secunet

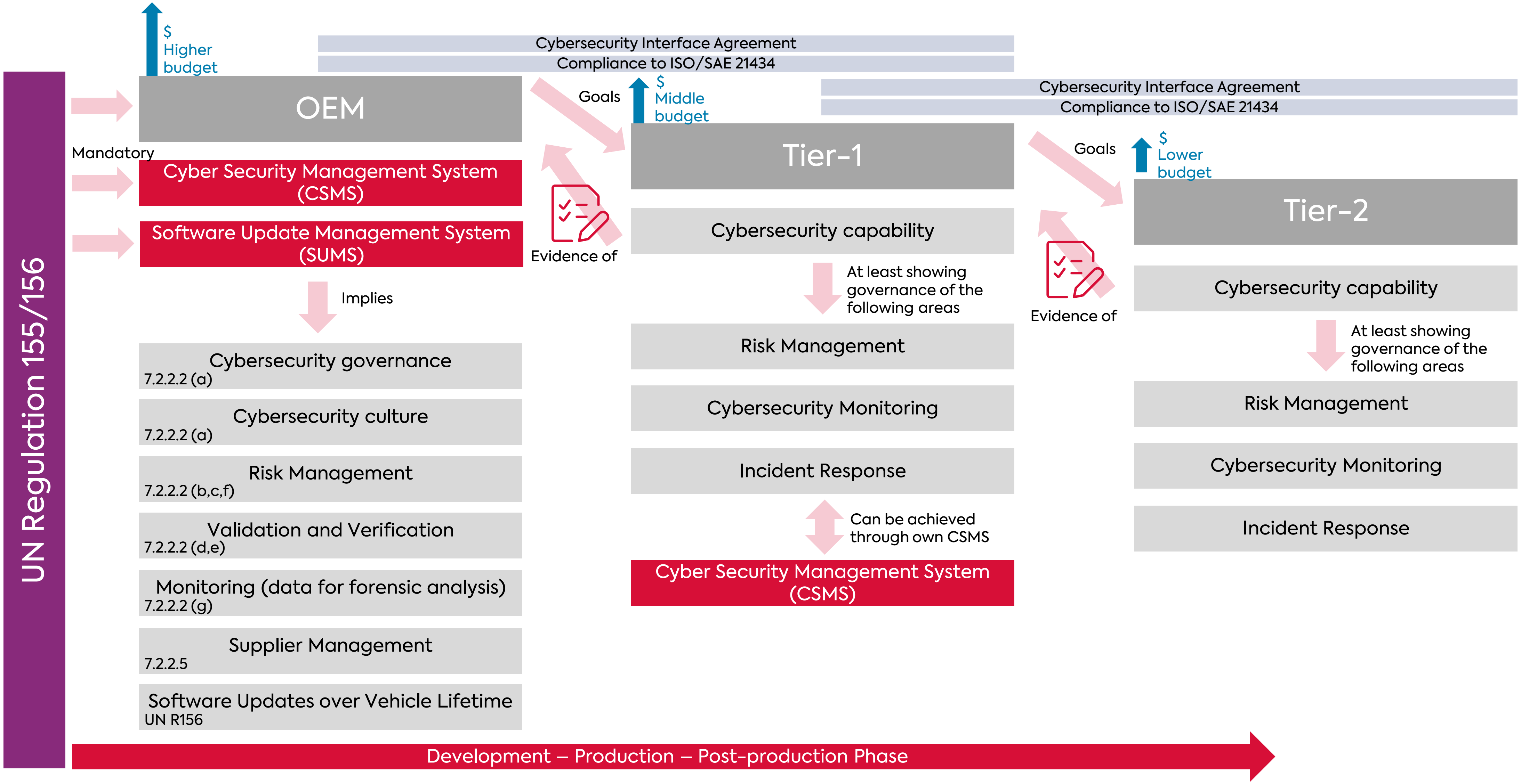
A very short intro: Achieving cybersecurity governance along the complete vehicle life-cycle – ISO/SAE 21434

Dr.-Ing. Rodrigo do Carmo

Team Lead Mobility & Operational Technology

Principal

Cybersecurity scope across production chain



UN Regulation 155/156

$ Higher budget

Cybersecurity Interface Agreement

Compliance to ISO/SAE 21434

OEM

Mandatory

Cyber Security Management System (CSMS)

Software Update Management System (SUMS)

Implies

Cybersecurity governance
7.2.2.2 (a)

Cybersecurity culture
7.2.2.2 (a)

Risk Management
7.2.2.2 (b,c,f)

Validation and Verification
7.2.2.2 (d,e)

Monitoring (data for forensic analysis)
7.2.2.2 (g)

Supplier Management
7.2.2.5

Software Updates over Vehicle Lifetime
UN R156

Goals

Evidence of

$ Middle budget

Cybersecurity Interface Agreement

Compliance to ISO/SAE 21434

Tier-1

Cybersecurity capability

At least showing governance of the following areas

Risk Management

Cybersecurity Monitoring

Incident Response

Can be achieved through own CSMS

Cyber Security Management System (CSMS)

Goals

Evidence of

$ Lower budget

Tier-2

Cybersecurity capability

At least showing governance of the following areas

Risk Management

Cybersecurity Monitoring

Incident Response

Development – Production – Post-production Phase

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

- Additional cybersecurity requirements for supply chain

NIS-2-Directive

- Gap Analysis
- Product / Process certification according to IEC 62443

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
- Product CS Project Management

Penetration Testing

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

Thank you!

Dr.-Ing. Rodrigo do Carmo
Team Lead Mobility & Operational Technology
Principal

Department Mobility & Information Security
Area Consulting Services
Division Industry
secunet Security Networks AG

Tel.: +49 201 54 54-2405,
Mobil: +49 175 7417504
E-Mail: rodrigo.docarmo@secunet.com
Mergenthalerallee 77, 65760 Eschborn, Germany
www.secunet.com