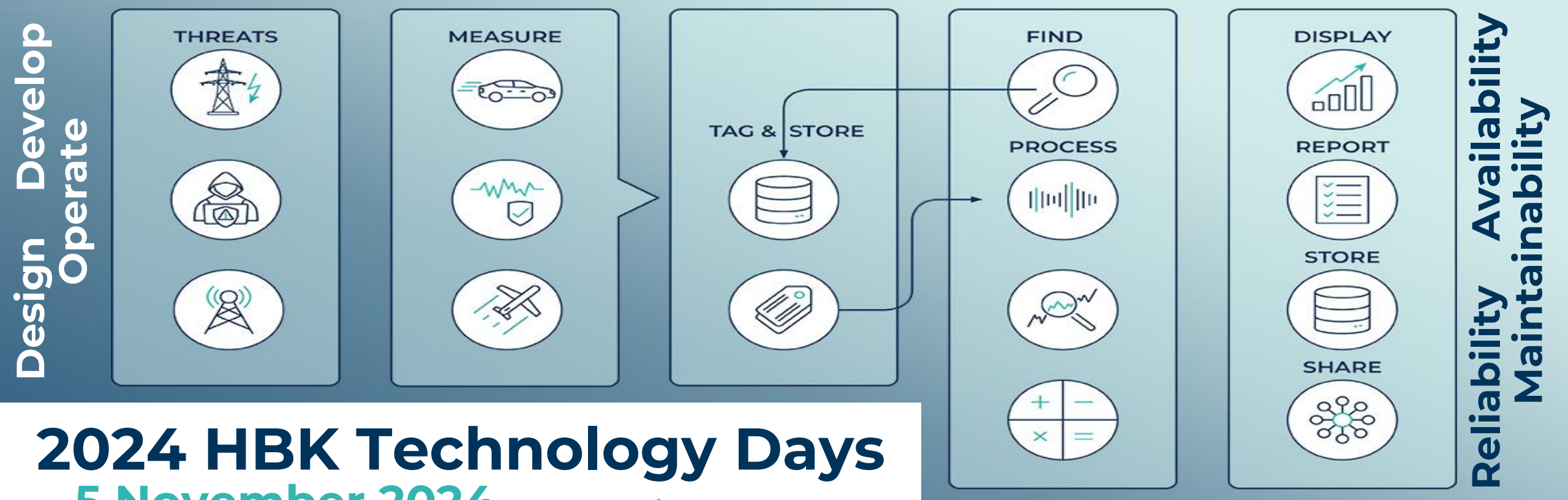




2024 HBK Technology Days

5 November 2024



Session 2: Minimising Cyber Threats to Sensors, Vehicles and Software

- Agile cybersecurity for the software-defined vehicle

Christof Ebert,
Vector Consulting Services



Agile Cybersecurity for the Software-Defined Vehicle (SDV)

Dr. Christof Ebert, Vector Consulting Services, HBK Technology Days, 5. Nov. 2024

Agile cybersecurity for the software-defined vehicle

▲ Abstract

- The software-defined vehicle (SDV) converges product IT in the vehicle with enterprise IT in the cloud and backbone infrastructure. Cybersecurity matters for SDV. There is no functional safety without security. With software and data being manipulated, the initial qualified, verified, or homologated functionality of systems is no longer guaranteed. With the exploding challenges of cybercrime, OEMs and suppliers must achieve adequate protection against manipulations of their enterprise and product IT systems. While SDV eases the evolution of functions based on a flexible hardware platform, it has more cybersecurity risks. SDV are a primary target for hackers because systems and components have high levels of always-on, connectivity, and smart application programming interfaces (APIs) for software updates and facilitate remote attacks. Many companies have no established product cybersecurity program and dedicated R&D security team. Standardized software stacks reduce the entry barrier for malicious actors. Starter kits for all sorts of malware are available, increasingly fueled by AI tools. However, generative artificial intelligence also has the potential to make software-defined systems more robust and secure, as we show in this presentation.

Agile cybersecurity for the software-defined vehicle

▲ Abstract (continued)

- This presentation shows agile cybersecurity development for SDV lifecycle risk mitigation:
 - Cybersecurity risks in SDV
 - Agile systems Engineering and test strategies for adaptive software
 - The dynamic safety case and its maintenance throughout the life cycle
 - Agile documentation of changing software for OTA and SUMS
 - Mitigating AI driven IPR risks as software productivity tools try to capture data
- To practically show innovative cybersecurity engineering we have developed generative AI-based methodologies for security analysis and design. The presentation will go beyond only AI and show methods to mitigate cybersecurity risks in SDV, such as deploying novel test coverage methods for grey-box Pen-Test. Practical examples will provide insight how to best mitigate cybersecurity risks with SDV.

Agile cybersecurity for the software-defined vehicle

- ▲ About the presenter, Christof Ebert
Managing Director, Vector Consulting Services
 - Christof Ebert is the managing director of Vector Consulting Services. A trusted advisor for companies and member of industry boards, he supports clients worldwide to sustainably improve product strategy and product development and to manage organizational changes. Dr. Ebert is teaching at university of Stuttgart and Sorbonne Paris. He has founded the Robo-Test incubator and holds several patents in the field of autonomous systems.



Agile Cybersecurity for the Software-Defined Vehicle (SDV)

Dr. Christof Ebert, Vector Consulting Services, HBK Technology Days, 5. Nov. 2024

Agenda

1.

Welcome

2.

Software-Defined Vehicle Trends and Challenges

3.

Patterns for Successful SDV Transformation

4.

Where Do YOU Go from Here?

Welcome

Who We Are

Vector Group



Employees:
> 4,500 Vectorians

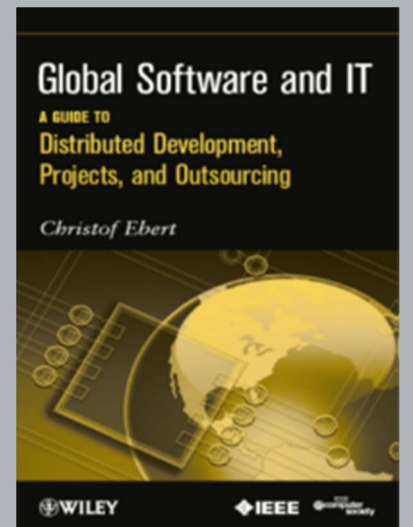
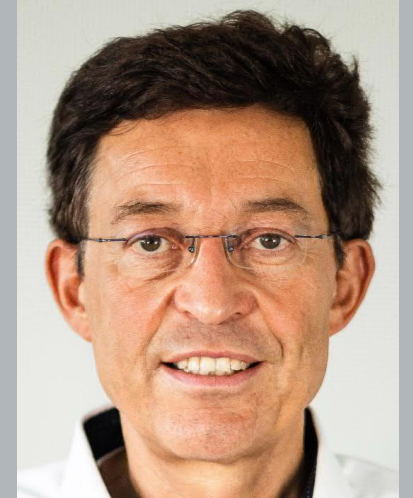
Customers:
> 9,000 companies
in 76 countries



Turnover:
1.16 bn €
in 2023

Christof Ebert

- ▶ Managing director of Vector Consulting Services.
- ▶ Supporting clients worldwide in technology and agile transformation.
- ▶ 12 years in senior positions with a global IT leader.
- ▶ Patents in AI and autonomous systems
- ▶ Member of several industry advisory boards.
- ▶ Ed. Boards of IEEE Computer, IEEE Software, JSS, SQJO
- ▶ Professor at Stuttgart University and the Sorbonne in Paris.



www.vector.com/consulting

Agenda

1.

Welcome

2.

Software-Defined Vehicle Trends and Challenges

3.

Patterns for Successful SDV Transformation

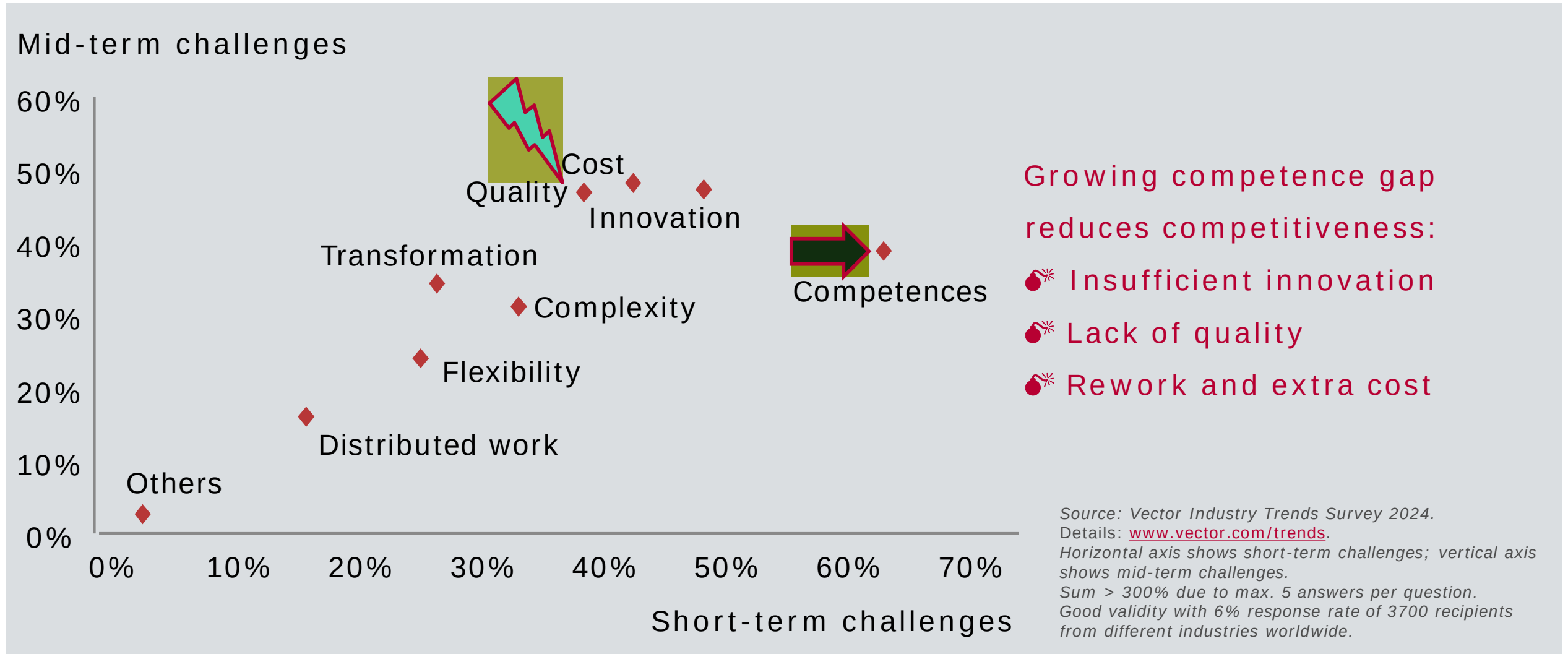
4.

Where Do YOU Go from Here?

Fast Technology Evolution...

Today		Tomorrow
Business	Value by tangible HW	Disruptive value generation with software
Organization	Function oriented	Distributed, dynamic ecosystems, cross-functional
Culture	Engineering	Software-Defined, Entrepreneurial, resilience
Risks	Exploding cost and delays	Legal demands on liability, security, etc.
IT	Separate ivory towers	Convergence of enterprise IT and product IT
Software	Components, libraries	Adaptive stacks, AI + ML, Green IT
Architectures	Monolithic, functions	Flexible, cloud+edge, SOA, micro-services
Testing	Ad-hoc, blind spots	Efficient and effective, TDD, TDRE, cognitive
Competences	Specialized, static	Learning, CS and engineering
Methodologies	Organic, technical debt	Systems engineering, modeling, low-code
Process/Tools	Heavy, inefficient	Agile, flexible, sharing, ContinuousX, DevOps

...but Insufficient Competences

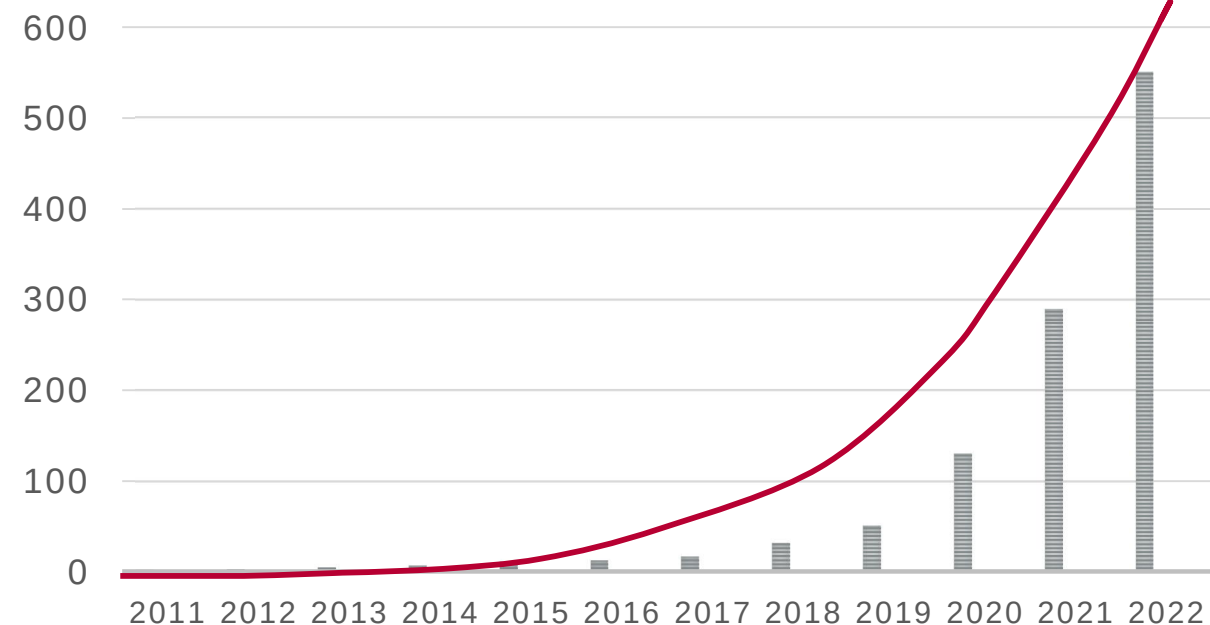


Vector provides tailored consulting solutions to stay competitive in times of uncertainty.

IT Convergence Open The Doors for Wide Range of Attacks Across Industries

- ▶ Industrial IoT is a primary target due to its impact on our society and economy
- ▶ Smart APIs present a new and significant industry-wide attack vector
- ▶ Hacking tools and knowledge advance fast and thus grow the window of opportunity
- ▶ Convergence of enterprise IT and product IT increases attack surfaces are fast evolving, and practically all (>95%) attacks are remote.
- ▶ Functional safety is blind spot of many cybersecurity programs.

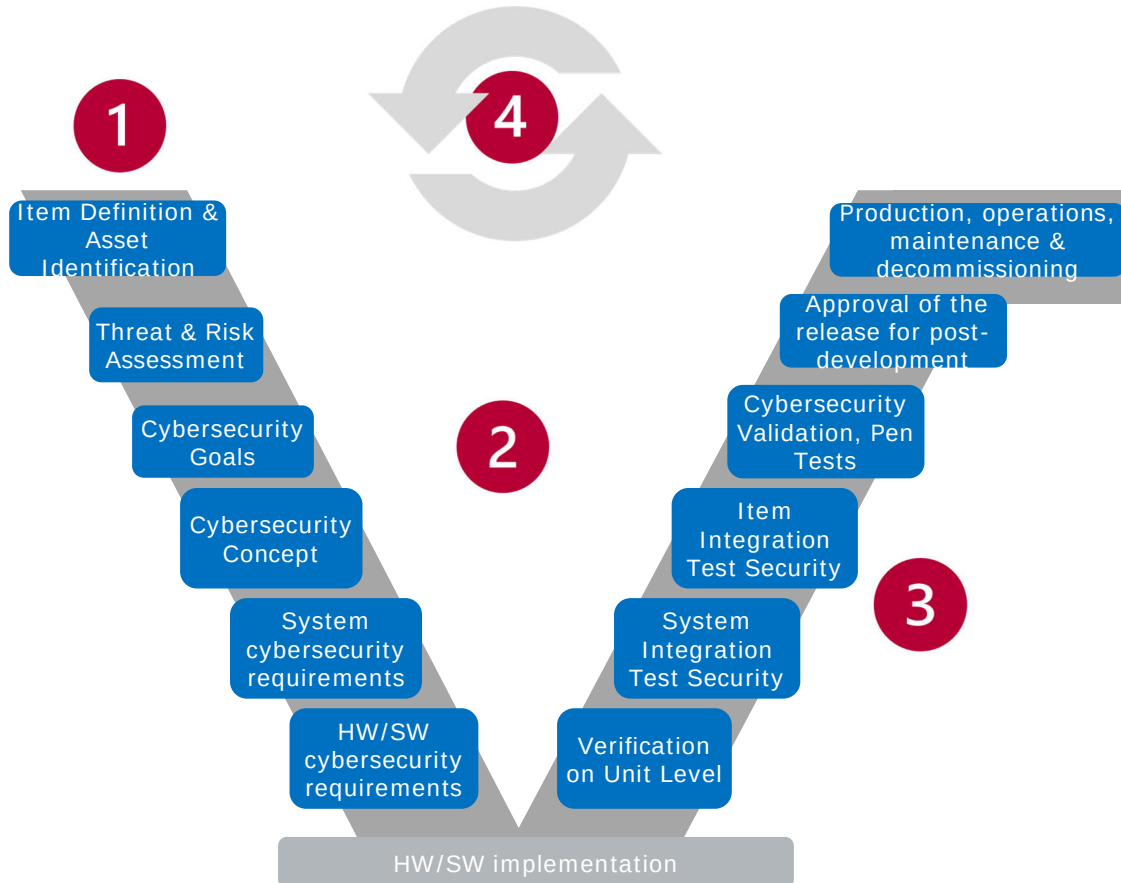
IIoT critical cybersecurity attacks



Sources: Vector 2024, www.securityweek.com 2023; IBM 2022 <https://www.ibm.com/security/data-breach/threat-intelligence>, Ponemon Institute study with 593 security and policy professionals; Results of 2023 Open-Source Security & Risk Analysis Report, Synopsis; Harman 2020; Continental 2020

Cybercrime is more profitable than the global illegal drug trade.
Current damage is estimated at 600 billion USD a year (400 billion USD for drug trafficking)

Growing Cybersecurity Weaknesses Observed with Vector Customers



1. Requirements

- ▶ Insufficient understanding of possible cyberattacks, e.g., diagnostics, labeling on PCB, etc.
- ▶ Insufficient supply-chain agreements for legal and technical responsibilities between OEM and suppliers

2. Lifecycle

- ▶ Overlapping unstructured documents for Security/Safety with many inconsistencies
- ▶ Incomplete operating environments, e.g., Production, diagnostics, SUMS
- ▶ Poor traceability cause inconsistencies between requirements and product and test

3. Test

- ▶ Lack of V&V strategy, such as minimum viable regression concept
- ▶ Uninformed security test, such as black-box Pen-Test

4. CS monitoring

- ▶ Insufficient coverage due to missing understanding of demands and tooling
- ▶ Incomplete, inconsistent and not traceable BOM

Legal Situation: Product Liability Needs Standards

Product Liability:
A product, that is put in service,
must provide the level of safety which can be expected by general public.

Functional Safety

- ▶ Product IT: IEC 61508 (electrical systems), ISO 26262 (automotive), IEC 60601 (medical)
- ▶ AI: ISO 21448 (SOTIF), ISO TS 5083 (automated driving), ISO/PAS 8800 (AI)
- ▶ Coexistence of standards: ISO/TR 4804 (development); ISO shared methods

Cybersecurity

- ▶ Product IT: ISO/SAE 21434 (automotive cybersecurity), ISO 14971 (medical device cybersecurity), ISO 27403 (IoT security)
- ▶ Enterprise IT: ISO 27001 (Security mgmt), ISO 15408 (Common Criteria), TISAX (Trusted Information Security Assessment Exchange)

Certification & Homologation

- ▶ Audits: ISO 19011 for all sort of management systems
- ▶ Automotive: Approval for vehicle type and updates based on UNECE, e.g., R.155 CSMS (Cybersecurity Management System), Chinese GB 44495
- ▶ Medical: FDA certification
- ▶ Railway: EBA etc. based on e.g., ISO 22163

Process Maturity: ISO 330xx, Product Quality: ISO 250xx
Methodological frameworks such as ASPICE, are demanded by “higher-level” quality standards

Product Development Process: ISO 9001, ISO 16949 (automotive), etc.

Agenda

1.

Welcome

2.

Software-Defined Vehicle Trends and Challenges

3.

Patterns for Successful SDV Transformation

4.

Where Do YOU Go from Here?

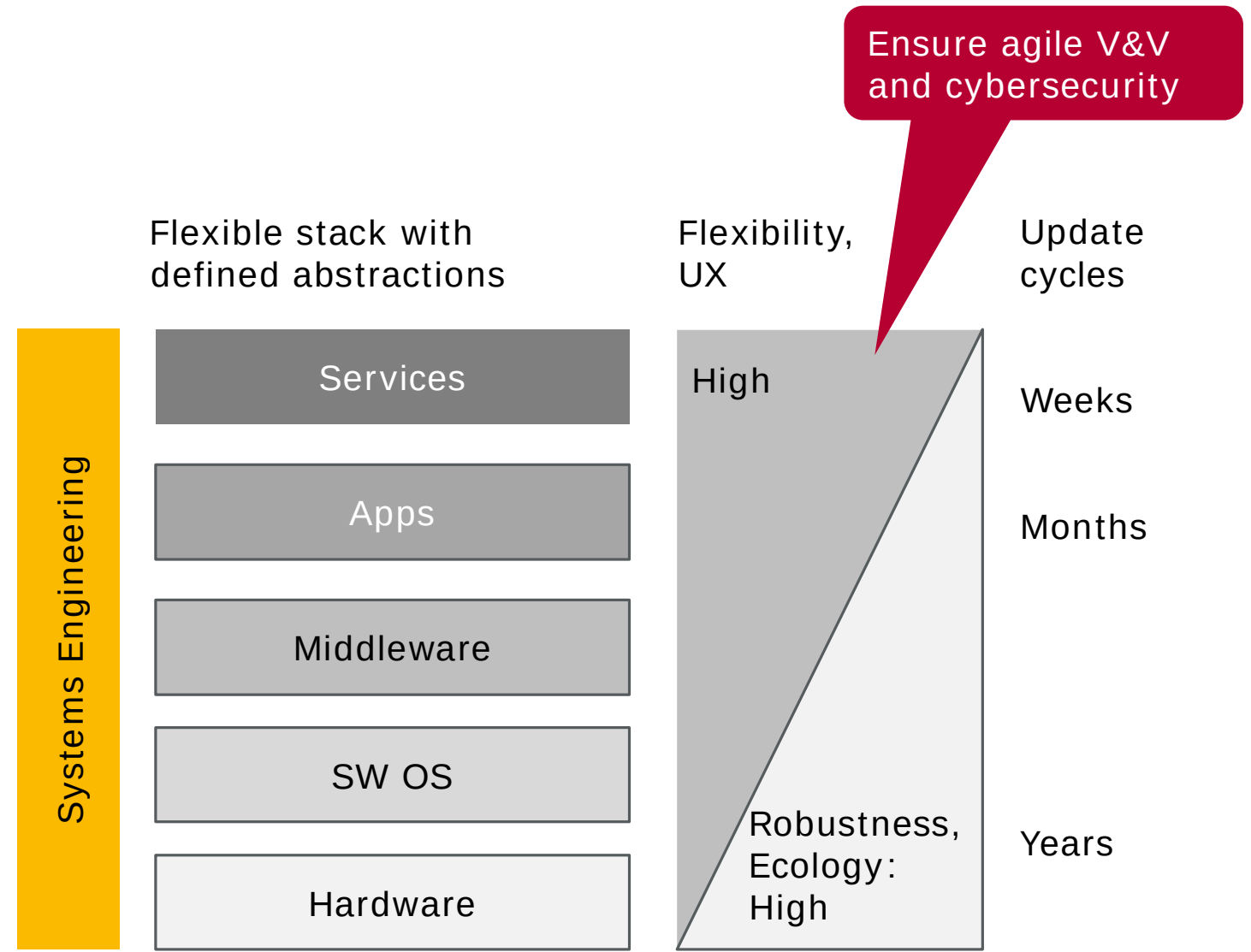
Solution: System Modeling and Simulation

Motivation:

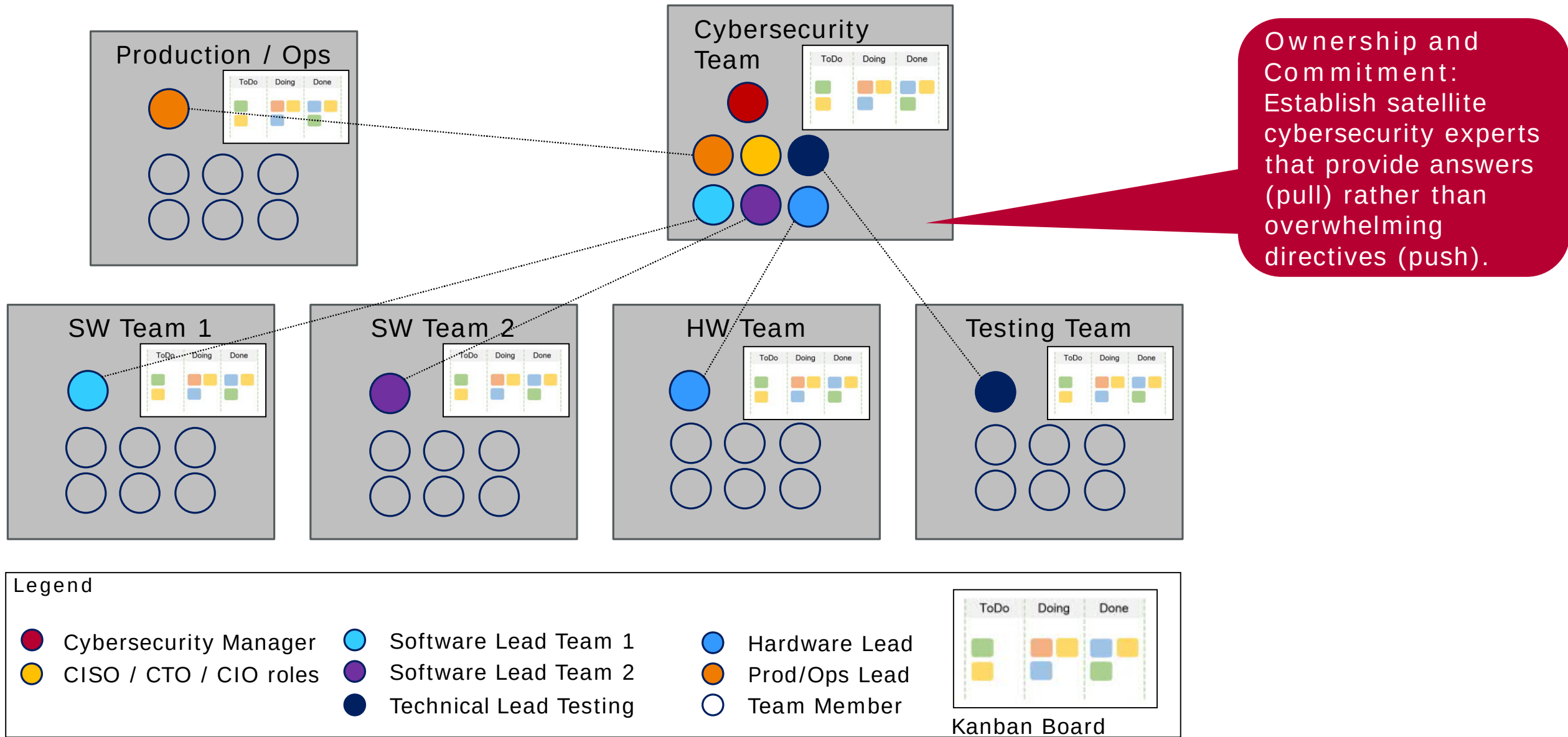
- ▶ Address complexity-competence gap with adequate abstractions
- ▶ Cover complex constraints with system of systems view
- ▶ Mitigate growing business risks such as legal demands
- ▶ Supplier management and flexibility for components and interfaces.

Current focus:

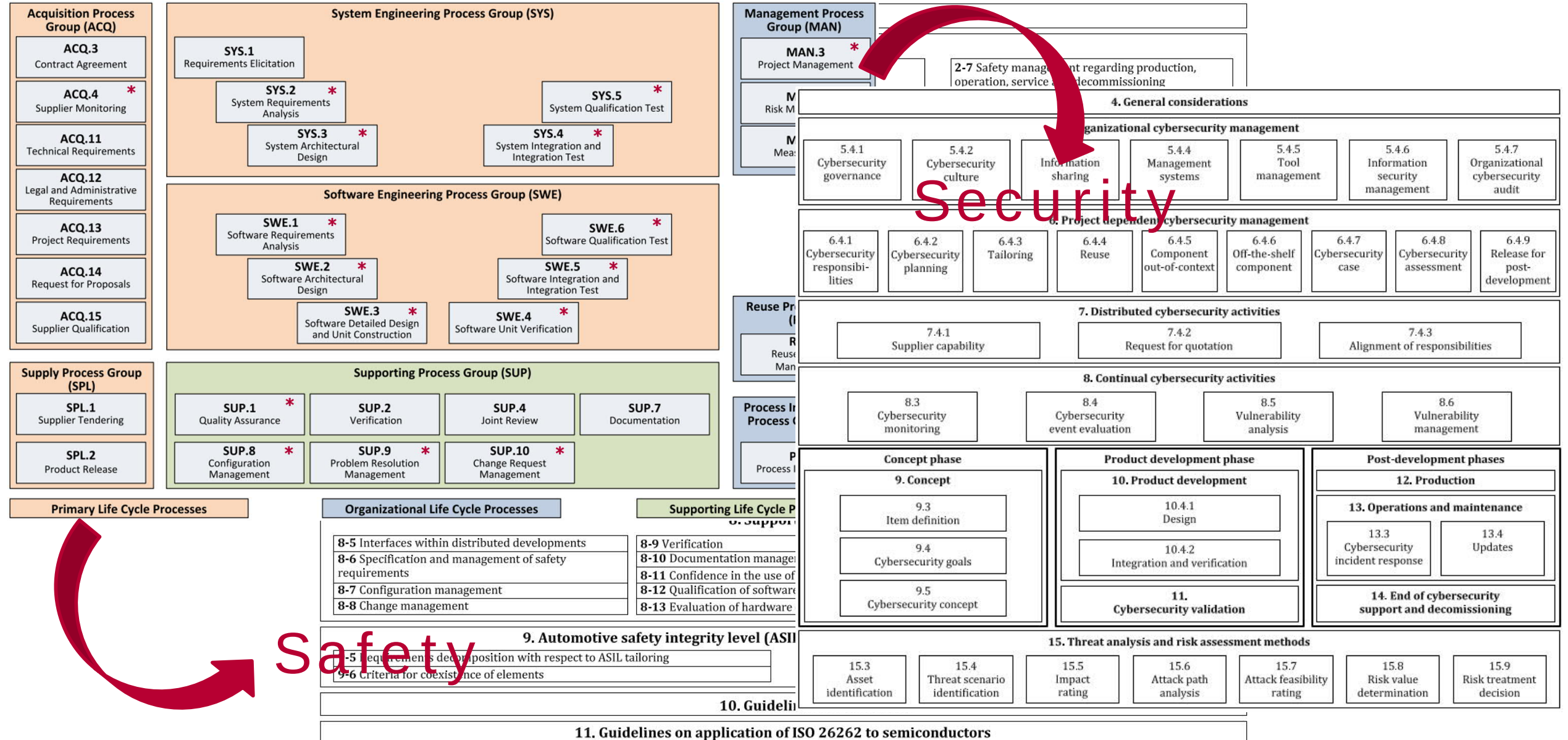
- ▶ Modeling architecture abstractions for quality attributes, e.g., safety, variance management, evolution
- ▶ Simulation and XiL V&V
- ▶ AI-based co-piloting to navigate between layers



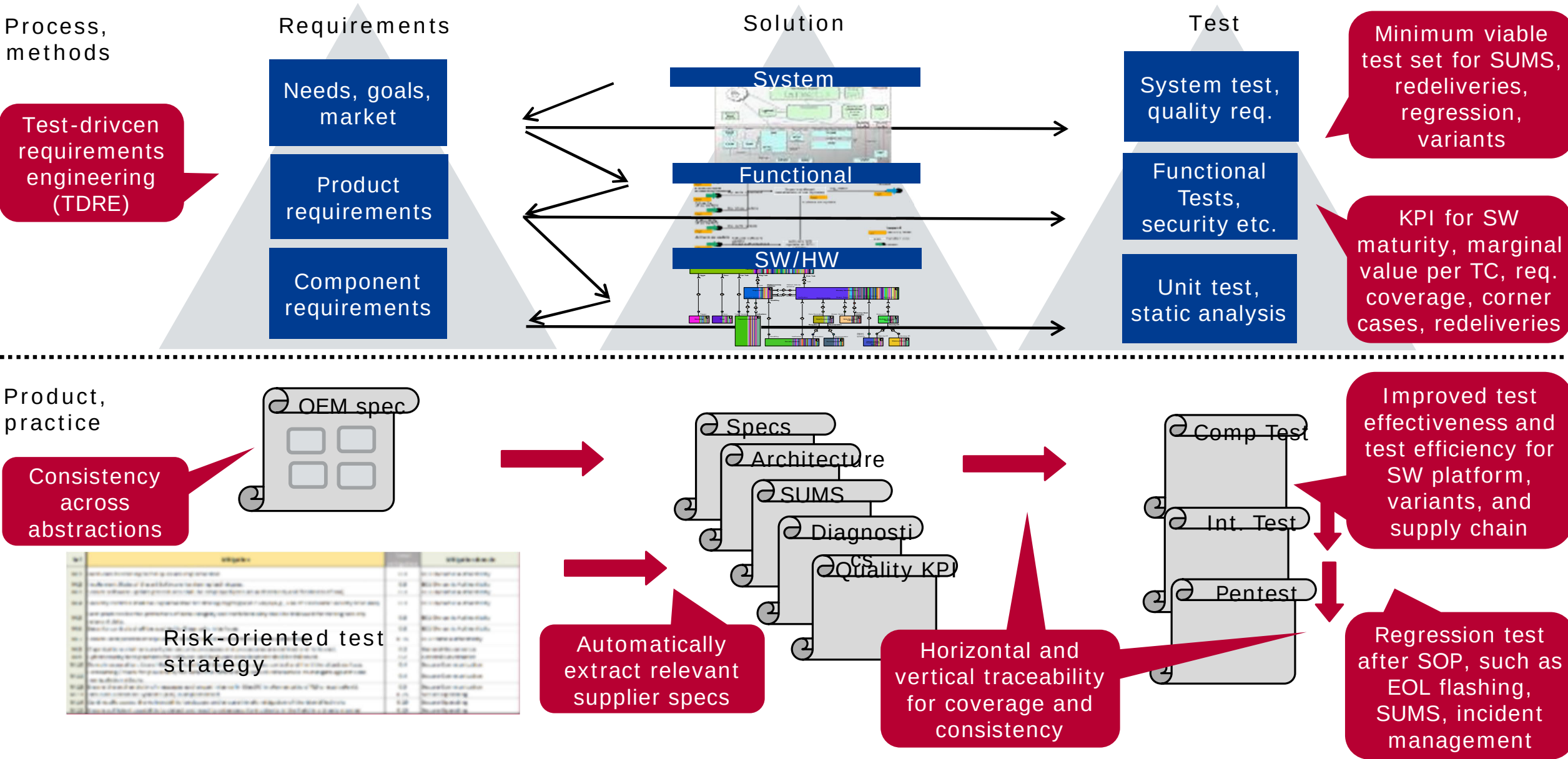
Solution: Pull Instead of Push



Solution: Efficiently Implement Mandatory Standards



Solution: Ensure Consistency with Test-Driven Requirements Engineering (TDRE)



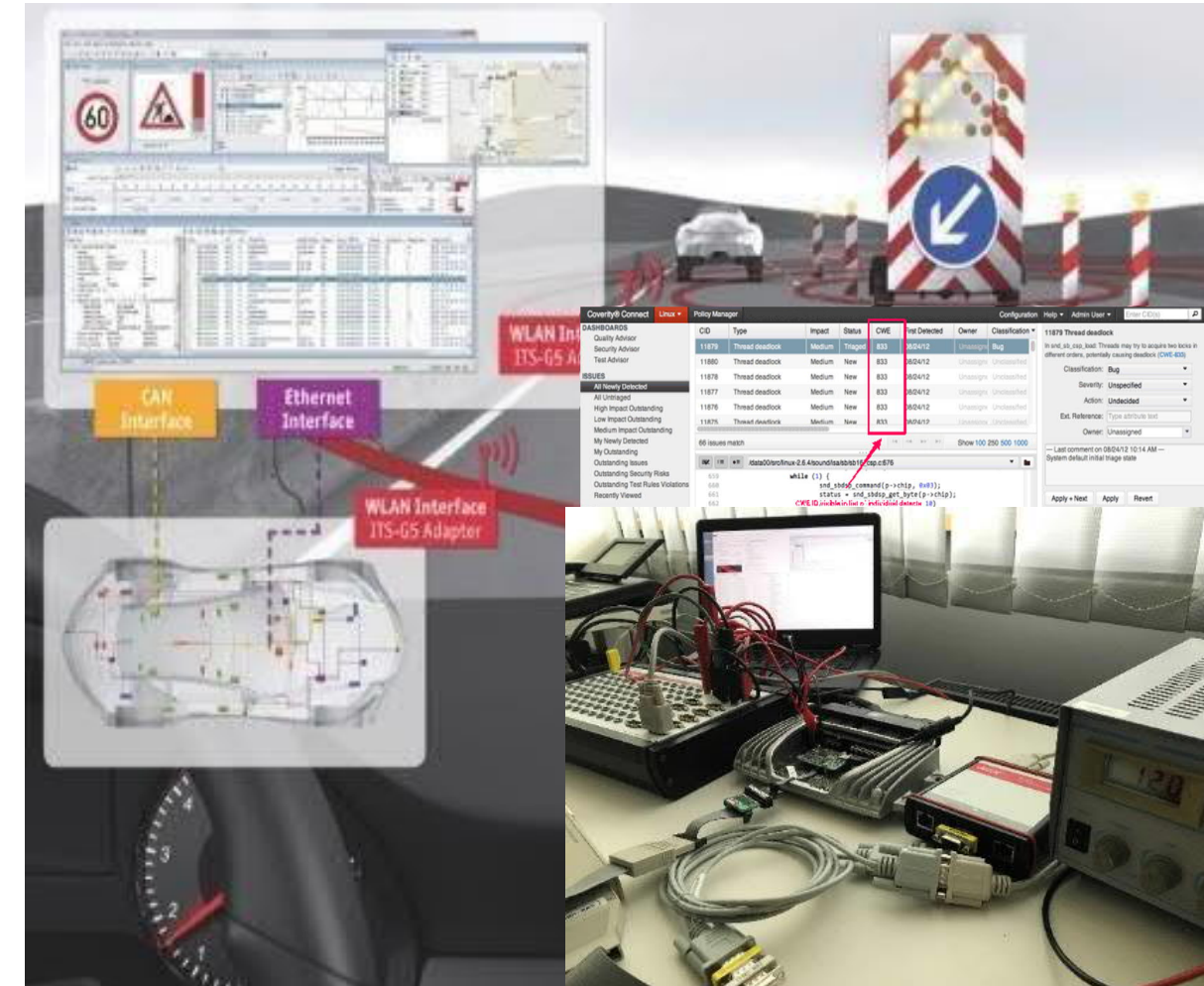
Solution: Combine Security-By-Design and Security-by-Lifecycle

Design

- ▶ Defensive coding, e.g., memory allocation, avoid injectable code, least privileges
- ▶ Programming rules such as MISRA-C, SEI CERT
- ▶ High cryptographic strength in line with performance needs
- ▶ Key management and HW-based security
- ▶ Awareness and governance towards social engineering

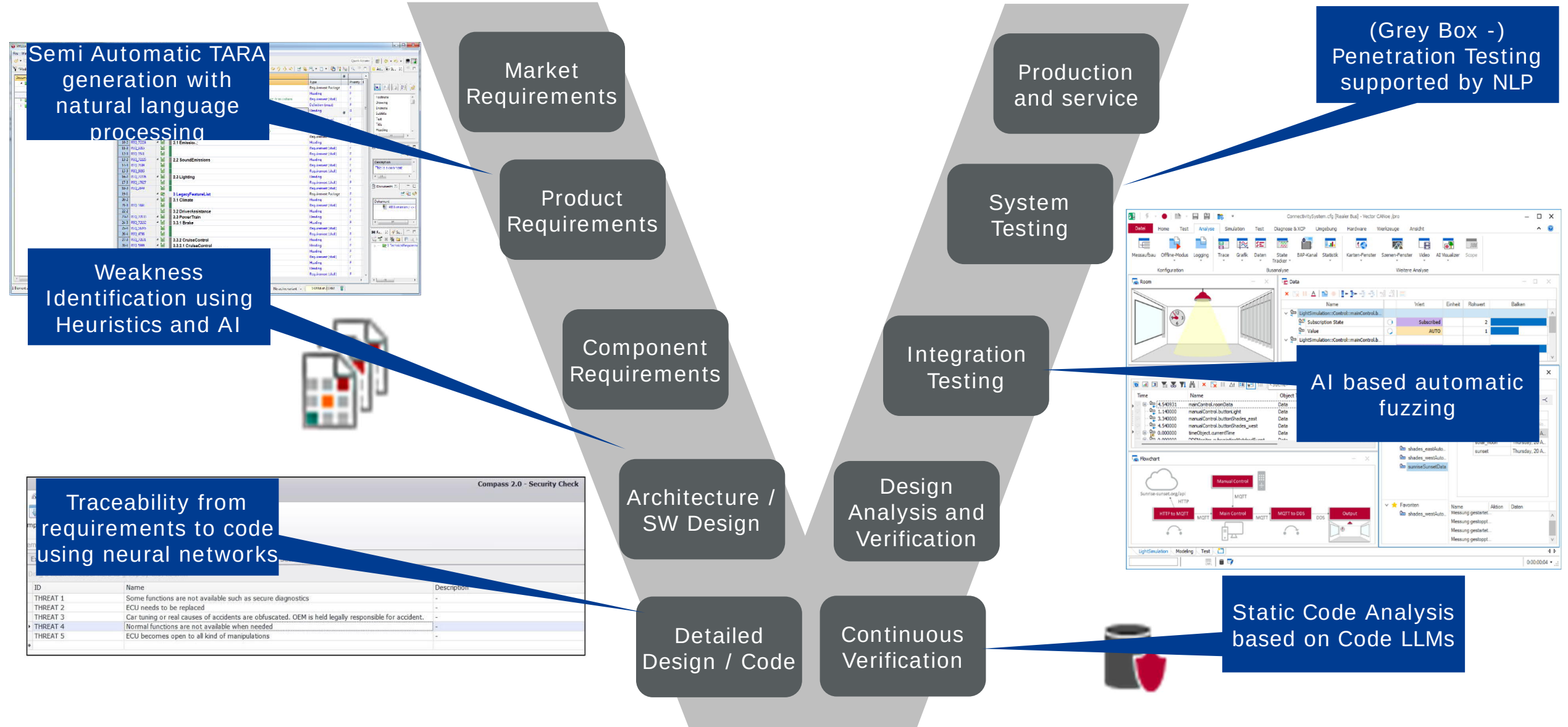
V&V Methods and Tools

- ▶ Static / dynamic code analyzer
- ▶ Unit test with focused coverage, e.g., MCDC
- ▶ Interface scanner, layered fuzzing tester, encryption cracker, vulnerability scanner
- ▶ Risk-based penetration testing

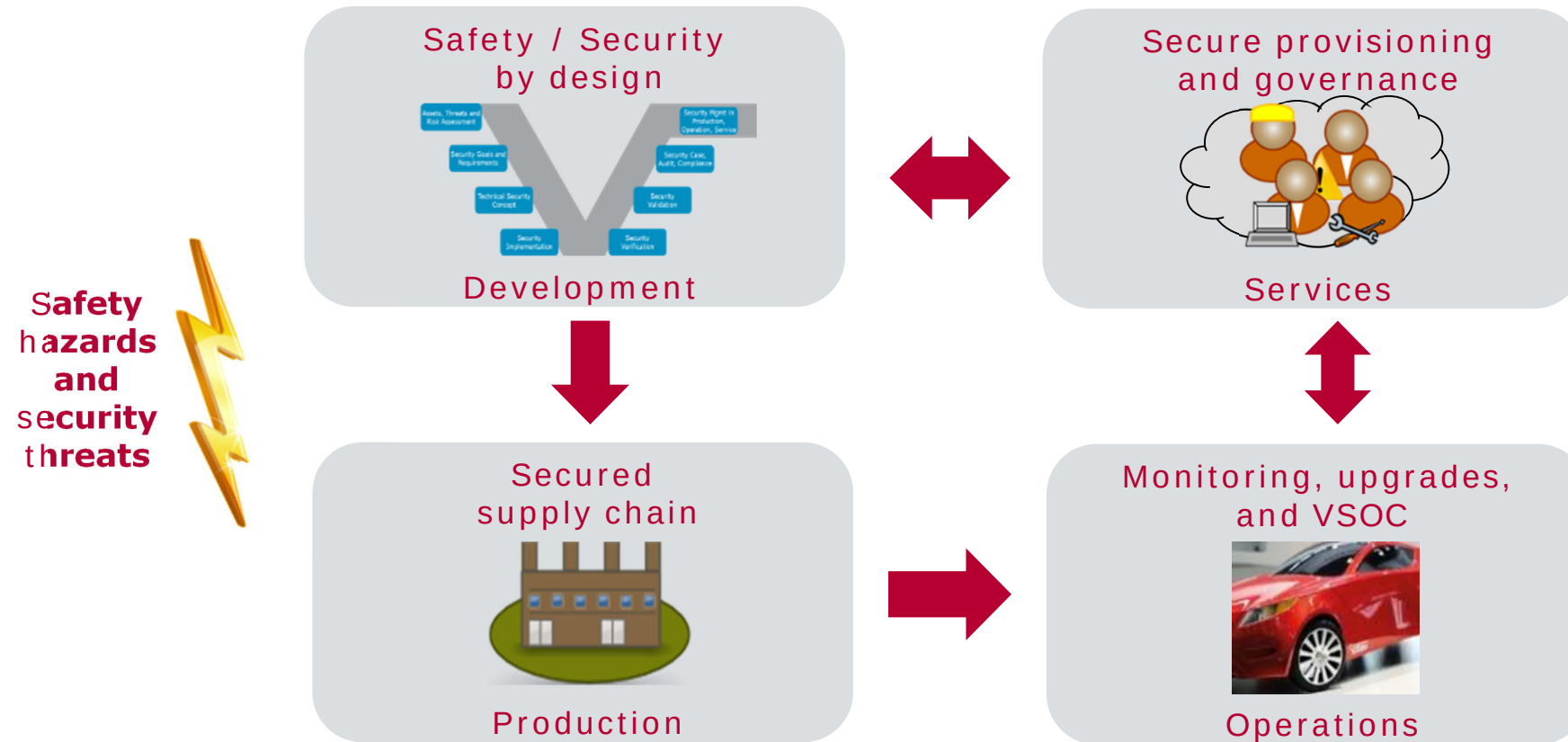


Systematically apply cybersecurity principles during development and test.
Ensure automatic regression tests are running with each delivery.

Solution: Introduce Cybersecurity for AI and AI for Cybersecurity



Solution: Connect VSOC with Analytics for Fast Resolution and Recovery



Needs for safety and security along the life-cycle:

- ▶ Systems and service engineering methods for embedded and IT
- ▶ Scalable techniques for design, upgrades, regressions, services
- ▶ Multiple modes of operation (normal, attack, emergency, etc.)

Agenda

1.

Welcome

2.

Software-Defined Vehicle Trends and Challenges

3.

Patterns for Successful SDV Transformation

4.

Where Do YOU Go from Here?

Risk-Oriented Cybersecurity for the Software-Defined Vehicle

- ▶ Risk-oriented cybersecurity
 - ▶ Apply systems engineering for cybersecurity
 - ▶ Systematically use professional tools such as Threat Analysis and Risk Assessment (TARA), vulnerability analysis, secure by design methods, hacking invitations, and various penetration testing
 - ▶ Audit your suppliers and achieve a holistic perspective on risks and solutions
- ▶ Culture change
 - ▶ Advance a cybersecurity culture across functions
 - ▶ Enforce strong governance end-to-end, not just encryption and key management

OEM:

“Good visibility on cybersecurity progress with my suppliers.”

Component Supplier:

“Efficient cybersecurity with Vector Consulting experiences.”

OEM:

“Collaboration effort was reduced by 20% with agile systems engineering.”

Use Vector professional support to close competence gaps.

Value from Vector

- ▶ Automotive Cybersecurity articles
 - ▶ Penetration Testing, atz, 2024
<https://www.springerprofessional.de/en/penetration-testing-for-automotive-cybersecurity/19219750>
 - ▶ Security Test, IEEE Software,
<https://ieeexplore.ieee.org/document/8994839>
 - ▶ Cybersecurity for the Software-Defined Vehicle, atz, 2024
- ▶ Artificial Intelligence for Cybersecurity
 - ▶ IEEE Software,
<https://ieeexplore.ieee.org/document/10339105>
 - ▶ Generative AI for automotive cybersecurity, atz, 2024
- ▶ Reference Architectures for the IoT
 - ▶ IEEE Software,
<https://ieeexplore.ieee.org/document/7367994>
- ▶ Agile Systems Engineering
 - ▶ ATZelectronics worldwide,
<https://www.springerprofessional.de/en/agile-systems-engineering/23788554>



Contact us and achieve value

Passion. Partner. Value.
Vector Consulting Services



www.vector.com/consulting



consulting-info@vector.com



+49-711-80670-1520

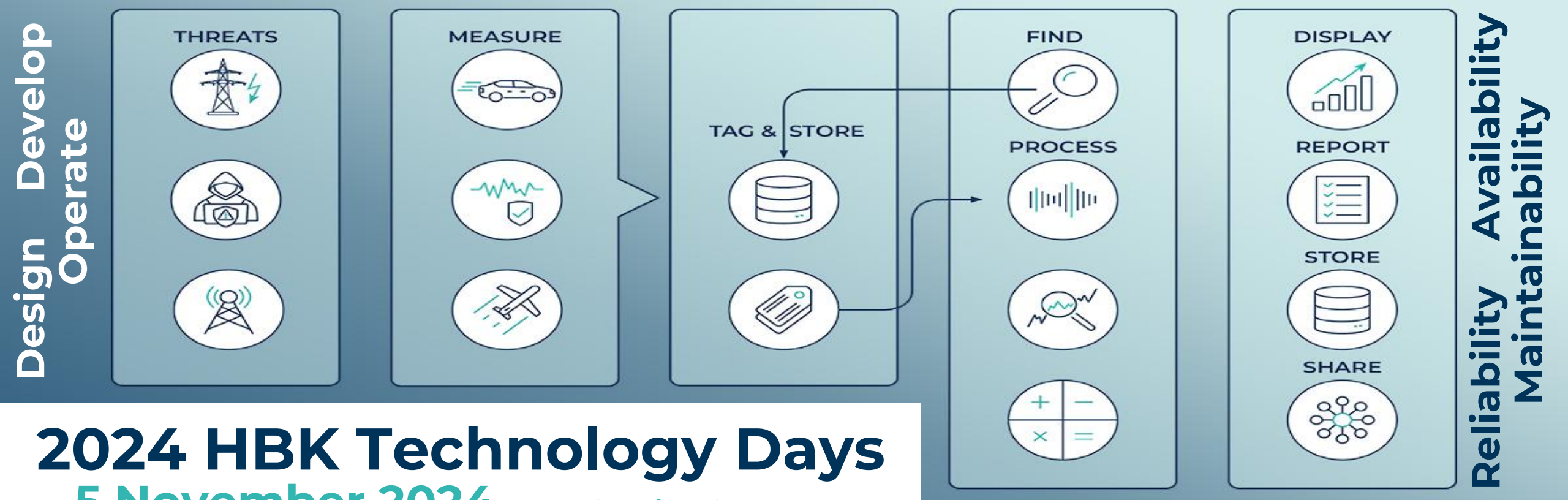


linkedin.com/company/vectorvcs



youtube.com/@VectorConsultingServices





2024 HBK Technology Days

5 November 2024



Session 2: Minimising Cyber Threats to Sensors, Vehicles and Software

- Agile cybersecurity for the software-defined vehicle

Christof Ebert,
Vector Consulting Services



Agile Cybersecurity for the Software-Defined Vehicle (SDV)

Dr. Christof Ebert, Vector Consulting Services, HBK Technology Days, 5. Nov. 2024