secunet

Umsetzung von TARA nach ISO/SAE 21434 bei KMU

Dr.-Ing. Rodrigo do Carmo

Senior Berater Mobility & Information Security

Ivanka Stefanova-Achter

Business Enablement Manager

secunet auf einen Blick – 25 Jahre Erfahrung!

secunet Security Networks AG

- **Öffentliche Auftraggeber**
- **Innere Sicherheit**
- **Verteidigung und Raumfahrt**
- **Gesundheits-markt**
- **Industrie**

Öffentlicher Sektor

Privater Sektor

Division Industry Fokus

- Automotive & Mobilität
- Digitale Infrastrukturen
- Versorger
- Industrielle Anlagen

IT-Sicherheitspartner der Bundesrepublik Deutschland

347m* Euro Umsatz

75 % Aktienanteil

Hauptaktionär: **Giesecke & Devrient**

*Im Jahr 2022

secunet auf einen Blick

12 Standorte
in Deutschland

über 1000
MitarbeiterInnen

secunet.com

Agenda

01 Short introduction to the regulations

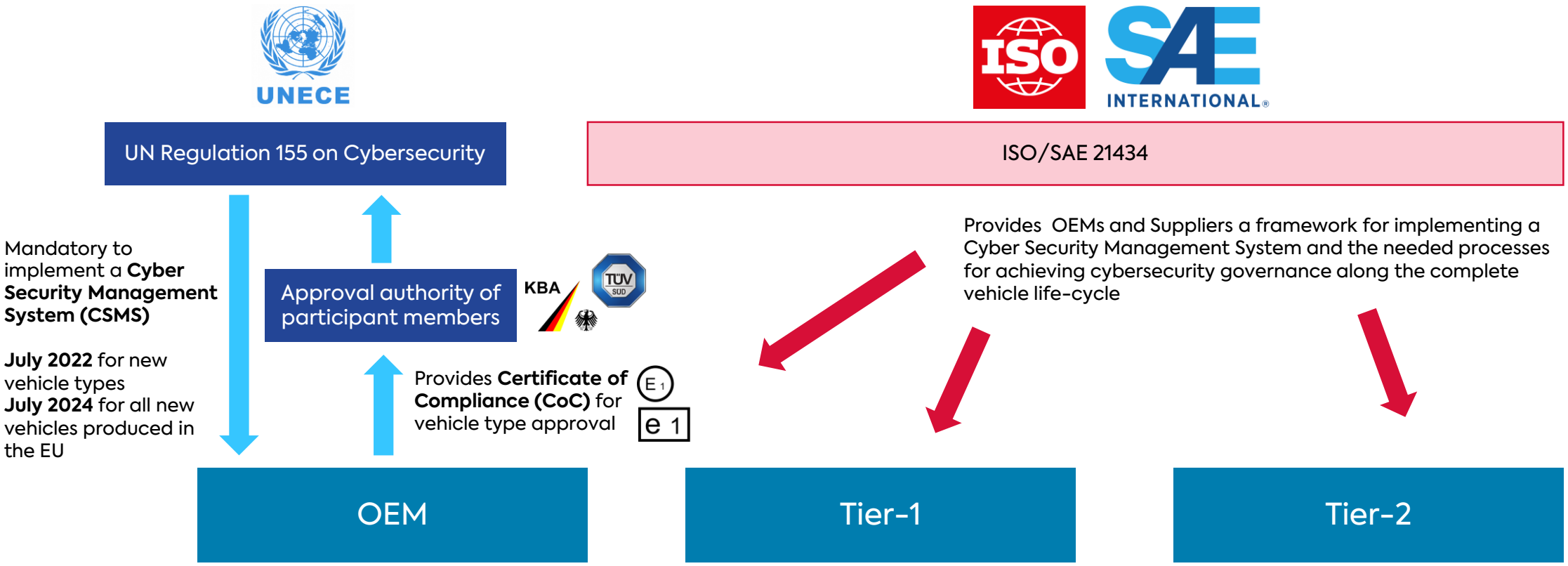
02 Cybersecurity capability across the production chain

03 Threat Analysis and Risk Assessment

01

Short introduction to the regulations

Cybersecurity regulations landscape – short overview



Supporting standards

NIST National Institute of Standards and Technology U.S. Department of Commerce

Bundesamt für Sicherheit in der Informationstechnik

- IEC 62443 for OT/Production
- ISO 2700X for ISMS
- ISO/IEC 15408 CC
- ISO/PAS 5112 Guidelines for auditing cybersecurity engineering
- ISO 24089 Software Update Engineering
- NIST Risk Mgmt. Framework
- BSI IT-Grundschutz
- ASPICE
- TISAX
- ...

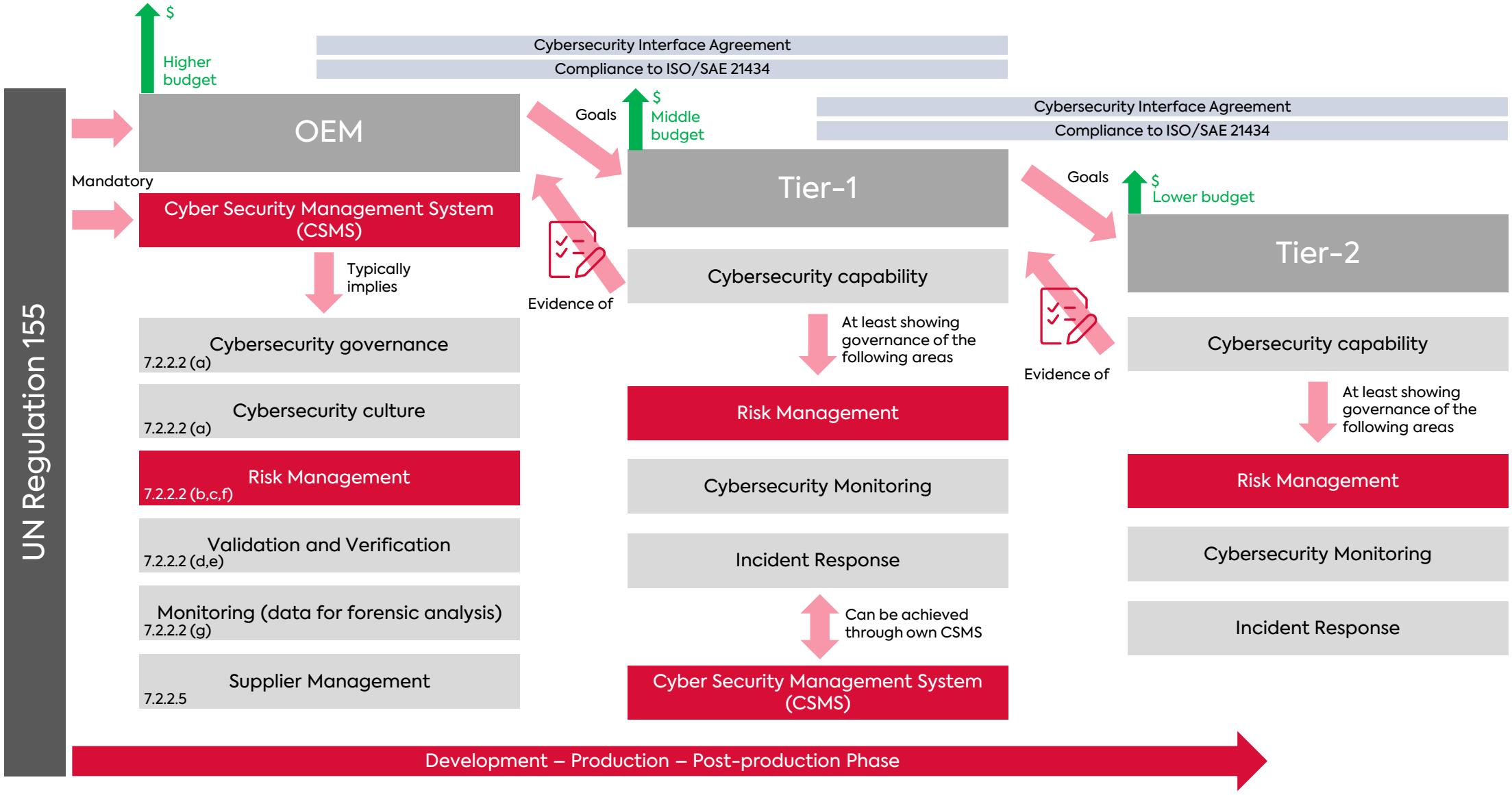
IEC

VDA

Supporting upcoming standards

- ISO/SAE 8475 Cybersecurity Assurance Levels (CAL) and Target Attack Feasibility (TAF)
- ISO 8477 Cybersecurity verification and validation
- ISO/IEC 5888 Security requirements and evaluation activities for connected vehicle devices
- ISO/TS 5083 Safety for automated driving systems – Design, verification and validation methods

Cybersecurity scope across production chain



Cybersecurity – huge challenges

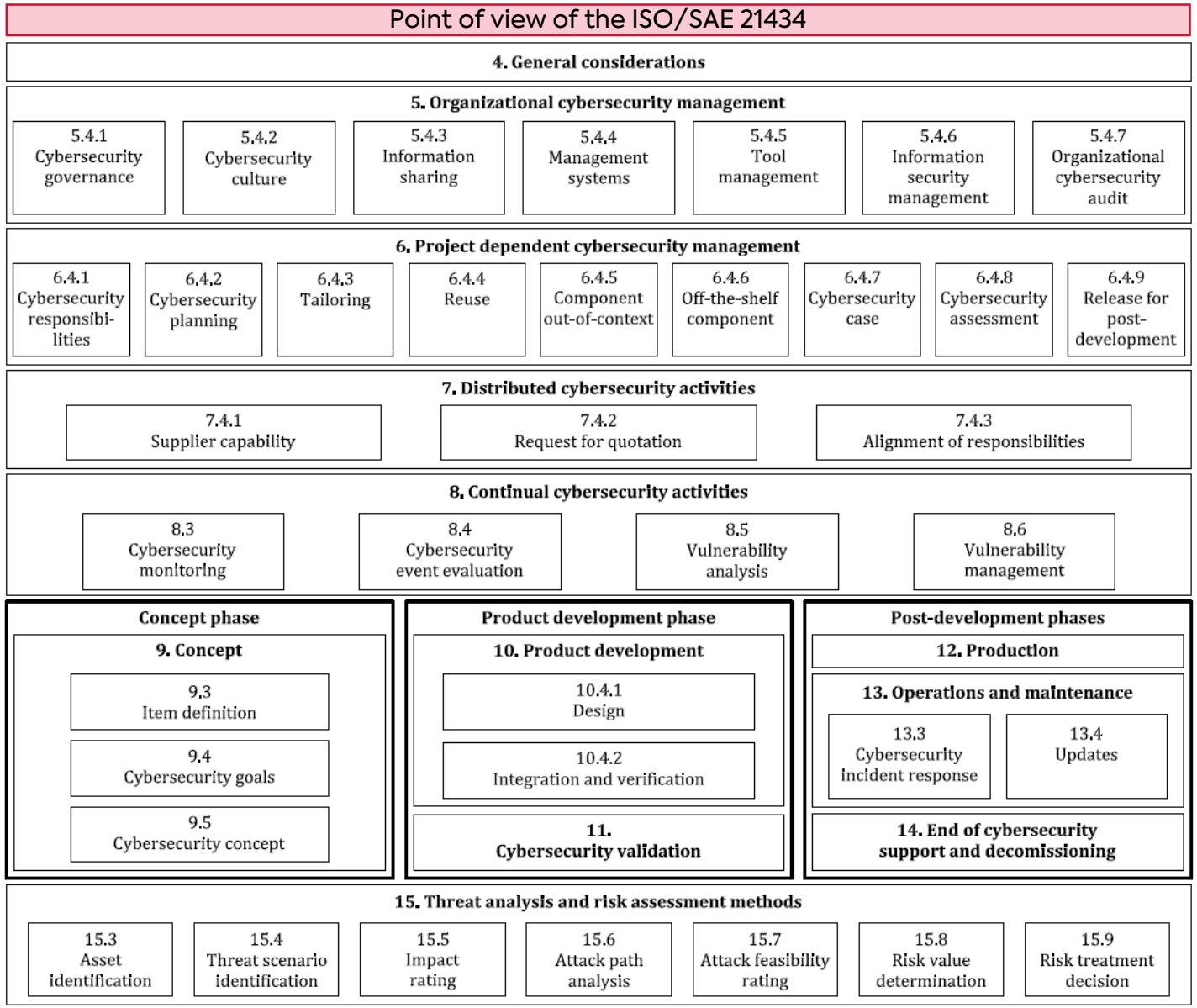
OEM

Tier-1

Tier-2

Cybersecurity Interface Agreement

Which work packages of the ISO/SAE 21434 have to be addressed depends on the supply pyramid (OEM, Tier-1, Tier-2, etc.) and their agreements



02

Cybersecurity capability across the production chain

What implies being “capable” of doing cybersecurity?

Tier-2

Cybersecurity capability

At least showing governance of the following areas

Risk Management

Cybersecurity Monitoring

Incident Response

- **Threat Analysis and Risk Assessment**
- Cybersecurity concept
- Cybersecurity engineering
- Assessments
- ...

Product Development

Products

Supporting Partner

Experience

Know-how

- Key Management and PKI systems

eID PKI Suite aaS

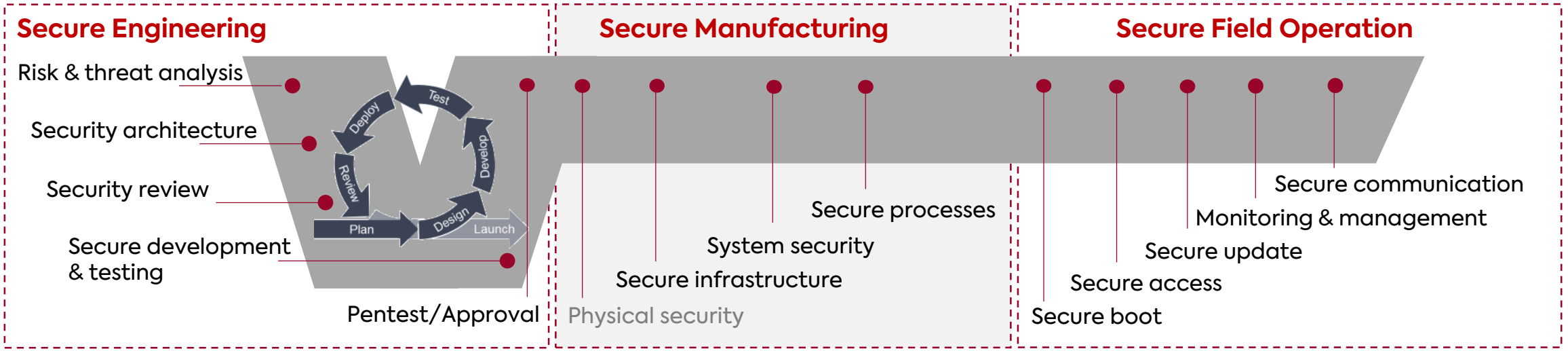
- Adaptation of production lines
- Adaptation of Tools
- Validation and verification processes

Production

- Incident Response (e.g. with participation at Auto-ISAC)
- Change management
- Continuous monitoring / SOC

Post-Production

How can a supporting partner improve the cybersecurity capability?



Regulations Consulting

Evaluation, assessment and implementation of industry standards and regulatory requirements

- IEC 62443 for OT/Production
- ISO 2700X for Risk Management
- NIST Risk Mgmt. Framework
- ASPICE
- TISAX
- ISO/PAS 5112 Auditing
- BSI IT-Grundschutz

Technical Consulting

Technical guidance regarding applied IT-security/cryptography for industry components and use cases

- Concepts
- TARA
- PKI

Penetration Testing

Vulnerability scanning and penetration testing for vehicles, ECUs and IoT components

03

Threat Analysis and Risk Assessment

Overview & History

History / Development

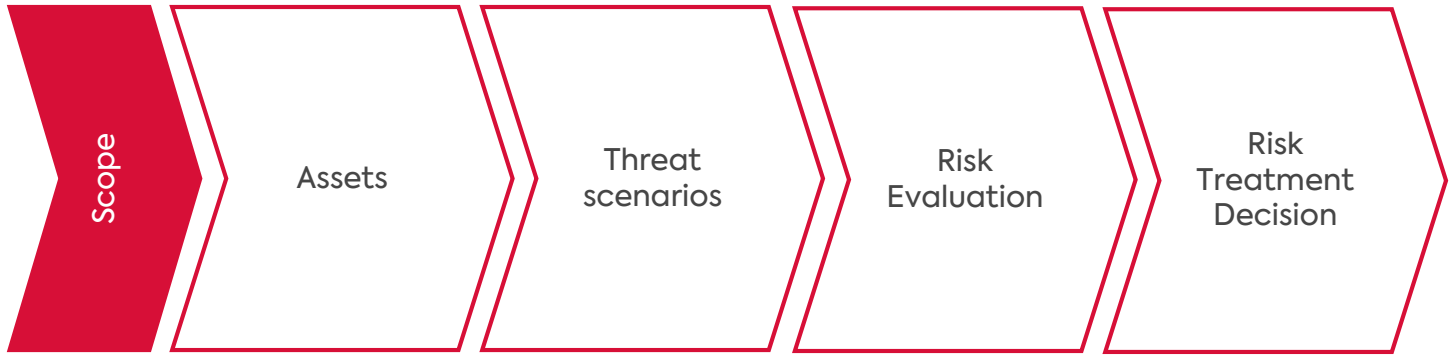
- secunet first automotive TARAs in 2012
- Functions based
- Several Standards
  - EVITA (E-safety vehicle intrusion protected applications), 2008
  - ISO 2700X-family
  - ETSI TVRA

Methodology today

- Adapted to ISO/SAE 21434 and UN Regulation 155
- Asset based
- Damage Scenarios
- Up-to-date threats and controls from different sources (e.g. secunet experience, OWASP Top 10, MITRE ATT&CK®, IEC 62443, UN R155, ISO 2700X, etc.)
- Own extensions and Excel template
- Continuous adaptations/improvements

Typical TARA project at secunet

General overview, steps and work packages



Input:
- Item definition
- Operational environment
- System Architecture
- Relevant documentation

Output:
- Scope of the TARA
- Assumptions
- Attacker Model

The definition of the **Scope** is the very first step of a TARA. It is important to define the boundaries of the system to be analyzed, define and document the components in scope and out of scope.

We propose to address the scope in a workshop together with project leaders, security engineers and system architects.

General overview, steps and work packages

Input:

- Technical Documentation and Interviews with Experts (SW/HW Engineers, Security Responsible, Project Managers, etc.)

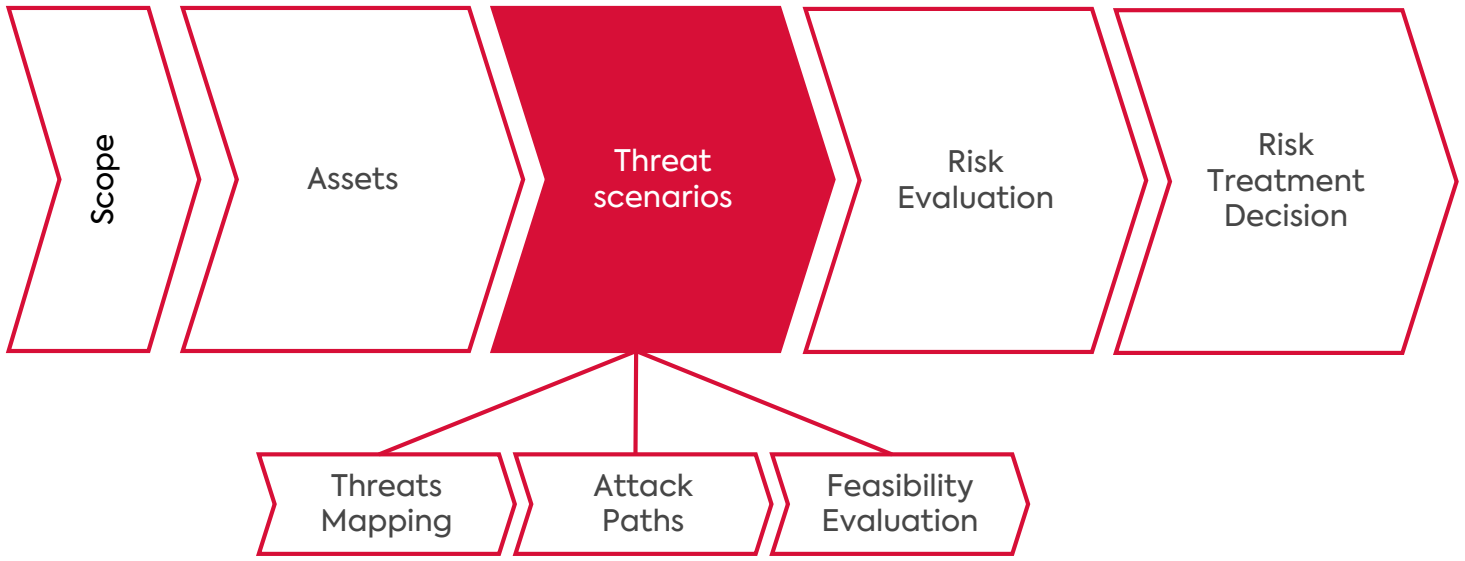
Output:

- Assets
- Cybersecurity properties
- Damage Scenarios and Impact Analysis

The analysis of the **Assets** can be separated into three tasks:

- **Identification of the Assets** of the system in scope that will be used for the risk analysis.
- **Assignment of the Cybersecurity Properties** to the assets. The key question for this step is to answer, which cybersecurity property is compromised in case of a successful attack.
- **Identification of the Impact** on different areas (e.g. functionality, business) that a successful attack on the asset has. In the context of the **ISO/SAE 21434**, the **Damage Scenarios** describe what could be the result of a threat scenario affecting a road user. The **Impact** of a successful attack for each damage scenario is evaluated at this step.

General overview, steps and work packages



Input:

- Assets and cybersecurity properties

Output:

- Threats identified
- Attack paths (can be also attack trees)
- Feasibility evaluation

The **Threats Mapping** is the process of assigning threats to the assets according to the affected security property. The threats come from different sources: expertise of security experts, specialized Internet sites, standards such as OWASP, etc. There is no definitive source of threats. The **Attack Path** is a written documentation of the steps needed to perform the specific attack that eventually compromises the specific assets. Attack Trees can be used as well. Finally, the **Feasibility Evaluation** determines the effort needed to actually perform the attacks.

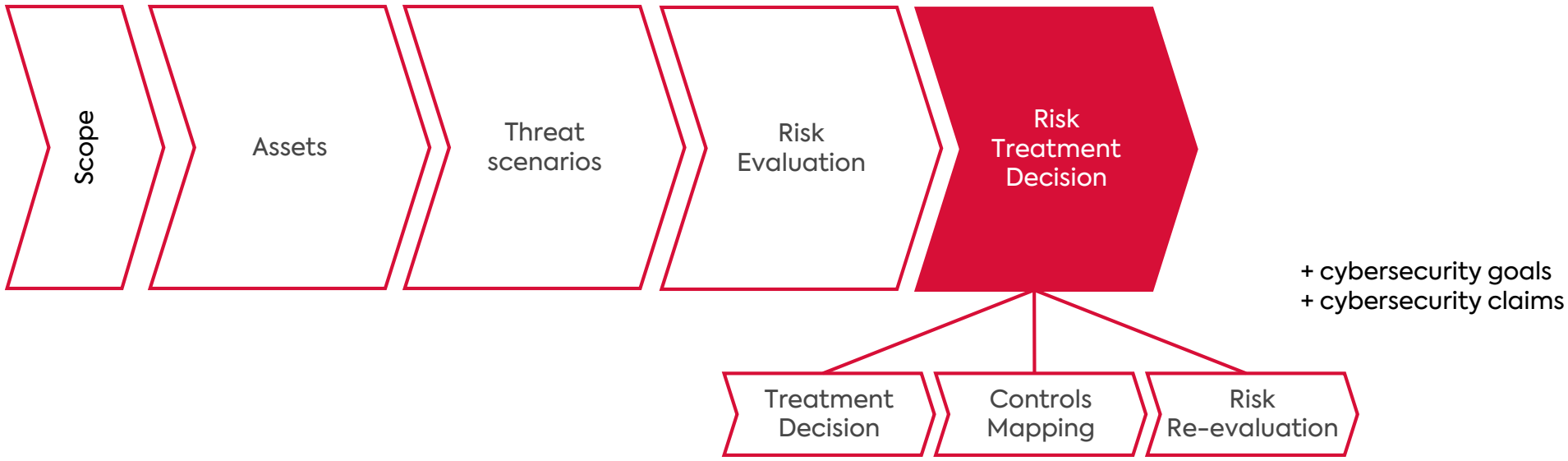
General overview, steps and work packages

Input:
- Threats scenarios are evaluated

Output:
- Risk evaluation of each threat of each asset

The **Risk Evaluation** quantifies the risk of each threat of each asset. The value of the risks results from evaluating the impact of an attack to the asset with the attack feasibility. The value of the risk is usually determined by either a risk matrix or a formula (e.g. Risk Value = Impact x Feasibility).

General overview, steps and work packages



Input:

- Threat scenarios are evaluated

Output:

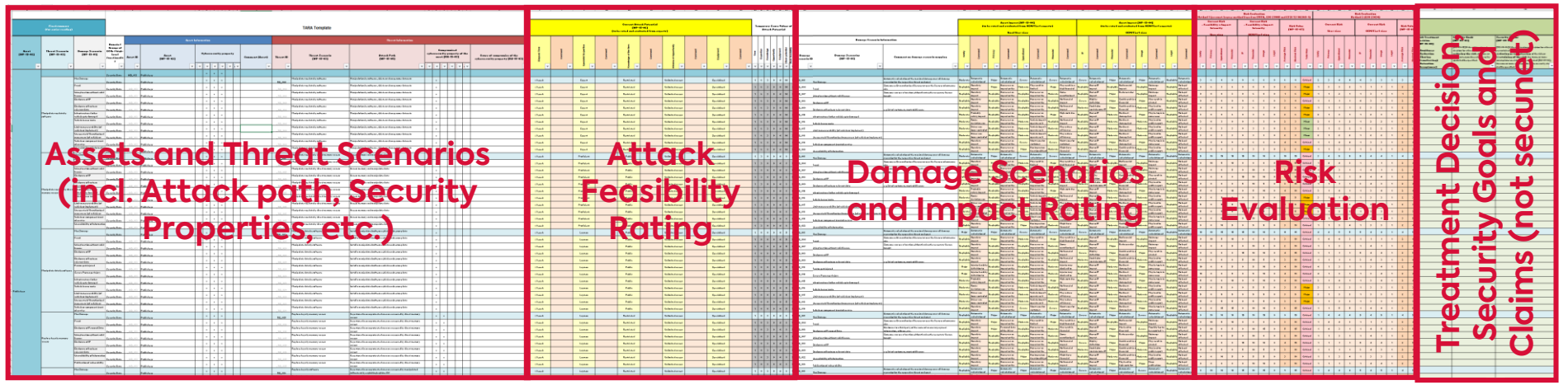
- Risk evaluation of each threat of each asset
- Treatment decision
- Controls mapping
- Risk re-evaluation (Residual risk)

The final step is the decision towards the evaluated risks. Usual actions for a risk are accept the risk, avoid the risk, reduce or mitigate the risk, or share the risk. The action is documented at the step **Treatment Decision**.

If the decision is to reduce or mitigate the risk, the next step is the **Controls Mapping**. Controls are countermeasures that aim at reducing the attack feasibility. The new risk value resulting of applying the control is calculated in the final step **Risk Re-evaluation**.

The risk after the treatment decision is called residual risk.

Documentation



All workpages (WP-15-...) and requirements (RQ-15-...) of the ISO/SAE 21434 documented

Kontakt

Dr.-Ing. Rodrigo do Carmo

Senior Berater Mobility & Information Security

secunet Security Networks AG

rodrigo.docarmo@secunet.com

Ivanka Stefanova-Achter

Business Enablement Manager

secunet Security Networks AG

ivanka.stefanova-achter@secunet.com

Save The Date – unsere Industrial Security Webinare

- **Cyberangriff – Notfallplan für den Ernstfall**

  24. April, 15:00 – 16:00 Uhr

- **Vorbereitung auf Cyberangriffe – Üben für den Ernstfall**

  15. Mai, 15:00 – 16:00 Uhr

Informationen und Anmeldung unter:
www.secunet.com/industrie


secunet