Secure Products & Systems

ASUT IoT Konferenz Bern

September 2020

INFOCLASS: UNCLASSIFIED
TLP: GREEN

DIGITAL TRUST SERVICES

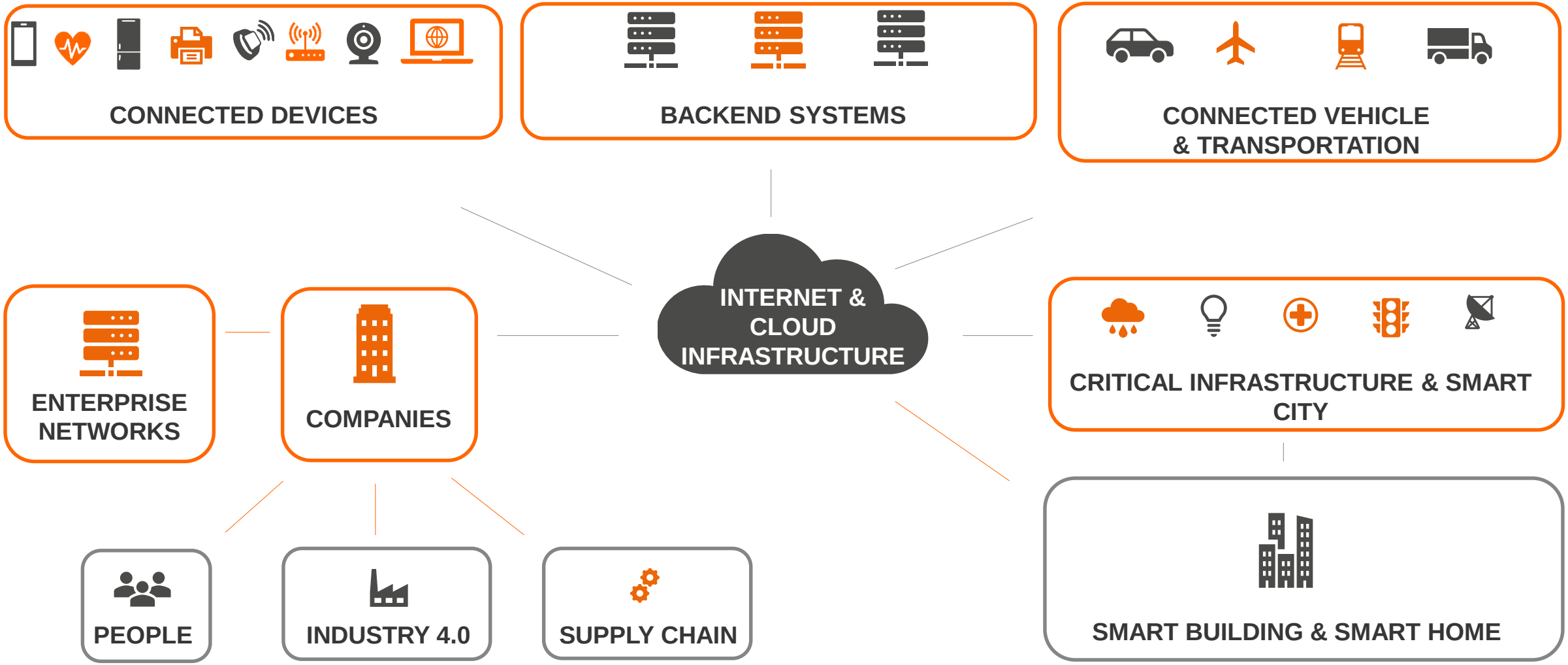
WHEN YOU NEED TO BE SURE

SGS

„IoT und Wege zu situations-angepasster IT-Sicherheit"

ASUT IoT-Konferenz, 3. September 2020

CHALLENGE
DIGITAL TRUST IN A CONNECTED WORLD



HIGH IMPACT CYBER ATTACKS
ACROSS MULTIPLE VERTICALS

Automotive

- **Jeep Hack** (2015)
- Hack firmwire update mechanisms
- Remotely control car

Consumer

- **Mirai Botnet** (2016)
- largest DDoS
- CCN, Netflix, Twitter down

Medical

- **Pacemaker** (2018)
- Remotely install update
- Modify configuration impacting health

IT & Comms

- **Wannacry** (2017)
- Ransomware hack
- All data encrypted

Transportation

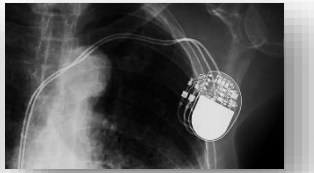
- **San Francisco Railway** (2016)
- Ransomware hack
- All data encrypted

Industrial

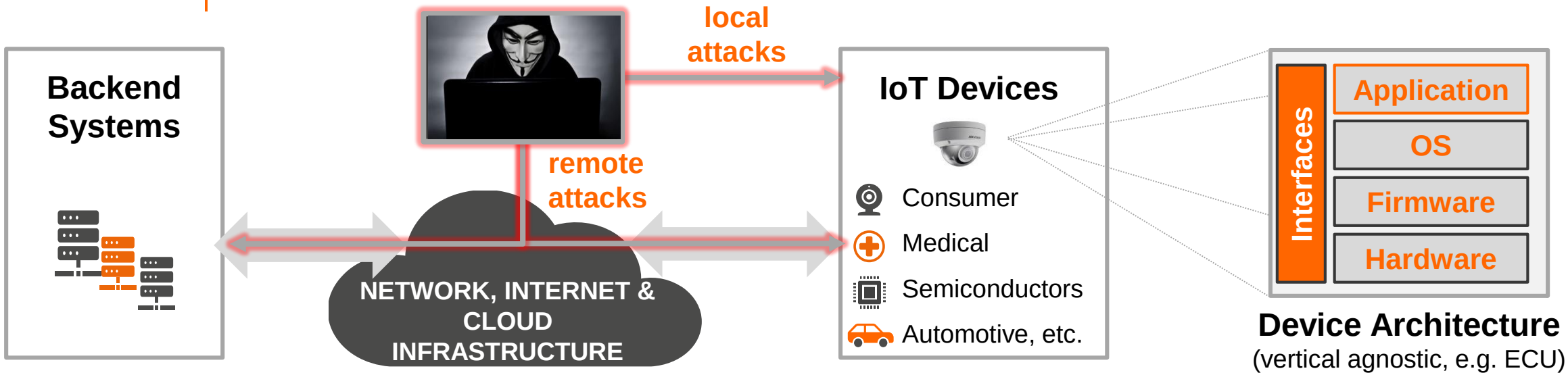
- **Triton 2017**
- Malware on Triconex safety controller model
- Taking over nuclear power plant

Semiconductor

- **Meltdown & Spectre** (2018)
- Extract memory content via side-channel attack
- Impact on ARM, x86, …



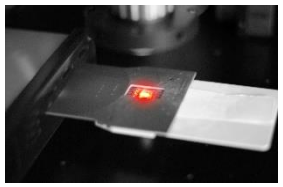
VERTICAL-AGNOSTIC
ATTACK PRINCIPLES



Device Architecture
(vertical agnostic, e.g. ECU)

local logical

e.g. test car maintenance interface



local physical

classical smartcard hacking

Successful attacks often combine several attack principles.

Local physical attacks can be used to reverse engineer a device. Leveraging this knowledge remote logical attacks can be developed and exploited for products installed.

remote logical

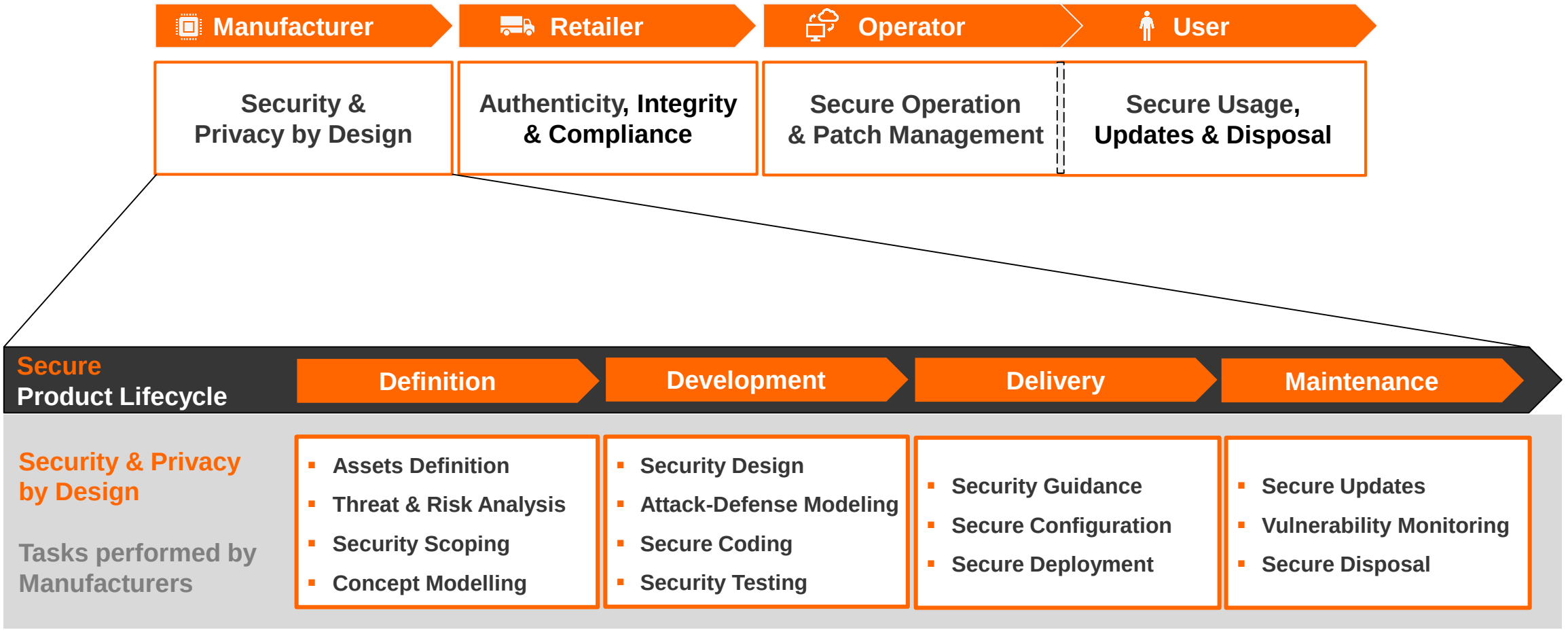
classical network hacking

remote physical

new category, where smartcard attacks are now applied remotely

SECURE PRODUCT LIFE-CYCLE PROCESS

SECURITY BY DESIGN



„… Wege zu situations-angepasster IT-Sicherheit“

Regulation & Standards

- Application & Use Case specific regulation and standards
- GDPR / CCPA
- EU Cybersecurity Act, California Bills
- MDR / IVDR / FDA Guidances
- ETSI EN 303 645
- IEC 62443 Standard Framework
- …

Skills & Security Capability Maturity

- Secure (Software) Development & Product Lifecycle
- Secure Design & Coding Principles
- Vulnerability Assessment & Testing Capabilities
- Vulnerability Monitoring
- Secure Product Platforms & FW/SW libraries
- …

Secure Production Sites & Supply Chain

- Secure & Trusted Production
- Trusted Supply Chains

Security Certification

- Risk-based certification approach
- Appropriate Certification Schemes
  - mix of vertical agnostic and vertical specific schemes
  - Schemes supporting different assurance levels
- Cross Recognition and Composite Certifications
- Modular Certifications
- Re-Certification

GOVERNMENTS PREPARING FOR STRINGENT REGULATION

enisa
European Network and Information Security Agency

There is a huge gap on trust on the digital market. Industrial and governmental stakeholders are taking action strengthening regulation across all regions …

- EU Cybersecurity Act being in force since June 27th 2019
- GDPR being effective since May 2018
- California Consumer Privacy Act (2018)
- California Bills: SB 327 & AB 1906
- MDR / IVDR and FDA Guidances related to Cybersecurity

CYBERSECURITY STANDARDS
EXAMPLES

Widely accepted standards, specifications & guidances:

- GSMA: IoT Security Guidelines
- IoT Security Foundation: IoT Security Compliance Framework & Secure Design Best Practice Guides and more

Standards tackling security maturity of organisations/industry 4.0:

- IEC 62443 Family: *Security for industrial automation and control systems*
- ISO/IEC 27001: *Information technology – Security techniques – Information security management systems*

US centric:

Regulation:

- Federal Trade Commission Act (FTC Act)
- CCPA: The California Consumer Privacy Act (2018)
- California Bills: SB 327 & AB 1906: reasonable security features for connected products
- Children's Online Privacy Protection Act (COPPA)
- Internet of Things (IoT) Cybersecurity Improvement Act

Standards / Specifications:

- UL 2900-1: Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements

Best Practices:

- NIST Cybersecurity Framework and NISTIR 8259A
- NIST Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

Certification:

- CTIA: IoT Cybersecurity Certification Program

EU centric:

Regulation:

- CE Marking
- GDPR regulation (effective since May 2018)
- EU Cybersecurity Act defining EU-wide cyber-security certification framework (in force since 06/2019)

Standards/Specifications:

- ETSI:
  - TS 103645 & EN 303 645 (in dev.) (Securing Consumer IoT)
  - TS 103 701 (in dev.) (Cybersecurity assessment for IoT products)
  - TS 103 485 (in dev.) (Privacy Assurance and verification)
- DIN SPEC 27072

Best Practices / Guidance Documents:

- IT-Grundschutz, SYS4.4. IoT Devices (BSI)
- ENISA
  - Good Practices for Security of IoT in the context of Smart Manufacturing (11/2018)
  - Good practices for security of IoT - Secure Software Development Lifecycle (11/2019)
  - Towards secure convergence of Cloud and IoT (09/2018)

SECURITY CAPABILITY MATURITY

GETTING PRODUCTS CYBERSECURITY-READY – 3-STEP APPROACH

1 Analyze Gaps

Understand the security maturity level of your

- products,
- development life cycle, and
- your employees

✓ Gap analysis report & action plan for raising security maturity

2 Raise the Security Maturity Level

Raise the security maturity level of your company by

- understanding how to setup a secure development lifecycle (SDLC),
- getting familiar with best practice and „security by design“, and
- training your team and onboarding dedicated cybersecurity experts

✓ Established processes and concepts for first projects

3 Demonstrate Effectiveness

Demonstrate your progress on cybersecurity by

- setting up internal & external security assessments in your SDLC,
- making use of independent 3rd party security evaluation & certification (e.g. Common Criteria)

✓ Establish processes and 3rd party attestation in place

SECURITY CERTIFICATION FOR PRODUCTS

VERTICALS

- Consumer
- Medical
- Semiconductors
- Automotive
- IT & Communication
- Industrial
- Agriculture
- Transportation

Certification Schemes need to fulfill requirements of fast moving markets

- Adoption of existing & implementation of new schemes required to support fast TTM
- Modular & composite certification, as well as cross recognition is key
- ENISA is taking this up within implementation of EU Cybersecurity Act

Examples for Certification Schemes available

Generic

- Common Criteria (CC) up to highest assurance levels

National Lightweight Security Schemes

- Beschleunigte Sicherheitszertifizierung (BSZ, Germany)
- LINCE (Spain)
- CSPN, BSPN, and others

IoT

- Security Evaluation Standard for IoT Platforms (SESIP)
- CTIA IoT Cybersecurity Certification (US)

SOGIS Recognition Agreement

COMMON CRITERIA CERTIFIED

CCN centro criptológico nacional

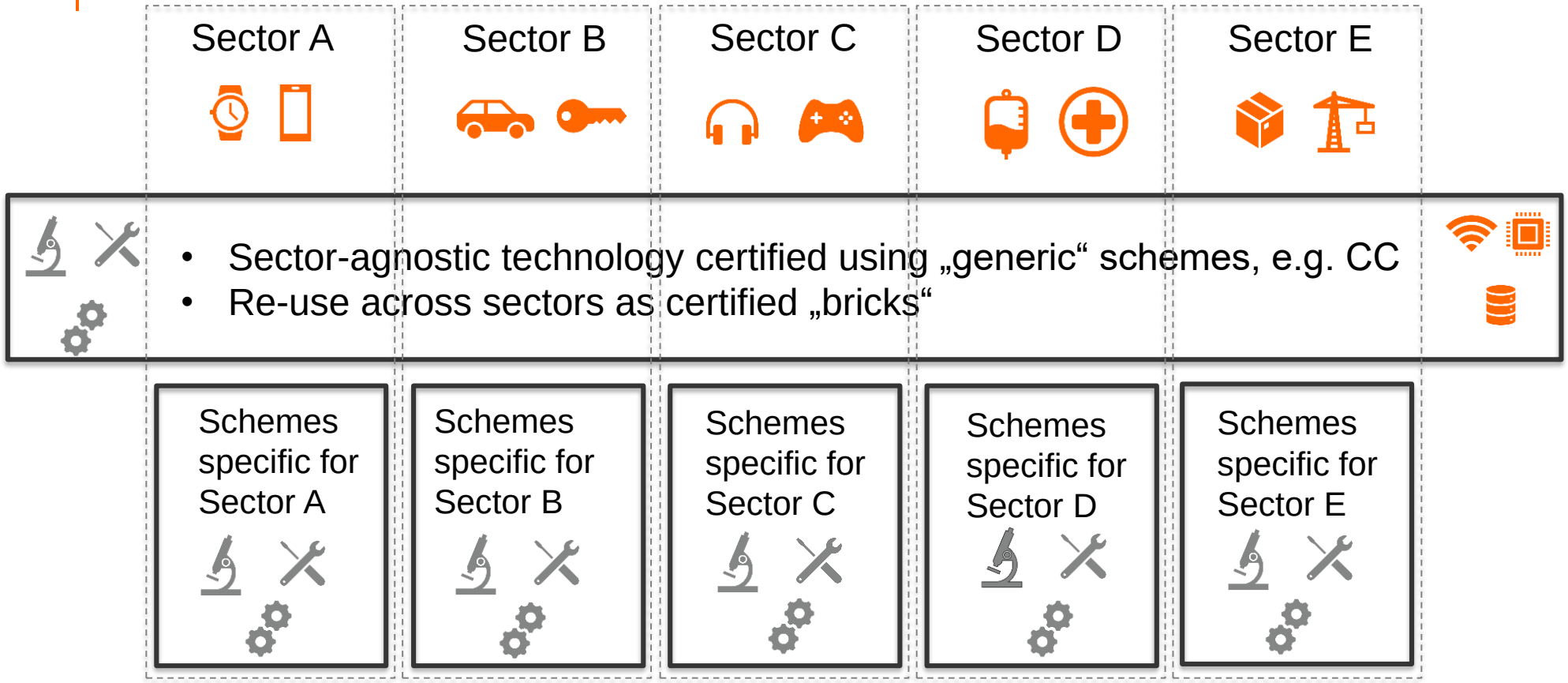
ctia

Bundesamt für Sicherheit in der Informationstechnik

SESIP

CERTIFICATION

CROSS RECOGNITION, COMPOSITION, MODULARITY

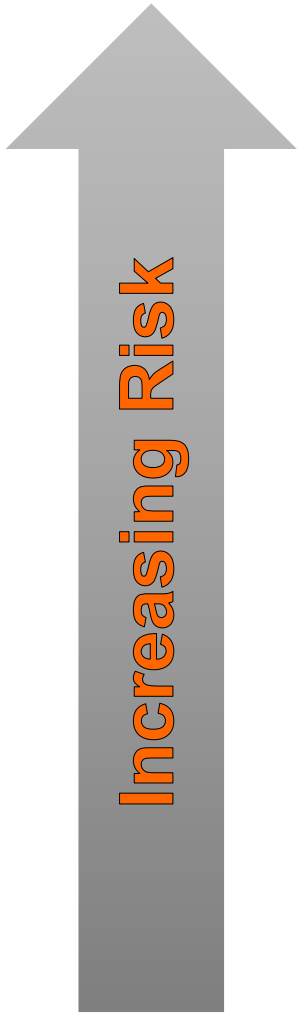


- Focus should be on sector-agnostic generic certification schemes
- Number of schemes should be kept minimal
- Cross-scheme composition should be fostered

SECURITY CERTIFICATION - EU CYBERSECURITY ACT

RISK AND ASSURANCE LEVELS

EU CSA LEVELS	RISK/IMPACT	TESTING APPROACH
High	▪ Government usage ▪ Life is at Risk ▪ Critical Infrastructure	▪ testing to demonstrate that the products, services or processes correctly implement the security functionalities ▪ an assessment of their resistance to skilled attackers using penetration testing
Substantial	▪ Personal Data compromised ▪ Privacy compromised ▪ Economic risk	▪ testing at a level intended to minimize the cybersecurity risks, cyber-incidents and cyber-attacks carried out by actors with limited skills and resources
Basic	▪ Low financial impact ▪ No personal data ▪ Not impacting safety	▪ testing at a level intended to minimize the known basic risks of cyberattacks



SECURITY CERTIFICATION
EXAMPLES VERTICALS & RISK LEVELS

RISK LEVELS	CONSUMER	MEDICAL	INDUSTRIAL	AUTOMOTIVE
High ▪ Government usage ▪ Life is at Risk ▪ Critical Infrastructure	 Baby care device	 insulin pump	 smart grid	 autonomous driving
Substantial ▪ Personal Data compromised ▪ Privacy compromised ▪ Economic risk	 IP camera device holding PII	 electronic patient record	 large factory	 infotainment system holding PII
Basic ▪ Low financial impact ▪ No personal data ▪ Not impacting safety	 Zigbee lightbulb with very simple logic	N/A	 standard ventilation system	 aircondition control

SECURE PRODUCTION SITES & SUPPLY CHAIN

Products <u>MUST</u> not be compromised during production and shipments throughout the supply chain

- Confidentiality to be ensured to protect sensitive data, e.g. cryptographic keys & credentials
- Integrity of HW / FW / SW to be ensured to protect products from manipulation

Not product related: Automated Industry 4.0 Production Sites to be secured ensuring Availability

Status:

- Depends on industry
- Consumer IoT: often low transparency due to production abroad
- Cases of compromised mobile phones have been reported: *„BSI warnt vor vorinstallierter Malware auf China-Handys“*
- Standards available defining requirements: IEC 62443, SOGIS MSSR, ISO 27001

STATUS

Regulation & Standards

- Industry, regulatory and governmental stakeholders are taking action
- Pace perceived low considering threat & damage situation
- Requirements could be more concrete supporting manufacturers with low level of understanding in decision making

Skills & Security Capability Maturity

- Manufacturers are struggling due to missing Cybersecurity legacy
- Security Maturity needs to be developed

Secure Production Sites & Supply Chain

- Depending on industry there are huge deficits
- Appropriate Requirements are available having been defined for certain industries

Security Certification

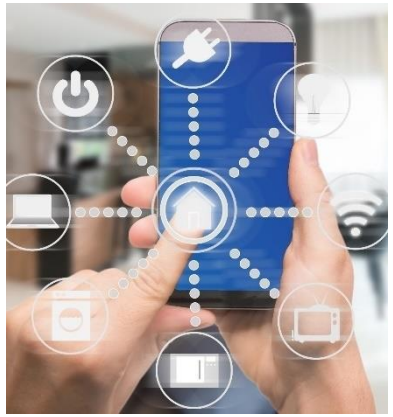
- Legacy certification schemes not sufficient
- Toolbox like approach still to be implemented covering different assurance levels & offering cross industry support

CONCLUSION

- Concerted regulation & standardization is key
  to get things moving faster
- Mandatory Baseline Security Requirements
  to be clearly defined
- Appropriate cross-regional certification schemes to be developed & implemented
- Above measures are required to
  make manufacturers invest into security maturity

The challenge is huge but managable. eGovernment and Payment industries provided proof of concept. Still, Cybersecurity will remain a continous effort.

SGS DIGITAL TRUST SERVICES



VERTICALS

- Consumer
- Medical
- Semiconductors
- Automotive
- IT & Communication
- Industrial
- Agriculture
- Transportation

Manufacturer	Retailer	Operator	User
Security & Privacy by Design	Authenticity, Integrity & Compliance	Secure Operation & Patch Management	Secure Usage, Updates & Disposal

DIGITAL TRUST SERVICES

- Training & Awareness
- Secure Product Life Cycle Support
- Security Evaluation & Certification

„from the smallest component to very complex systems“

THANKS

For more questions:

DIGITALTRUSTSERVICES@SGS.COM

DIGITAL TRUST SERVICES

WHEN YOU NEED TO BE SURE

SGS

SPEAKER

Thomas Röder

Global Head of Marketing & SalesRole

SGS DTS Secure Products & Systems

thomas.roeder@sgs.com

Thomas Röder, aufgewachsen im süddeutschen Raum, Diplom Physiker mit Studium an der Universität Stuttgart, hat derzeit die globale Verantwortung für die Marketing & Sales Aktivitäten der Business Unit „Secure Products & Systems“ bei SGS Digital Trust Services in Graz.

Herr Röder hat mehr als 25 Jahre Erfahrung in der High Tech Industry mit starkem Fokus auf Produkte und Systeme in der ICT und Halbleiter Branche.

Herr Röder beschäftigte sich 10 Jahre mit hochsicheren Halbleiterbausteinen für eGovernment, Chipkarten und Automotive Lösungen. Er hielt Positionen in den Bereichen Produkt Marketing, Produkt & Programm Management bei Unternehmen wie Alcatel, Siemens, Infineon und NXP.