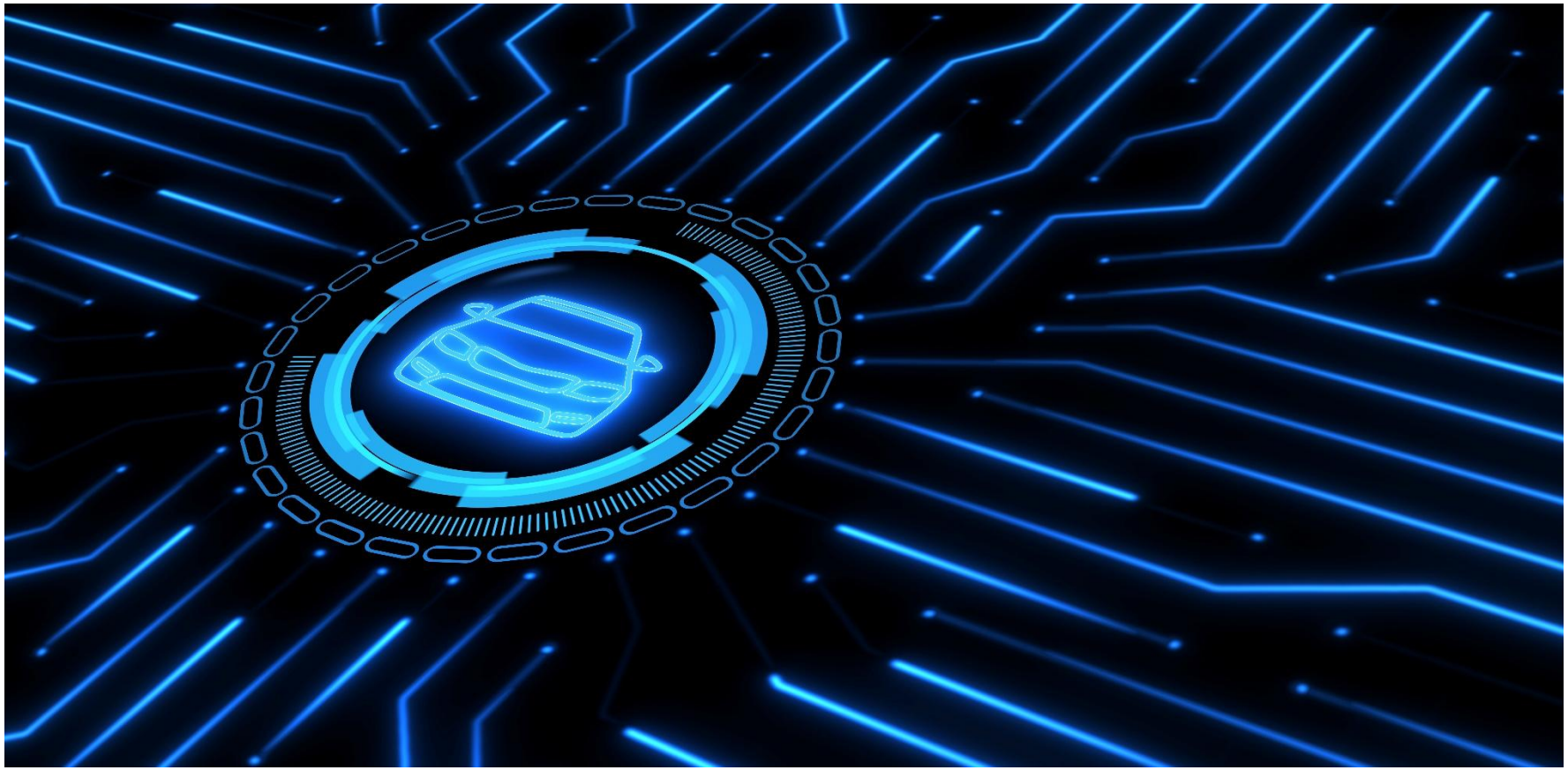
AUTOMOTIVE SYS®

VDA QMC
Verband der Automobilindustrie
Qualitäts-Management-Center

Distributed Cybersecurity Risk Analysis

Focus Matters



Über mich

Zeitschiene:

- 1995-2004: Mathematik & Informatik in Erlangen und Cambridge (UK)
- 2000-2003: SuSE Linux
- 2003-2025: Automotive GmbH
  Director, Head of quality, functional safety, cybersecurity and software compliance
- 2025: Safionyx GmbH & Co KG, Founder

Qualifizierungen:

- Principal Automotive SPICE assessor
- ECQA certified automotive quality manager
- ECQA certified functional safety manager
- EuroSPI certified cybersecurity manager
- OpenChain (ISO/IEC 5230)

Aktuelle Gremien:

- VDA Automotive SYS conference
- EuroSPI conference
- Intacs working group cybersecurity
- Soqrates working group
- Intacs working group AI

Cybersecurity Risk Analysis aka “TARA”

VDA QMC
Verband der Automobilindustrie
Qualitäts-Management-Center

Why? Well, standards…

Standard for manufacturing and Automotive Industries:

- ISO /SAE 21434 – Road vehicles – Cybersecurity engineering
- IEC 62443 – Industrial automation and control systems
- ISO / IEC 27001 – Information security management
- ISO / SAE PAS 8475 – Cybersecurity Assurance Levels
- ISO PAS 5112 – Auditing cybersecurity engineering
- ISO / SAE TR 8477 – Cybersecurity verification
- ENX and TISAX® - Auditing information security
- VDA Information Security Assessment
- ENX VCS – Vehicle Cyber Security Audit
- EU CRA – Cyber Resilience Act
- Etc.

CC0 image: https://www.rawpixel.com/image/5911853/image-public-domain-red-free

We focus on vehicle engineering today!

A full book on the topic:
Rodrigo do Carmo, Alexander Schlensog: “Automotive Threat Analysis and Risk Assessment in Practice”

Safionyx From code to compliance
AUTOMOTIVE SYS®

Distributed

Situation today: partnerships, long supply chains and operations

- Hardware manufacturer
- MCAL / BSP supplier
- BSW vendor
- Engineering service providers
- Vehicle backend provider

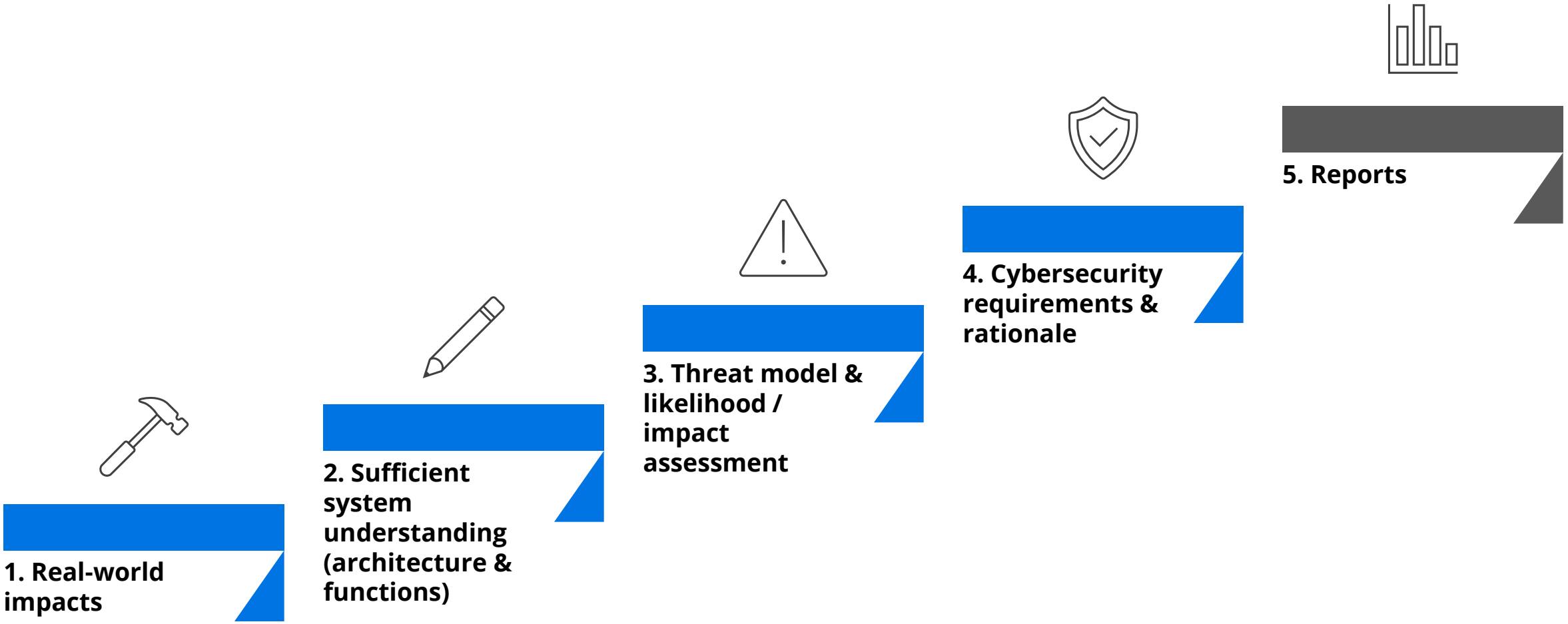
- Overall: supply chain got more complex, new players and operations is much bigger!

- Manufacturing! The whole supply chain! Also for manufacturing!
  When and where does a TARA stop?

Pixybay.com: https://picryl.com/media/russian-culture-matrjoschka-russkaya-kultura-matryoshka-4a1781

5 Elements of a good risk analysis[1]

The real intention!



[1] Sarah Fluchs, https://fluchsfriction.medium.com/f%C3%BCnf-elemente-einer-guten-cybersecurity-risikoanalyse-5fca30068ff4

1. Real-world impacts

The documents don’t go into the car, your software does!

1. Mindset

- Cybersecurity spans the whole organization, not just the system.
- System-only, vulnerability, or configuration analysis is not a real risk analysis. It is a compliance dance.
- Think worst case: high-consequence events and damage scenarios.
- Reuse the functional-safety HARA as input — safety severities are usually rated as high consequence.[1]

2. Key factors

1. Start early — then continuously
   - Early E/E architecture draft available
   - Begin during supplier selection & acquisition
   - Define scope — and what is explicitly out of scope
   - Define operational environment & impact categories
2. Involve real decision-makers
   - Present risks to customers, management, finance, etc.
   - First session with 1h is often enough

Impact categories (ISO 21434) — rate each damage scenario: Severe / Major / Moderate / Negligible

[1] See e.g. SAHARA: A security-aware hazard and risk analysis method

2. Sufficient System Understanding

Architecture & Functions

Understanding the system is key:

- This is the difference between a pure “compliance analysis” and the foundation for decisions.
- Without it there is no basis for attack models — and without attack models, there is no basis for credible security requirements.

Key factors

1. Don’t get stuck in the details
   - Knowing the assets is fine, but not enough as a basis for a risk analysis.
   - System understanding — especially the interactions — feeds the next step: threat modelling.
2. Create diagrams; reuse suppliers’ diagrams
   - Interactions and data flow are key inputs.
3. Simplify; start over if necessary
   - Cybersecurity diagrams can start quite simple — unlike huge, detailed system diagrams.
4. User interactions, also during operations
   - Humans belong in the risk analysis — they can be a threat or a countermeasure.
5. Think in functions
   - Functions are the bridge between the real world, business processes and the risk analysis for assets.

Cybersecurity properties (ISO 21434) — a compromised property of an asset enables a damage scenario

Confidentiality | **Integrity** | **Availability**

3. Threat Model & Likelihood / Impact Assessment

VDA QMC
Verband der Automobilindustrie
Qualitäts-Management-Center

- Threat or attack modelling is not academic reasoning about theoretical things — it needs focus.
- Attack scenarios are the step from system and impact to useful security requirements.
- A good attack scenario is so specific that deriving a security requirement is a simple, logical step.
- Use established methods and threat catalogues, but don't rely on them alone:
  - Use UN ECE R155 as a starting catalogue — it makes risk analysis comparable and credible.
  - Then continue with STRIDE, DREAD, PASTA or the MITRE ATT&CK framework.
  - Don't reinvent the wheel (unless necessary).

Key factors

1. Think from the impact: which attack could produce it?
2. Completeness is not the goal
   - Focus on scenarios with big impact or high likelihood.
   - After all, why would an attacker choose inconvenience?
3. Stay close to the system
   - E.g. place attack scenarios directly in the diagrams.
4. Simple attack paths
   - Probability and effect of a single attack path — no complex probability ratings.
5. Don't overthink risk ratings
   - More categories don't make it better.

ISO 21434 risk determination — Risk = Impact × Attack feasibility

Threat scenarios

Attack paths

Attack feasibility

Risk value

Safionyx
From code to compliance

AUTOMOTIVE SYS®

4. Cybersecurity Requirements & Rationale

Assumptions, Limitations, etc.

The purpose of a risk analysis is to find good cybersecurity requirements:

- **Treatment decision** — for each risk: avoid, reduce, share or retain (see below).
- **Cybersecurity goals** — the top-level security objective for each risk you reduce.
- **Cybersecurity controls** — the concrete technical & process measures that meet a goal.
- **Cybersecurity claims** — what you assert is handled elsewhere or accepted, incl. assumptions of use passed to the next party.

...and each is only as good as its rationale and traceability →

Key factors

1. Traceability
   - Clear which systems they apply to, and which scenario and impact they prevent.
2. Explicit rationale
   - Ideally all security decisions are risk-based; some are demanded by a framework.
   - Document requirements not implemented due to feasibility or other restrictions.
3. Assignment to regulations
   - Map standards and regulations to your own requirements — which shouldn't change when standards do.

ISO 21434 risk treatment decision (Clause 15.9)

Avoid | **Reduce** | **Share** | **Retain**

5. Reports & Communication

Idea from Automotive SPICE:

- Newer versions focus on communication between parties, e.g. “Communicate the agreed XY…”
- In ISO 21434, only responsibilities within the project and decommissioning are required.
- A risk analysis without a dedicated, targeted communication strategy is not effective.
- Reports are extracts from the risk analysis, tailored to target groups: suppliers, customers, decision-makers, or those without the know-how to work with the full analysis.
- This is essential for a living security culture, especially in distributed setups.

Good communication helps with:

1. Inform decision-makers
   - No decision-maker has time for 1000-line Excels.
   - Actively prepare the decisions you need and the remaining risks.
2. Support implementation with targeted information
3. Inform customers
   - Customers may need results from your analysis (limitations, assumptions) to do theirs properly.
4. Pass audits
5. Raise awareness

ISO 21434 reporting — tailor each extract to its audience

Decision-makers | **Customers** | **Suppliers** | **Auditors**

Distributed Risk Analysis: Challenges

Three challenges at the OEM–supplier boundary

1 · Scope & assets

Where does the item boundary stop?

- Stable item boundary + complete asset list — but attack paths ignore project lines.
- ISO 21434 Cl. 7: assumptions of use & cybersecurity claims must be agreed.
- A “SEooC-style” can lead to bad engineering (overengineering?)
- However, getting these written down, agreed and consistent is challenging

2 · Methods & rating

Whose rating scale wins?

- Different schemes clash: CVSS vs. attack-potential.
- Impact is the worst offender — a supplier can’t rate it without the OEM’s vehicle-level or system-level context.
- Harmonizing methods up front is usually cheaper.
- What appears to be a problem for a party may not be a problem for anyone else.

3 · Info flow & upkeep

Neither side sees the whole picture.

- Suppliers protect IP; OEMs withhold the full architecture — deliberately. Both analyse with gaps.
- No shared tooling or traceability across organizational boundaries.
- Even harder during operations: the distributed parties have to stay synchronized for years after SOP.
- In fact: many distributed TARAs quietly rot, which may lead to incomplete or slow vulnerability handling

All three are managed up front through the **Cybersecurity Interface Agreement (ISO 21434, Clause 7)**.

Summary and Outlook

What to take away — and where to go next

Summary

1. **Many rules, one focus** — ISO/SAE 21434 for vehicle cybersecurity engineering (amid CRA, IEC 62443, …).
2. **It's distributed** — a complex supply chain (OEM, Tier-n, service & backend providers). Where does a TARA stop?
3. **5 elements of a good TARA** — impact → system → threats → requirements → reports.
4. **The boundary is the challenge** — OEM–supplier scope, methods, information flow, keeping the TARA alive.

Outlook — what to improve

- **Agree the interface up front** — ISO 21434 Cybersecurity Interface Agreement (Cl. 7): scope, assumptions, claims.
- **Harmonize methods** — one shared impact & feasibility rating across partners.
- **Share more, safely** — controlled exchange of architecture & assumptions despite IP limits.
- **One living TARA** — shared tooling & traceability, kept in sync — also after SOP.
- **Stay lean** — focus on high-impact scenarios; don't over-engineer ratings.
- **Grow security culture** — communication & decisions built into the process.

Quality, Safety, and Security for Automotive Software-Based Systems

23–25 June 2026 • Potsdam

Safionyx
From code to compliance

Thank you!

Alexander Much – alexander.much@safionyx.com

LinkedIn: https://www.linkedin.com/in/alexander-much-88403853/

+49 151 6843 2342

Safionyx GmbH & Co KG – https://www.safionyx.com

Hagsfelder Allee 19a

76131 Karlsruhe

Germany

Safionyx
From code to compliance

AUTOMOTIVE SYS®