Smart Mechatronics

RED IM FOKUS

So setzen Sie die neuen Cybersicherheitsanforderungen erfolgreich um

Heutige Referenten

Malte Konzels

Torben Lammers

Sven Schwarzer

Über uns

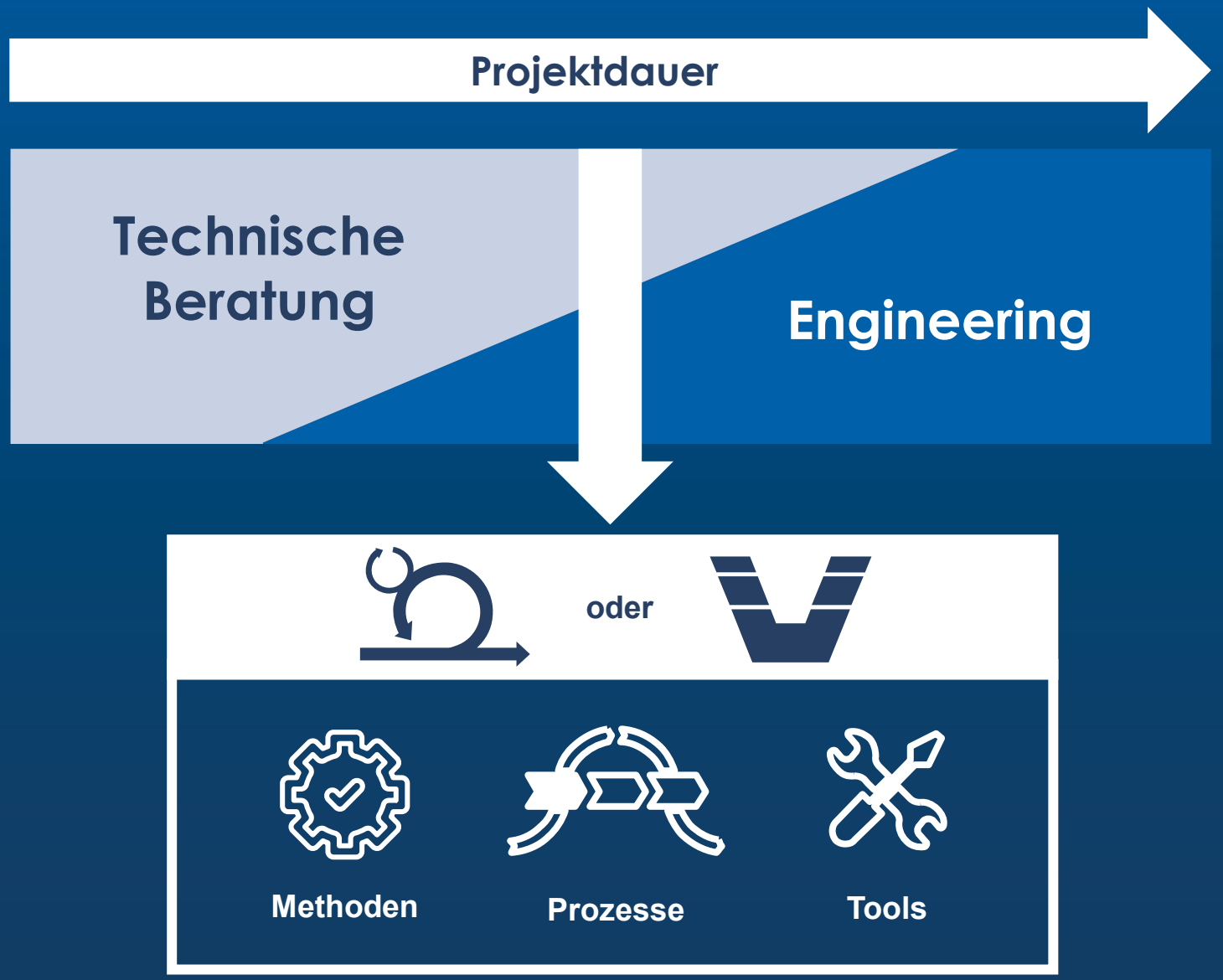
135 Mitarbeiter

Qualität
Zertifiziert nach DIN EN ISO 9001:2015

Standorte
Köln
Dortmund
Paderborn
München

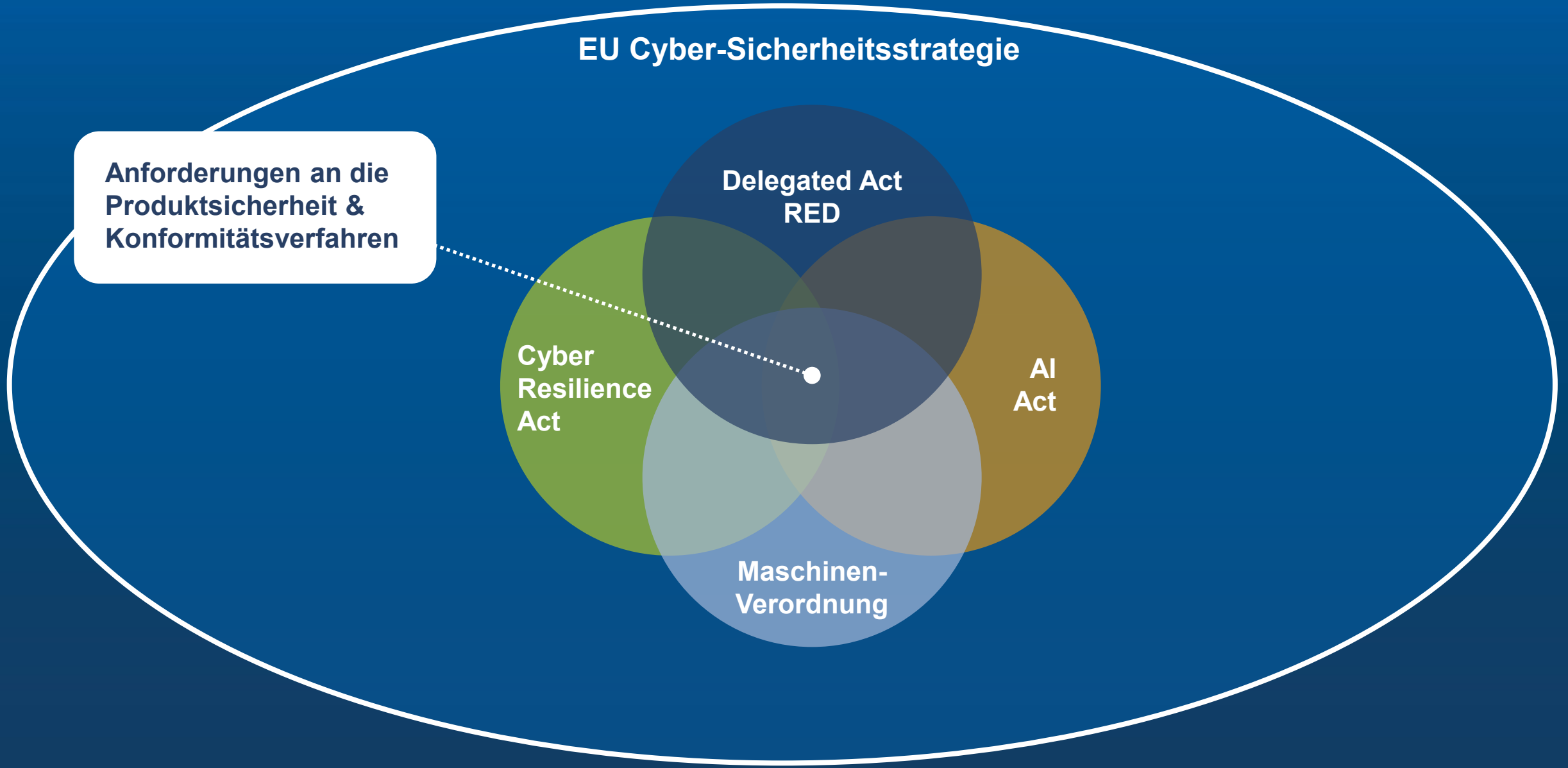
Gründung
Januar 2008

Smart Mechatronics

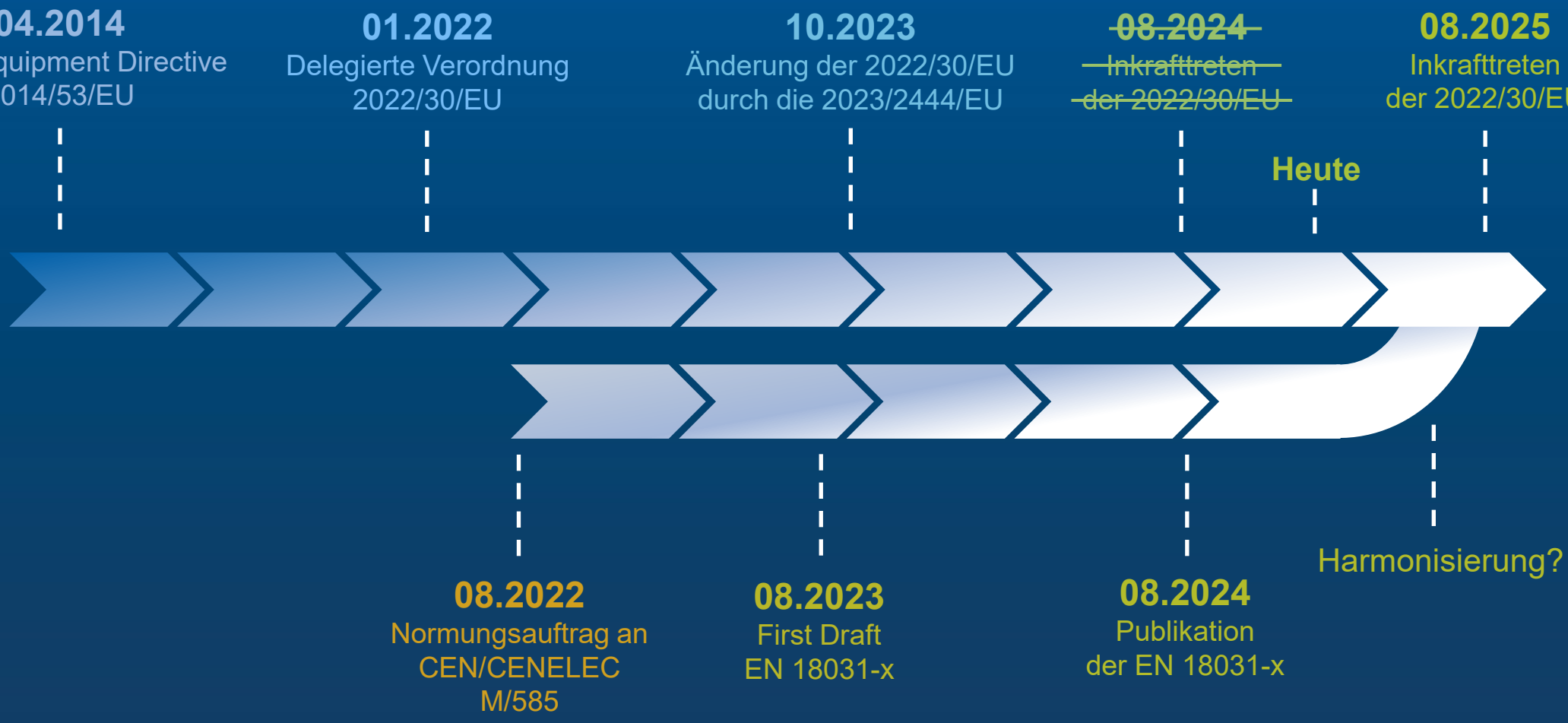


Produktsicherheit wird nicht nur durch die RED reguliert

Smart Mechatronics



Die Zeit drängt…



Was ändert sich?

- Die Anforderungen A.3.3.d/e/f der RED werden durch die delegierte Verordnung 2022/30/EU um den Schutz vor Cybersicherheitsrisiken erweitert.

(d) Schutz des Netzbetriebes

„Sie haben weder schädliche Auswirkungen auf das Netz oder seinen Betrieb noch bewirken sie eine missbräuchliche Nutzung von Netzressourcen, wodurch eine unannehmbare Beeinträchtigung des Dienstes verursacht würde.“

(e) Schutz der Privatsphäre und personenbezogener Daten

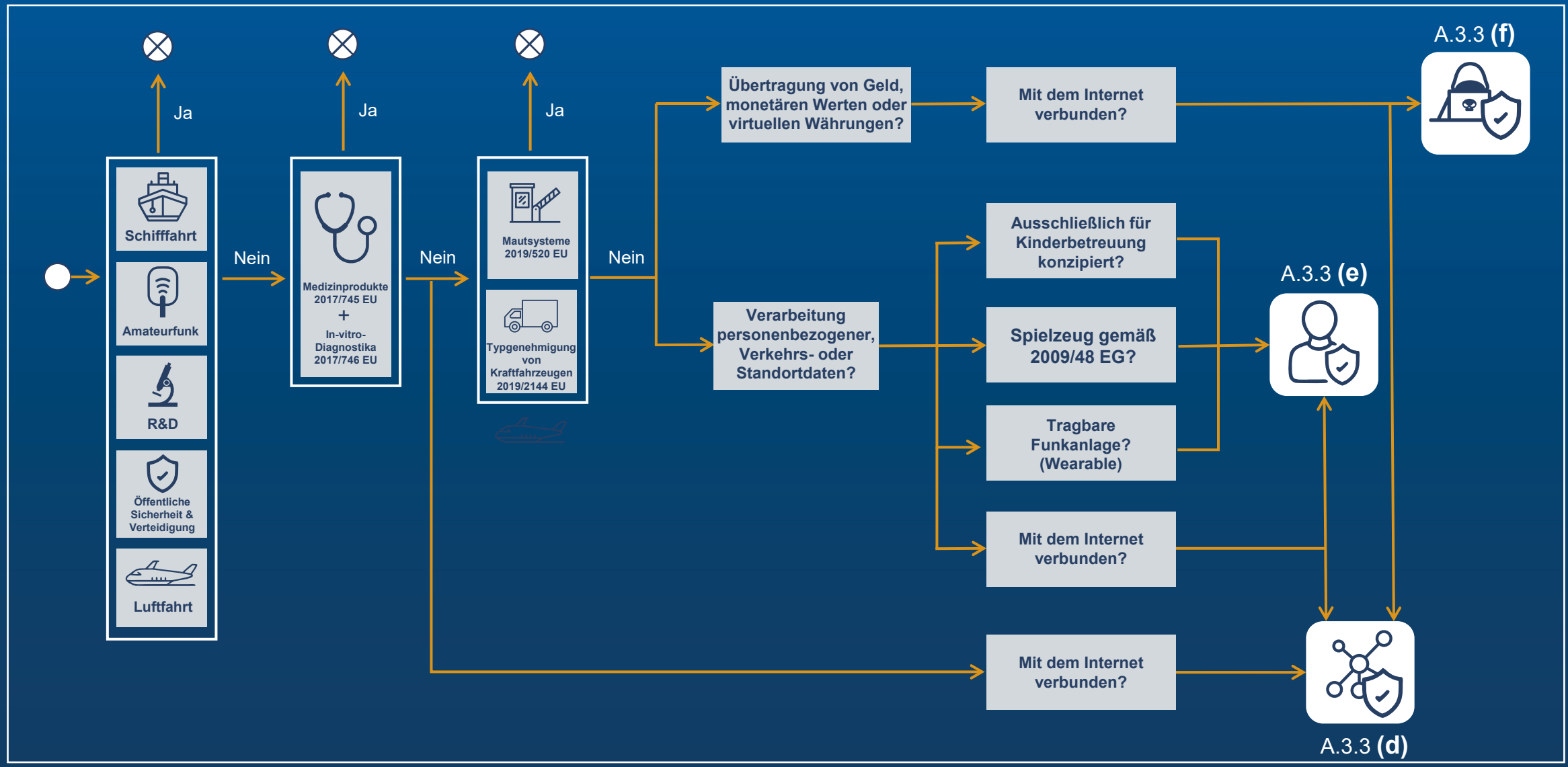
„Sie verfügen über Sicherheitsvorrichtungen, die sicherstellen, dass personenbezogene Daten und die Privatsphäre des Nutzers und des Teilnehmers geschützt werden.“

(f) Schutz vor Betrug

„Sie unterstützen bestimmte Funktionen zum Schutz vor Betrug.“

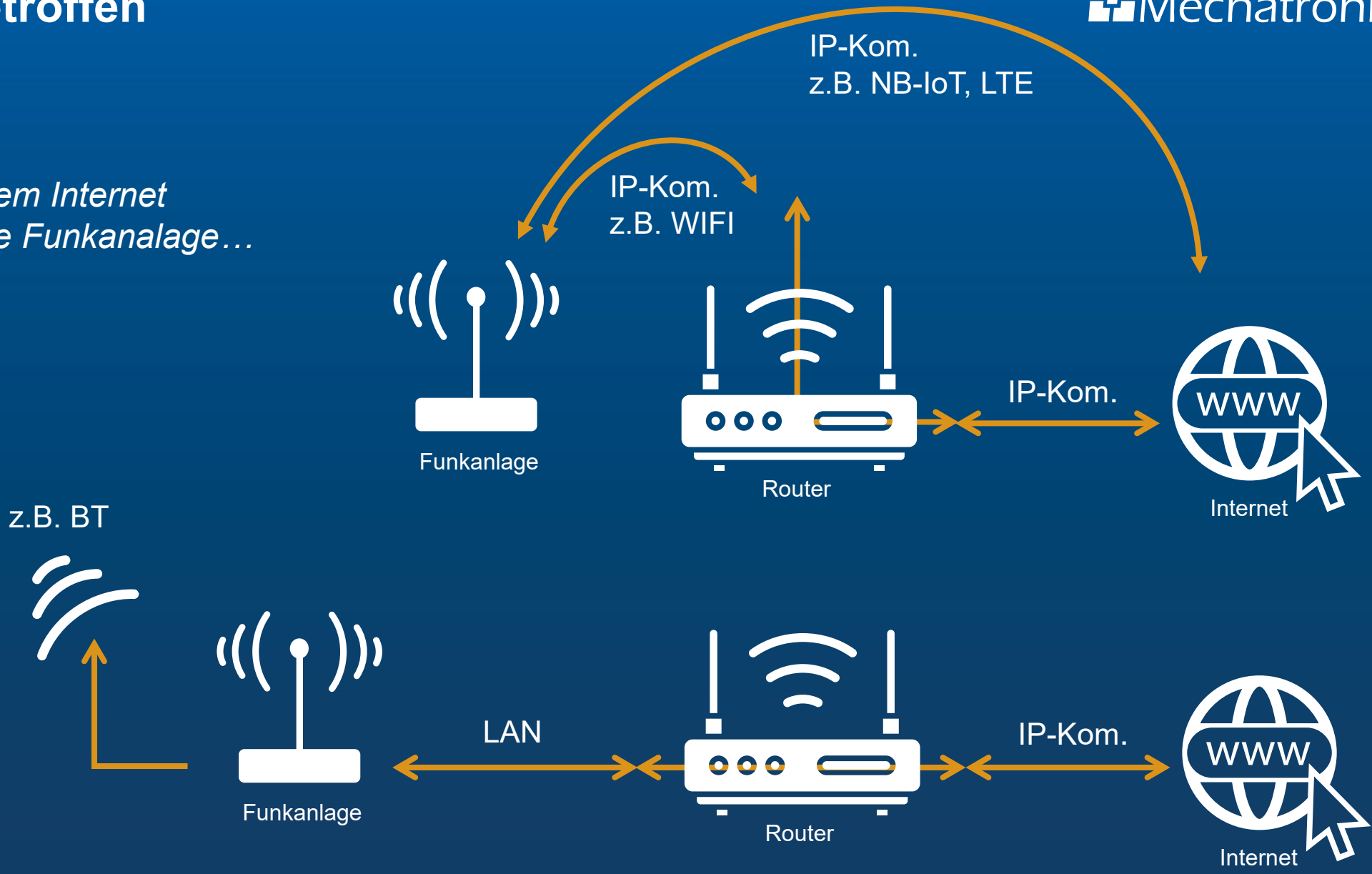
Das macht betroffen

Prüfung ob und welche Cybersicherheitsanforderungen gelten

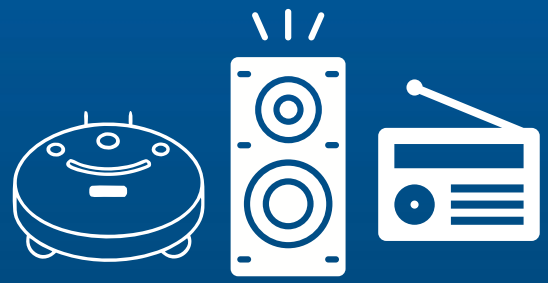


Das macht betroffen

Mit dem Internet verbundene Funkanalage…



Das macht betroffen



Staubsaugerroboter, Smarte Soundbox oder WLAN-Radio mit Verarbeitung personenbezogener Daten

(d) (e)

Internet

LTE

Smarter Drucker mit LTE-Modem und Bezahlfunktion per RFID

(d) (e) (f)

(e)

Konformität herstellen

Interne Fertigungskontrolle

- *Anwendung harmonisierter Normen*
- *Technische Dokumentation*

Baumusterprüfung

- *Durchführung einer EU-Baumuster-prüfung durch eine notifizierte Stelle*
- *Technische Dokumentation*

Qualitätssicherung

- *Etablierung eines Qualitäts-sicherungssystems mit Überwachung durch eine notifizierte Stelle*
- *Technische Dokumentation*

?

Welche Technischen Spezifikationen sind einzuhalten?
Welche Maßnahmen müssen ergriffen werden?

Konformität

Zulässige Vermarktung der Produkte auf dem EU-Markt

Konformität herstellen

- Mechanismen aus der EN 18031-x, zur Evaluation der geforderten technischen Spezifikationen
- Die Grundlage ist die Durchführung eines Risk Assessment und einer Threat Analyse (TARA)
- Erstellung eines individuellen produktspezifischen Maßnahmenkatalog und Prüfschemas

Grundlegende Anforderung	Normenteil
(d) Schutz des Netzes	EN 18031-1
(e) Schutz der Privatsphäre und personenbezogener Daten	EN 18031-2
(f) Schutz vor Betrug	EN 18031-3

Mechanismen/Anforderungen	-1	-2	-3
[ACM] Access control mechanism	X	X	X
[AUM] Authentication mechanism	X	X	X
[SUM] Secure update mechanism	X	X	X
[SSM] Secure storage mechanism	X	X	X
[SCM] Secure communication mechanism	X	X	X
[LGM] Logging mechanism	-	X	X
[DLM] Deletion mechanism	-	X	-
[UNM] User notification mechanism	-	X	-
[RLM] Resilience mechanism	X	-	-
[NMM] Network monitoring mechanism	X	-	-
[TCM] Traffic control mechanism	X	-	-
[CCK] Confidential cryptographic keys	X	X	X
[GEC] General equipment capabilities	X	X	X
[CRY] Cryptography	X	X	X

Entwicklung energieautarkes Raumthermostat

AUFGABE

Konzeptionierung und Entwicklung der Steuerelektronik

- Requirements- und Systems Engineering für das Thermostat im Zusammenspiel mit LoRaWAN-Gateway
- Übernahme des Entwicklungsprozesses für Elektronik und Software
- Benchmark von elektronischen Kernkomponenten

Beispielabbildung

UMSETZUNG

- Anforderungsanalyse & Produktkonzeption
- Security-by-Design
- Entwicklung energieoptimierter Hardware
- Softwareentwicklung und drahtlose LoRaWAN-Kommunikation
- Modul-, Software-, Integrations- und Systemtest
- Projektmanagement und Koordination externer Partner
- Begleitung der Zertifizierung durch den EMC-Test & VDE

PROJEKTDAUER

14 Monate

SMART PROJEKTTEAM

9 Mitarbeiter

Herausforderungen 1/2

Drahtlose Kommunikation personenbezogener Daten mit Constraint Device

Schutz personenbezogener Daten

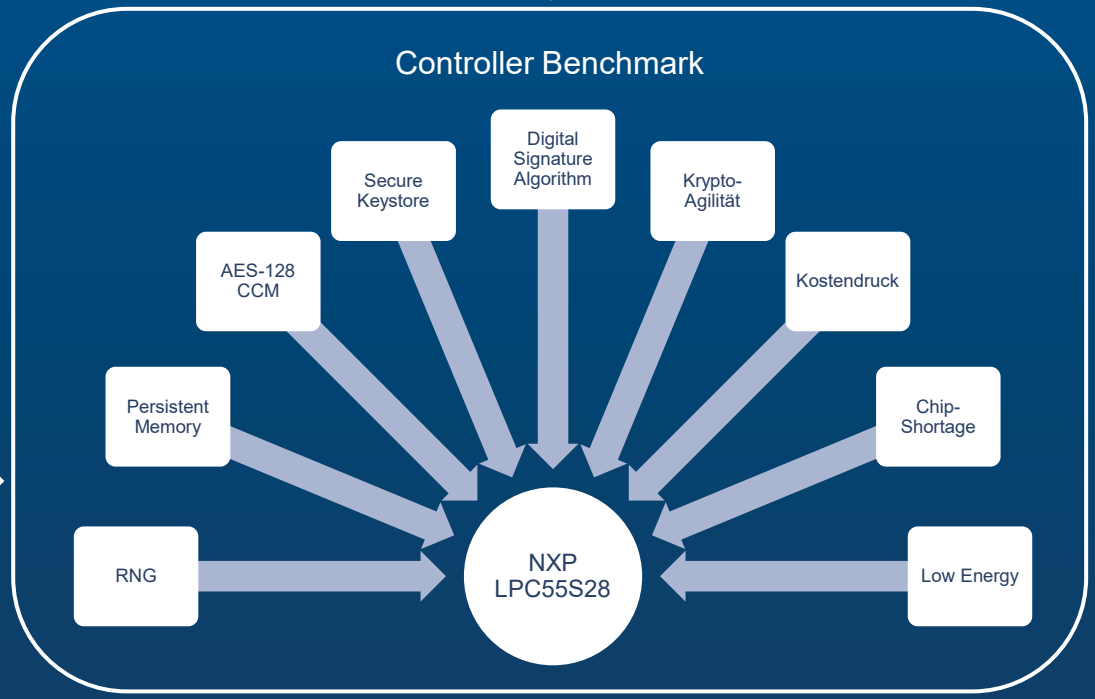
[SCM] Secure communication mechanism

Symmetrisch oder Asymmetrisch?
Welcher Cipher?
Welcher Modus?
Welche Schlüssellänge?

AES-CCM 128Bit

Security by Design
- Anforderungen aus Security Analyse
- Anforderungen abgeleitet von LoRaWAN

→ Anforderungen an Controller



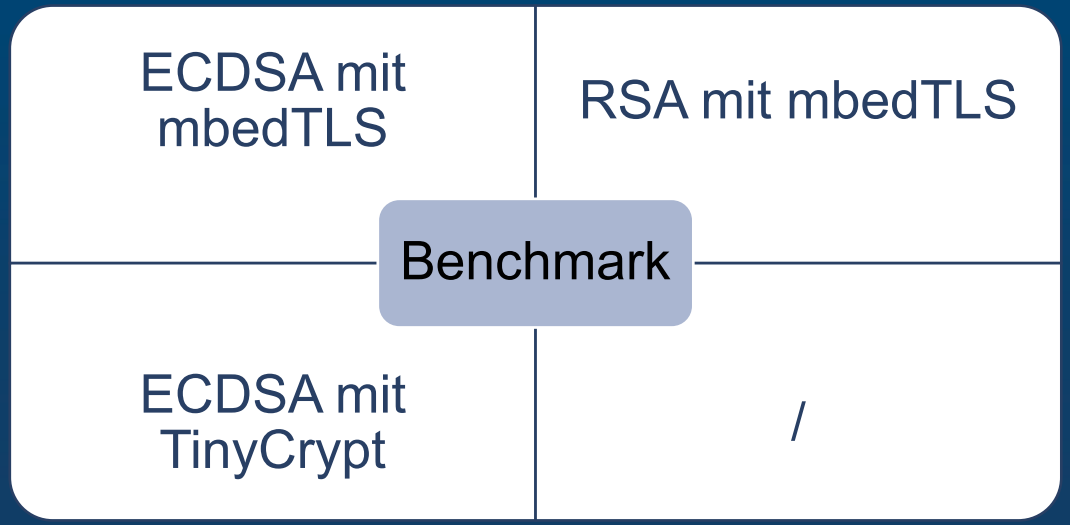
Security früh im Entwicklungsprozess adressieren,
um rechtzeitig die richtigen Entscheidungen zu treffen

Herausforderungen 2/2

[SUM] Secure update mechanism

- Verfahren soll sicher sein
- Algorithmus soll wenig Speicherplatz beanspruchen
- Verifizierung des Updates soll schnell gehen
- Update-Pakete sollen klein sein

Kriterien
- Auswahl Algorithmen
- Maintenance
- Codesize
- Execution time
- Signaturgröße



Algorithmen
- RSASSA-PSS
- ECDSA

Crypto-Libraries
- mbedTLS
- TinyCrypt

Herausforderungen 2/2 – Codesize

Referenz*:

O0	Os
text data bss dec hex filename 190380 1120 19224 210724 33724 _LPC55S28JBD100.axf	text data bss dec hex filename 112412 872 19184 132468 20574 _LPC55S28JBD100.axf

Optimierung	RSA (mbedtls)	ECDSA (mbedtls)	ECDSA (TinyCrypt)
O0	Mit HW SHA256: text data bss dec 221736 1132 19236 242104 221736 + 1132 – 191500 = 31368 Bytes Ohne HW SHA256: text data bss dec 231080 1132 19236 251448 231080 + 1132 – 191500 = 40712 Bytes	text data bss dec 232276 1464 19236 252976 232276 + 1464 – 191500 = 42240 Bytes	text data bss dec 199068 1120 19228 219416 199068 + 1120 – 191500 = 8688 Bytes
Os	Mit HW SHA256: text data bss dec 127616 884 19196 147696 127616 + 884 – 113284 = 15216 Bytes Ohne HW SHA256: text data bss dec 130120 884 19196 150200 130120 + 884 – 113284 = 17720 Bytes	text data bss dec 138760 1208 19196 159164 138760 + 1208 – 113284 = 26684 Bytes	text data bss dec 116872 872 19188 136932 116872 + 872 – 113284 = 4460 Bytes

* Basierend auf Commit ohne Signatur-Überprüfung (SHA1: 961054be089356c3b38172be4c28f40b9c23f7b2)

Herausforderungen 2/2 – Execution Time

Ausführungszeit ohne Hash-Berechnung und Initialisierung der benötigten Komponenten (vernachlässigbar).

Optimierung	RSA (mbedtls) mbedtls_rsa_rsassa_pss_verify()	ECDSA (mbedtls) mbedtls_ecdsa_verify()	ECDSA (TinyCrypt) uECC_verify()
O0	2945687 CpuCycles = 30,68 ms	30390529 CpuCycles = 316,57 ms	143031990 CpuCycles = 1489,92 ms
Os	2783638 CpuCycles = 28,99 ms	28115227 CpuCycles = 292,87 ms	143031975 CpuCycles = 1489,92 ms

* Basierend auf Commit SHA1: 961054be089356c3b38172be4c28f40b9c23f7b2

Herausforderungen 2/2 – Ergebnis

	RSA (mbedtls)	ECDSA (mbedtls)	ECDSA (TinyCrypt)
Codesize	2	5	1
Execution time	1	3	5
Signaturgröße	2	1	1
Lib-Maintainace	1	1	4
Summe	7	11	12

Legende:
1 sehr gut … 5 sehr schlecht

	mbedTLS	tinyCrypt
Maintenance	Latest Release Sep. 2024	Latest Release Aug. 2017

- Entscheidung für eine Technologie bzw. die beste Lösung ist nicht trivial
- Es sollten alle Faktoren im Entscheidungsprozess berücksichtigt werden

Erforderliche Schritte

- Produktanalyse und -klassen
- Produkteinordnung
- Einordnung in Normen- und Verordnungslandschaft
- IST-Standbewertung
- Maßnahmendefinition
- Umsetzungsplanung

Security Konformitätscheck

- Analyse und Erstellung notwendiger Dokumente
- Erarbeiten technischer Anforderungen/Mechanismen
- Ableiten von Maßnahmen
- Umsetzung der Maßnahmen
- Konformitätsbewertung

Zertifizierungsprozess

- Doomsday Scenarios
- Context-Diagrams
- Trust Boundaries
- Threat Identification
- Risk Assessment
- Mitigations

Security Analyse / TARA

Smart Mechatronics

Q&A

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

NOCH FRAGEN?

Wir stehen Ihnen gerne zur Verfügung!

Malte Konzels

Malte.Konzels@smartmechatronics.de

Torben Lammers

Torben.Lammers@smartmechatronics.de

Sven Schwarzer

Sven.Schwarzer@smartmechatronics.de