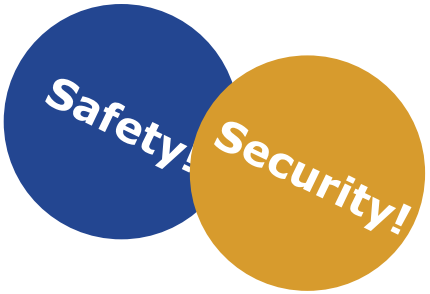
→ **Signal confusion**



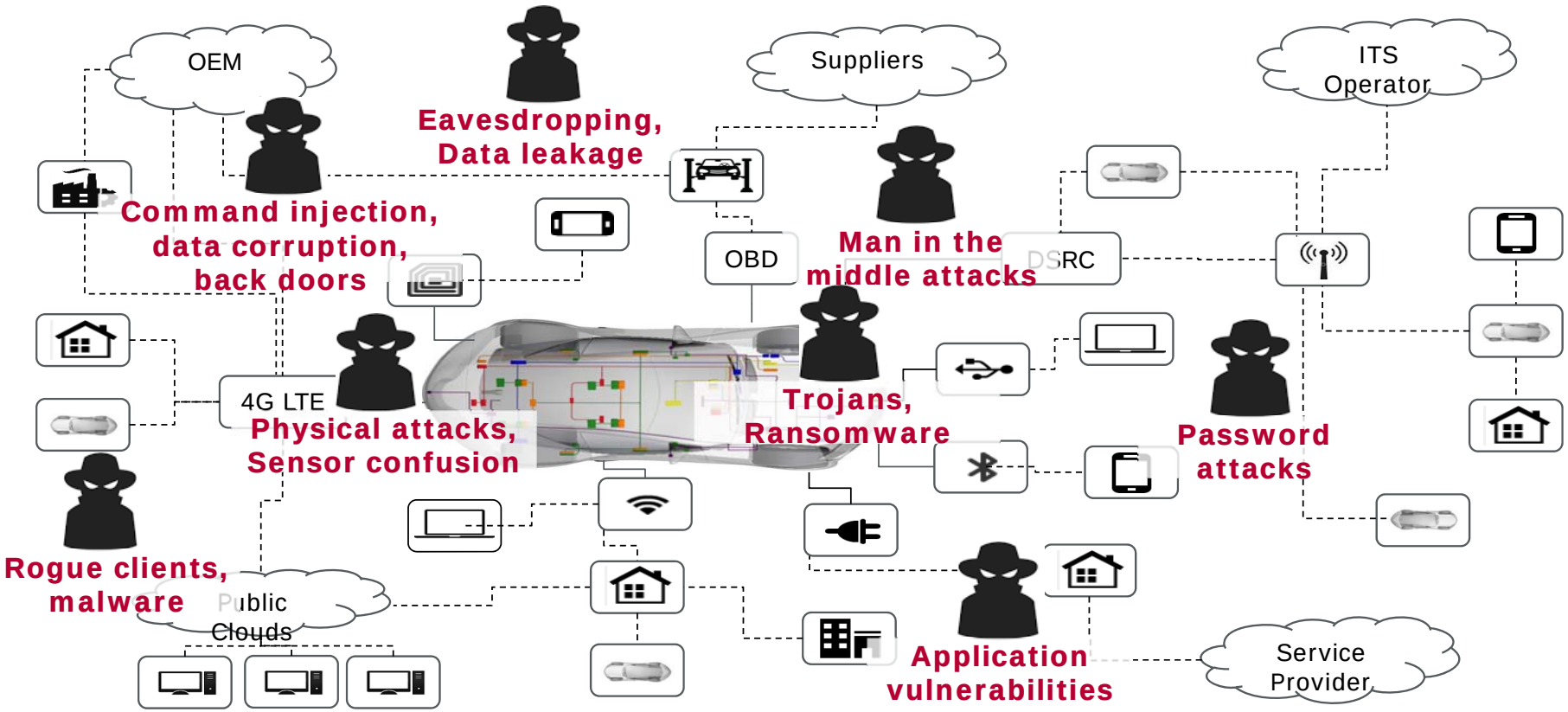
3. Connectivity

→ Always connected

→ **Sudden Driver distraction**



CASE (Connectivity, Autonomy, Sharing, Efficiency) ▶ **Cyber-Attacks**



Security will be the major liability risk in the future.
Average security breach is detected in of 70% cases by third party – after 8 months.

Agenda

Combined Safety and Security Need Holistic Systems Engineering

Functional Safety

- Goal: Protect health
- Risk: Accident
- Governance: ISO 26262 etc.
- Methods:
  - HARA, FTA, FMEA, ...
  - Fail operational, ...
  - Redundancy, ...

Cyber-Security

- Goal: Protect assets
- Risk: Attack, exploits
- Governance: ISO 27001 etc.
- Methods:
  - TARA, ...
  - Cryptography, ID/IP, ...
  - Key management, ...

Privacy

- Goal: Protect personality
- Risk: Data breach
- Governance: Privacy laws
- Methods:
  - TARA,...
  - Cryptography,...
  - Explicit consent, ...

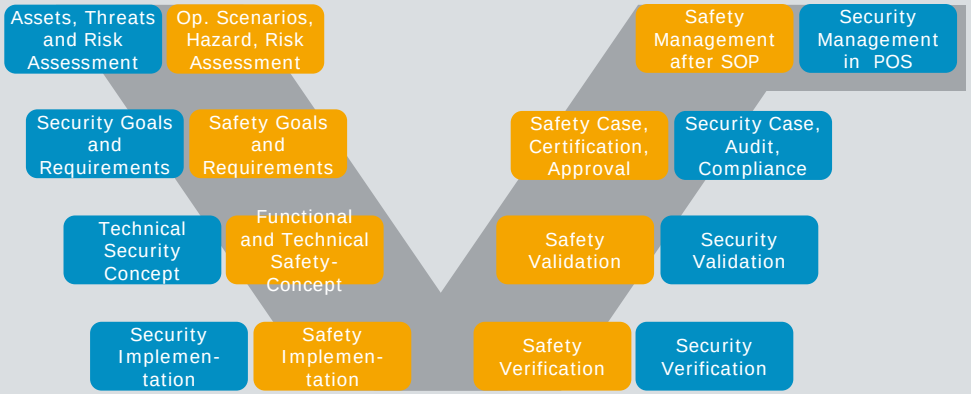
Liability ➔ Risk management ➔ Holistic systems engineering

Standards Demand Risk-Oriented Approach

Functional Safety (IEC 61508, ISO 26262)

- Hazard and risk analysis
- Functions and risk mitigation
- Safety engineering

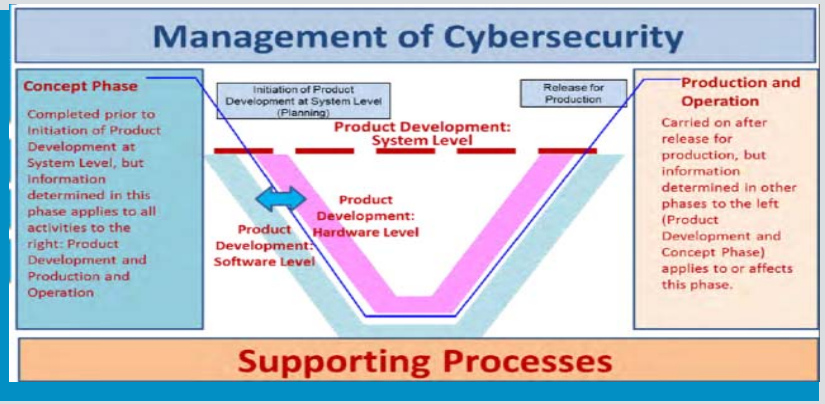
ISO 26262 ed.2 will not comprehensively address security, but include shared methods, such as TARA



+ Security (ISO 27001, ISO 15408, ISO 21434, SAE J3061)

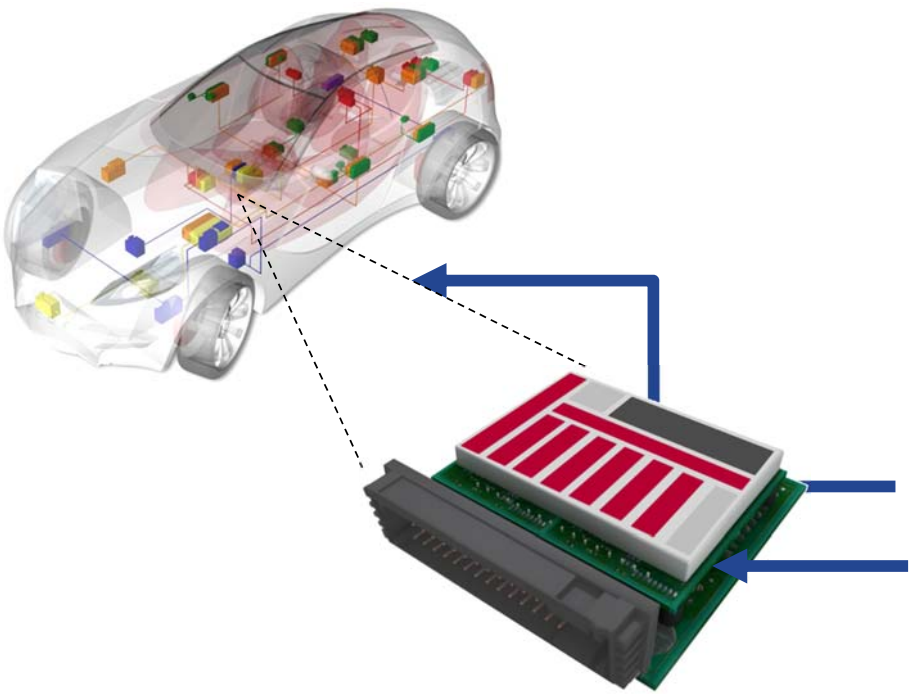
- Threat and risk analysis
- Abuse, misuse, confuse cases
- Security engineering

Security and Safety are interacting and demand holistic systems engineering



For (re) liable and efficient ramp-up connect security to safety governance

State of the Art: Functional Safety



Relevance of ISO 26262 is basically understood

1.	Driving Situations	OEM
2.	Hazards	OEM
3.	Risks and Safety Integrity Level	OEM
4.	Safety Goals → Safety Requirements	OEM
5.	Technical Safety Concept	OEM/Tier1
6.	Safety requirements on ECU level	OEM/Tier1
7.	Software Safety Requirements	Tier1/Vector

Functional safety can be efficiently achieved
on the basis of mature development processes

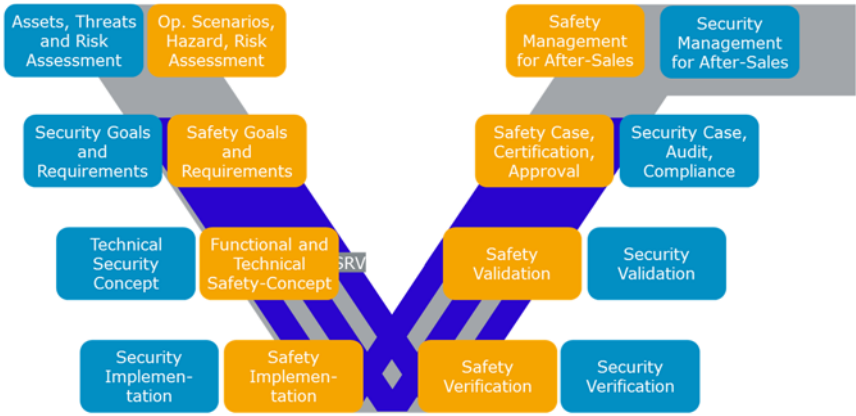
State of the Art: Cyber-Security

Security demands are growing fast

- Connectivity and open channels allow security attacks
- Exploits will persist beyond “zero-day” because so far no OTA governance
- Safety-critical systems connected to potentially unsecure bus systems

Practical experiences are available

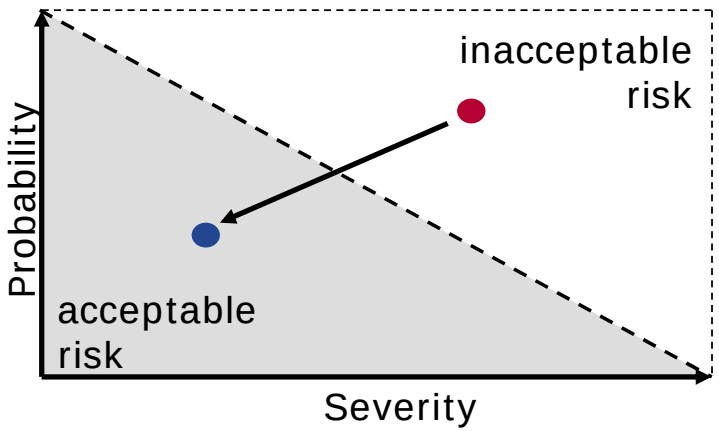
- Extend hazard analysis with threat analysis and automotive attack models
- Reuse existing safety artefacts to ensure robust safety case
- Define tailored security protection for safety-critical systems
- Encrypt entire bus communication, e.g. AUTOSAR
- Protect ECUs with secure boot and HW-defined security
- Completely separate infotainment and HU

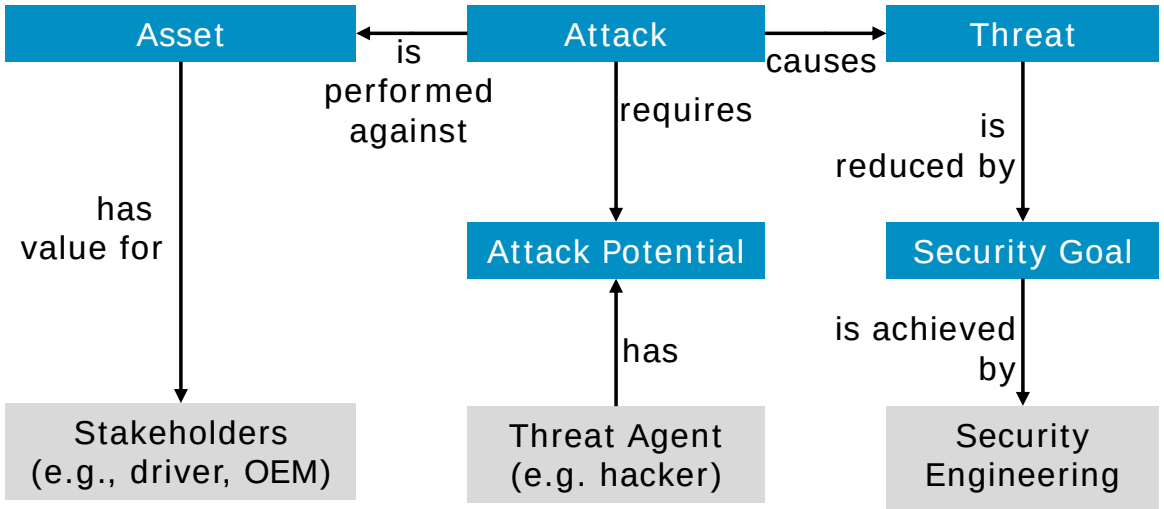


Do not copy paste standards because it increases overheads and complexity

Functional Safety and Cyber-Security Demand Risk-Oriented Development

Risk = Severity of harmful event × Probability of occurrence





Risk-oriented engineering means to **intelligently mitigate the residual risks**

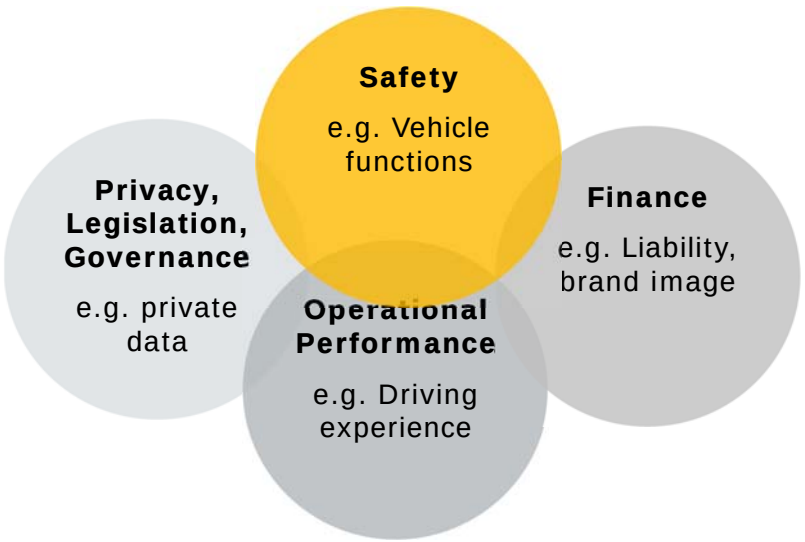
Agenda

VECTOR

Concept of Combined Threat/Hazard Analysis and Risk Assessment

Assets → Threat-Model & Risks → Measures → Concept for Solution → Verification

Specific automotive asset categories



Example: Identified threats

- **Safety**
  - Injuries because of malfunctioning Passive Entry
- **Financial**
  - Extra cost due to call-back and law-suits
- **Operational Performance**
  - Car cannot be started, doors cannot be opened
- **Privacy / Legislation**
  - Theft of personal data

Consider specific automotive assets derived from CIAAG (Confidentiality, Integrity, Authenticity, Availability, Governance) scheme

Tool Support: Vector SecurityCheck (1/3)

Delete	Asset ID:	Assetname:	Source:	Description:	Status:	Source Of Scope Definition:
☐	1	Software update, vbf-file (stored at diagnostics PC, in transit etc.)	VCS	Software image	possibly in scope	-
☐	2	Public signing key (vehicle)	VCS	The system will store private keys for software signing in the vehicle.	in scope	-
☐	3	Privacy relevant information	Vector	-	possibly in scope	-
☐	4	Log files, security log	Vector	-	possibly in scope	-
☐	5	ECU Parameters	VCS	Needs clarification how this is different from Diagnostic Messages 'IPR, parameter and algorithms for ADAS'.	possibly in scope	-
☐	6	ECU software (installed, flashing during boot)	VCS	Needs clarification how this is different from Asset ID 1 'Software update, vbf-file'.	possibly in scope	-
☐	7	Bootloader software (in transit during update, installed etc.)	Vector	-	possibly in scope	-

Apply tools

- **Consistent risk assessment** and management
- Enable traceability to development
- Governance by continuously updated documentation

Tool Support: Vector SecurityCheck (2/3)

TARA Entry

Assetname / ID:	ECU software (installed, flashing during boot) 6
Ciaag:	Auth
Attack Vector:	DOS attack KEY6
Effect Of Attack:	Denial of Service
Threat ID:	th - 6
Threat:	threat6
Expertise:	Proficient
Window Of Opportunity:	Critical
Equipment, Effort:	Standard
Safety:	Mod. Injuries
Financial:	High
Operational:	High
Privacy:	Medium
SGID:	6
Security Goal:	Mitigate DOS attacks None
Comment:	N/A
Valid?	yes

Add

< previous | next >

New

								THREAT LEVEL				SECURITY LEVEL								
Delete	No.:	Asset ID:	Assetname:	CIAAG:	Attack vector:	Effect of attack:	Threat ID:	Threat:	Expertise:	Window of Opportunity:	Equipment, Effort:	Threat Level:	Safety:	Financial:	Operational:	Privacy:	Security Level:	SGID:	Security Goal:	Comment:	Valid
	1	6	ECU software (installed,	Auth	DOS attack	Denial of Service	th - 6	threat6	Proficient	Critical	Standard	0	Mod. Injuries	High	High	Medium	Critical	6	Mitigate DOS attacks	N/A	yes

Apply

< previous | next >

< previous | next >

New

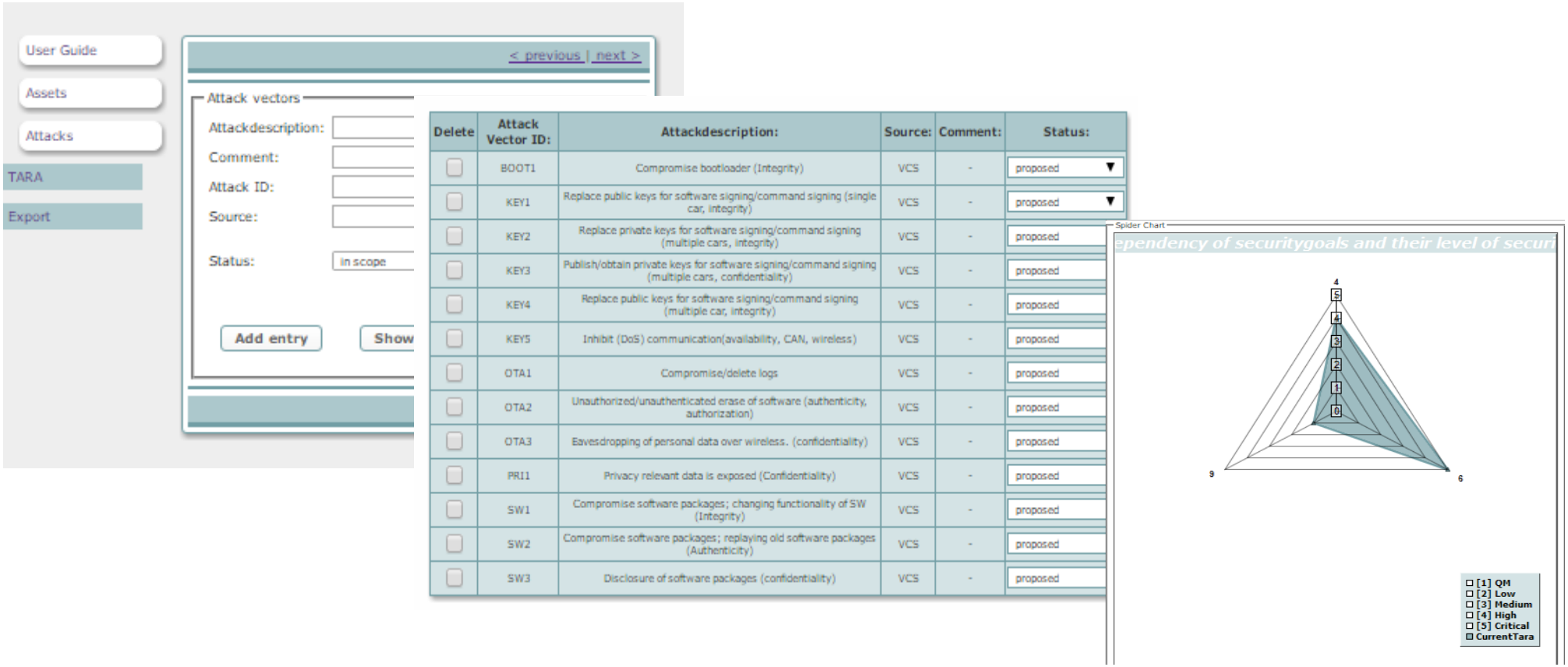
								THREAT LEVEL				SECURITY LEVEL								
Delete	No.:	Asset ID:	Assetname:	CIAAG:	Attack vector:	Effect of attack:	Threat ID:	Threat:	Expertise:	Window of Opportunity:	Equipment, Effort:	Threat Level:	Safety:	Financial:	Operational:	Privacy:	Security Level:	SGID:	Security Goal:	Comment:	Valid
	1	6	ECU software (installed,	Auth	DOS attack	Denial of Service	th - 6	threat6	Proficient	Critical	Standard	0	Mod. Injuries	High	High	Medium	Critical	6	Mitigate DOS attacks	N/A	yes
	2	2	Public signing key (vehicle)	Auth	Publish/obtain	High	th-3	threat3	Layman	Critical	Standard	0	No injury	Low	Medium	Low	High	4	High risk	N/A	yes
	3	4	Log files, security log	Auth	Unauthorized	High	th - 4	threat4	Proficient	Critical	Standard	0	No injury	No impact	No impact	No effect	QM	9	Mitigate	N/A	yes

Apply

< previous | next >

Consider relevant assets/attacks and relate to HARA for safety coverage

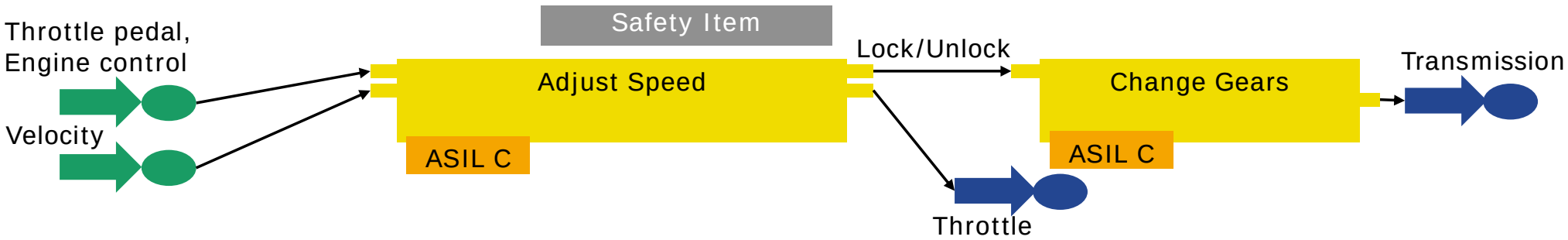
Tool Support: Vector SecurityCheck (3/3)



Delete	Attack Vector ID:	Attackdescription:	Source:	Comment:	Status:
	BOOT1	Compromise bootloader (Integrity)	VCS	-	proposed
	KEY1	Replace public keys for software signing/command signing (single car, integrity)	VCS	-	proposed
	KEY2	Replace private keys for software signing/command signing (multiple cars, integrity)	VCS	-	proposed
	KEY3	Publish/obtain private keys for software signing/command signing (multiple cars, confidentiality)	VCS	-	proposed
	KEY4	Replace public keys for software signing/command signing (multiple car, integrity)	VCS	-	proposed
	KEY5	Inhibit (DoS) communication(availability, CAN, wireless)	VCS	-	proposed
	OTA1	Compromise/delete logs	VCS	-	proposed
	OTA2	Unauthorized/unauthenticated erase of software (authenticity, authorization)	VCS	-	proposed
	OTA3	Eavesdropping of personal data over wireless. (confidentiality)	VCS	-	proposed
	PRI1	Privacy relevant data is exposed (Confidentiality)	VCS	-	proposed
	SW1	Compromise software packages; changing functionality of SW (Integrity)	VCS	-	proposed
	SW2	Compromise software packages; replaying old software packages (Authenticity)	VCS	-	proposed
	SW3	Disclosure of software packages (confidentiality)	VCS	-	proposed

Use heuristic checklists for informed analysis – specifically for the unknown

Case Study Powertrain: Threats and Hazards



Function	Hazard	S/E/C	ASIL
Adjust speed	Speed is unintentionally increased during normal operation in cruise control while driving in a city	S3/E3/C1	C
Change Gears	During driving on high speed (Highway) the gear is changing to a higher gear thus reducing acceleration when it is needed during overtaking	S3/E4/C3	C

Relate identified security threats to safety hazard analysis

VECTOR

Case Study Powertrain: From TARA to Technical Safety/Security Concept

1 Security goal and derived functional security req.

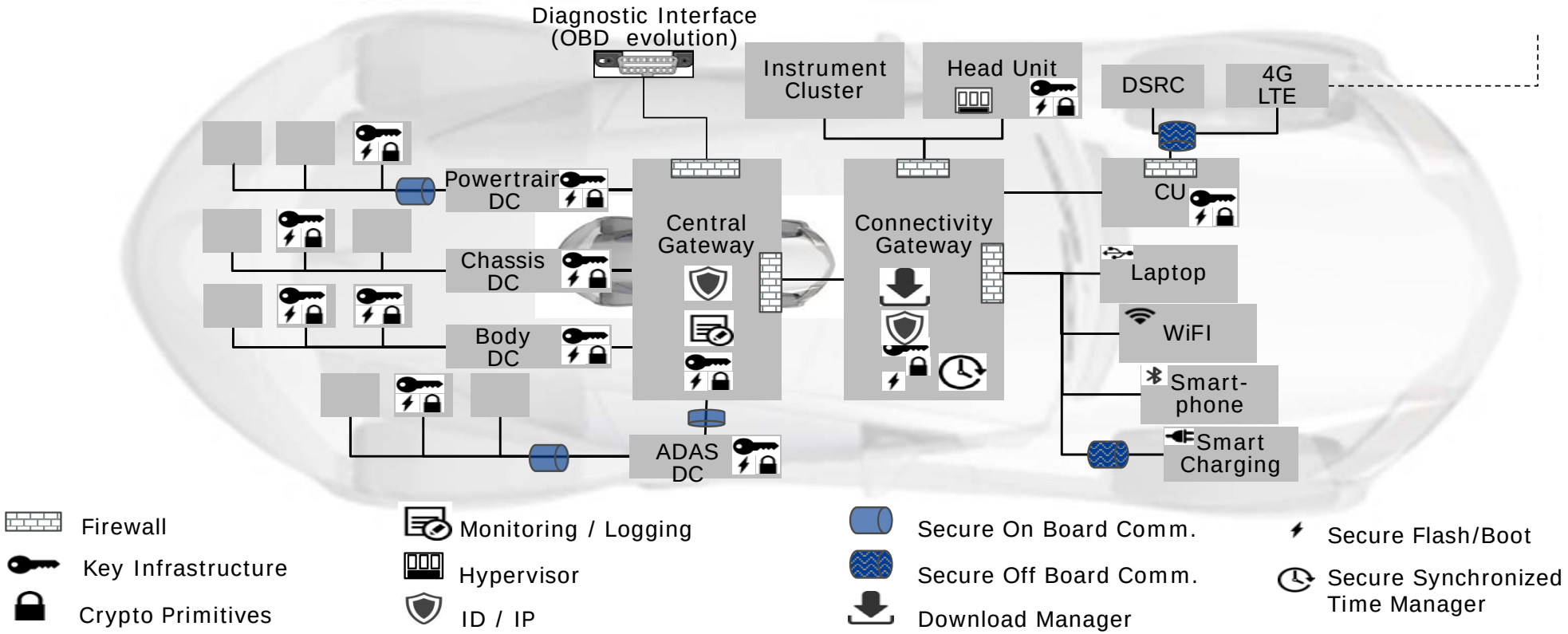
2 Elements of functional architecture

3 Allocation of req. to architecture elements

Security Goal			Functional Security Requirement		Entities of Functional Security Architecture					
ID	Level	Security Goal	ID	Requirement	Inputs			Function Blocks		
					Update sw command	Authenticity and Integrity of sw update (signature)	sw update	Prevent unauthorized update	Install sw in ECU	sw storage (e.g. flash memory)
SG05	High	It shall be prevented that unauthentic software is installed on vehicle ECUs.	FSR 1	The authenticity and integrity of the user_command signal during reading and transmission shall be assured.	x			x		
			FSR 2	The authenticity and integrity of the authenticity signal during reading and transmission shall be assured.		x		x		
			FSR 3	The authenticity and integrity of the sw_update during reading and transmission shall be assured.			x	x	x	
			FSR 4	It shall be assured that the signal allow_update generated from the input signals is calculated correctly.	x	x	x	x		
			FSR 5	The authenticity and integrity of the allow_update signal during transmission shall be assured.				x	x	
			FSR 6	It shall be assured that the signal change_sw generated from the input signals is calculated correctly.					x	x
			FSR 7	If an error with regards to authenticity and integrity during reading, transmission or calculation of signals or the actuator status occurs, the system will not install the sw update.	x	x	x	x	x	x

Transform technical security concept to security requirements.
Handle security requirements exactly like functional requirements.

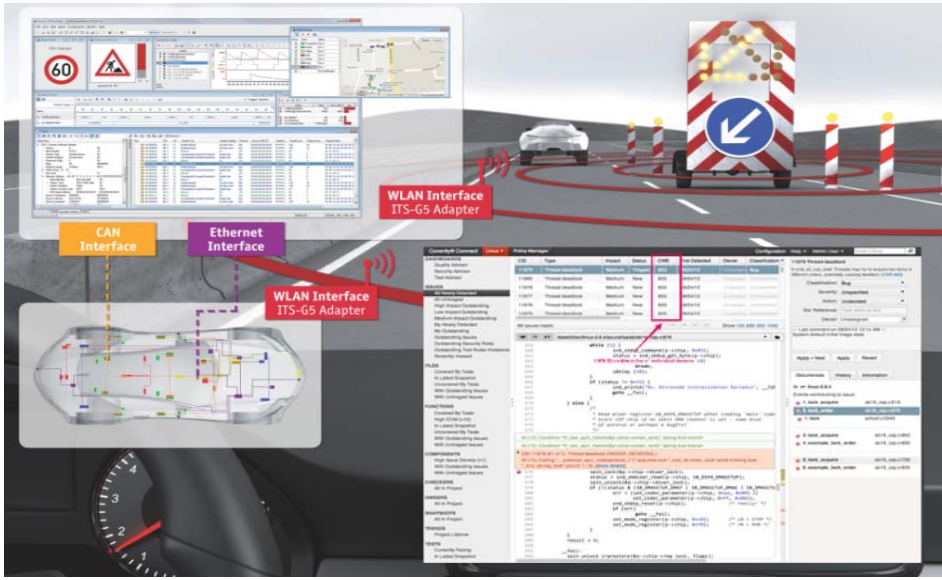
Case Study Powertrain: Separate Concerns



Incrementally harden your E/E and IT functions, architectures and components.

Security by Design: Implementation, Verification and Validation

- **Design**
  - Use programming rules such as MISRA-C
  - Avoid injectable code
  - Enforce high cryptographic strength
  - Assign least privileges to any function
  - Static and dynamic code analysis

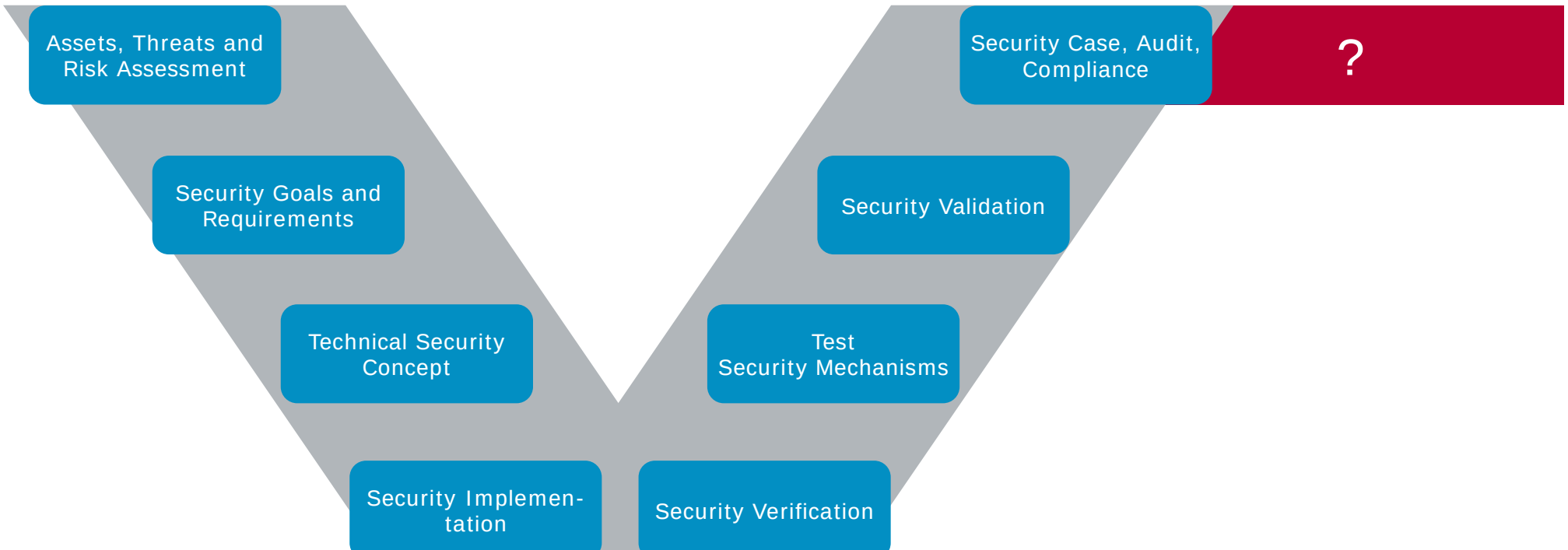


- **Test**
  - Encryption cracker, vulnerability scanner
  - Network traffic analyzer, stress tester, interface scanner
  - Layered fuzzing testing

- **Life Hacking**
  - Penetration testing
  - Governance and social engineering attacks

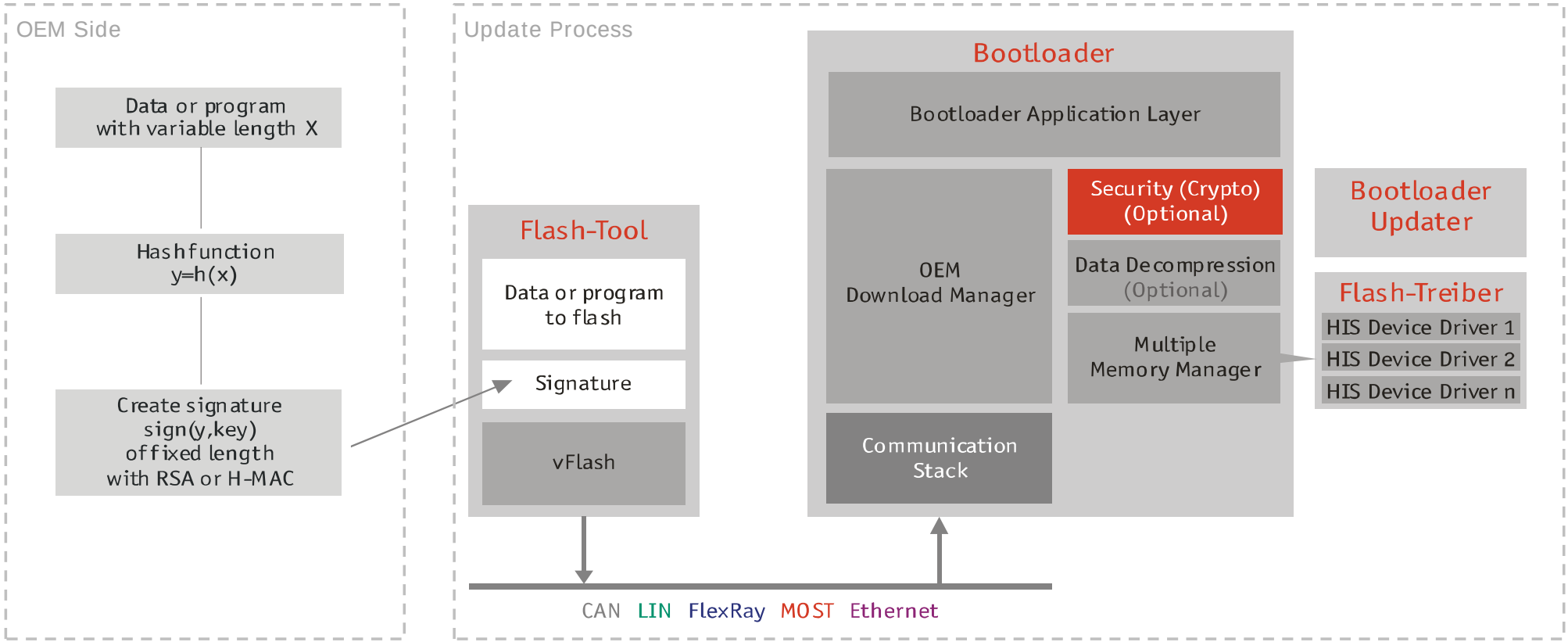
Test for the unknown. Run automatic regression tests with each delivery.

Consider Risk-oriented Development throughout the life-cycle



Begin with the end in mind:
After Sales Support needs early development decisions:
Resilience, fail operational strategies, alert center, repair / OTA, governance

Game Changer: OTA Facilitates Security Across the Life-cycle

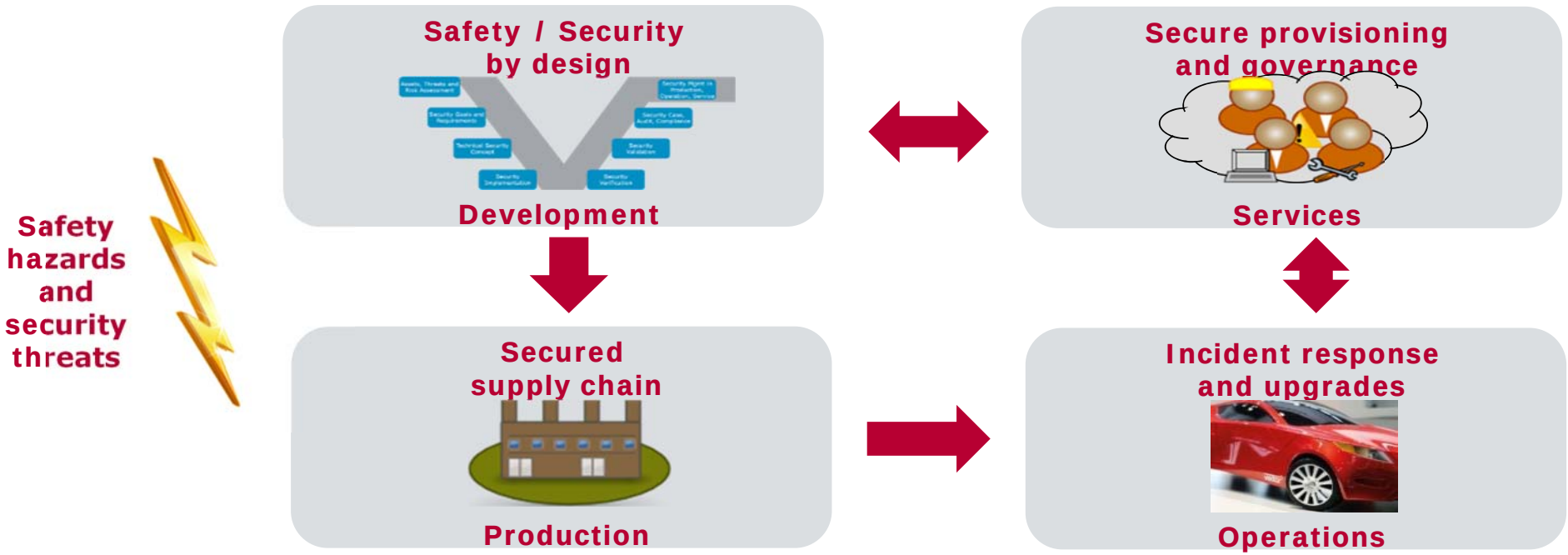


There is no security without continuous **Over the Air (OTA)** update strategy

Agenda

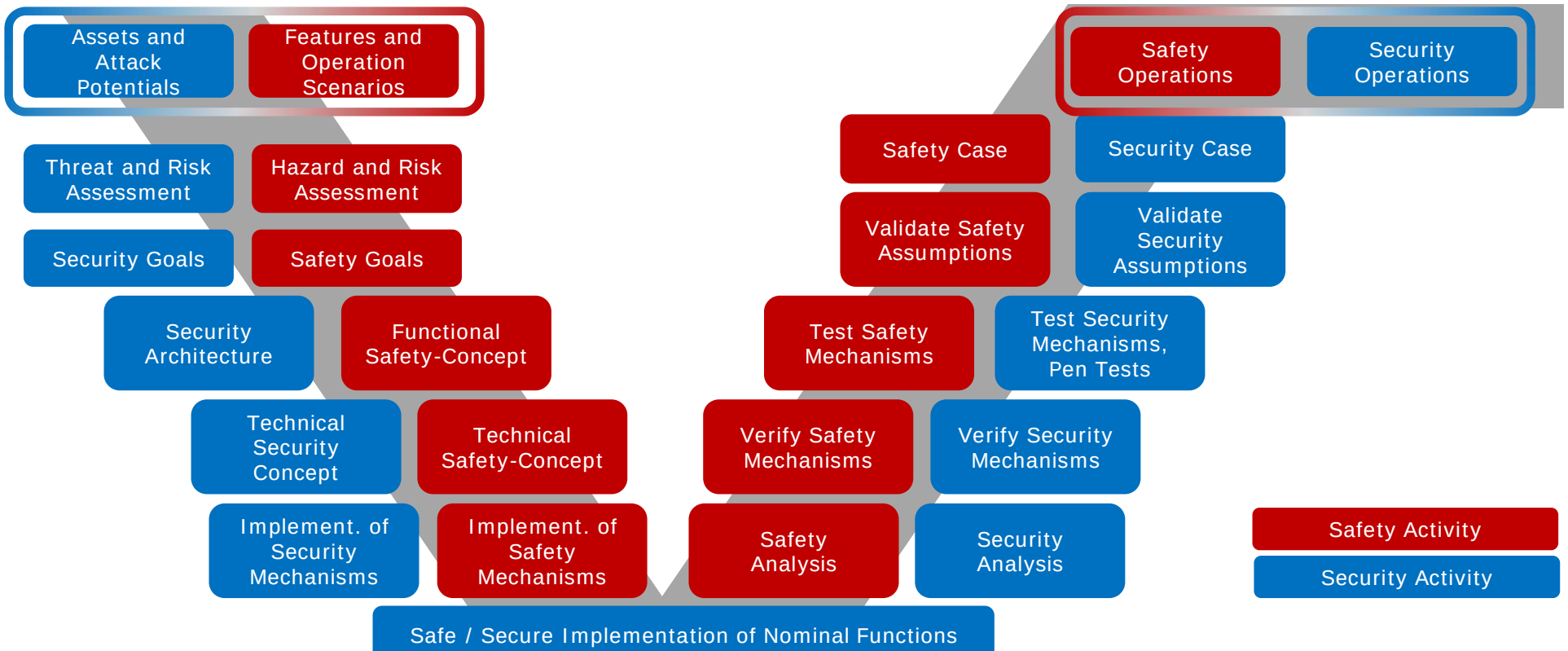
VECTOR

Risk-Oriented Development Must Cover the Entire Life-Cycle



- Systematic safety and security engineering
- Scaleable incident monitoring and response
- Multiple modes of operation (normal, attack, emergency, fail operational, fail safe, etc.)

Integrated Development for Safety and Security



- Similar to Safety, Security needs to be an integrated part of the development process.
- Build security upon existing safety governance.

VECTOR

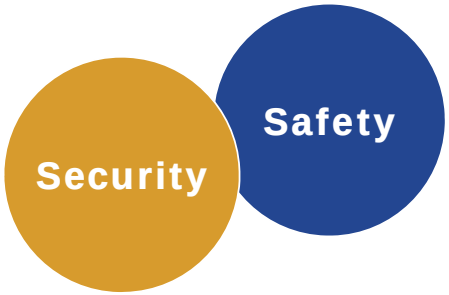
Conclusion: Combine Synergistic Safety & Security Techniques Across Life-Cycle

Security Techniques	Cost	Benefit
Quick Wins		
Vector SafetyCheck and Vector SecurityCheck for risk assessment and implementation guidance	Low	Medium
Role of Virtual Security Manager	Medium	High
Safety and Security Training and compliance audits	Low	High
Technology		
Secure boot, communication, storage	High	High
Secure run-time (e.g. CFI, DFI, MACs)	High	High
IDS/IPS, Firewall with adjusted policies	Medium-High	Medium
Process and Governance		
Development for safety and security	Medium-High	High
Test strategy, e.g. Fuzz Testing, Penetration Testing etc.	High	Medium
Secure Key Management	High	Medium
Security task force and response team (internal or virtual)	Medium	High

VECTOR

Safety and Security Matter

- **Safety and Security demands a thorough culture change**
  - Build necessary competences for safety and security
  - Do not simply copy-paste elements from current standards
  - Enforce strong governance end-to-end



- **Risk-oriented development is the order of the day**
  - Apply systems engineering for safety and cyber-security
  - Systematically use professional tools, such as PREEvision and CANoe
  - Close known vulnerabilities as soon as possible, preferably with OTA
  - Audit your suppliers and achieve a holistic perspective on risks and solutions
  - Use the hacker's view for security risks, and not that of developer or safety expert

To know your enemy, you have to become your enemy. (Sun Tzu, The Art of War)

In other words: **Think like a Criminal and preemptively act as an Engineer.**

Vector Offers a Comprehensive Portfolio for Cyber-Security and Functional Safety

Vector Cyber-Security and Safety Solutions

Security and Safety Consulting

AUTOSAR Basic Software

HW based Security

Tools (PLM with PREEvision, Architecture, Test, Diagnosis etc.)

Engineering Services for Safety and Security

Thank you for your attention.
For more information please contact us.

Passion. Partner. Value.

Vector Consulting Services

www.vector.com/consulting
consulting-info@vector.com
Phone: +49 711 80670-0