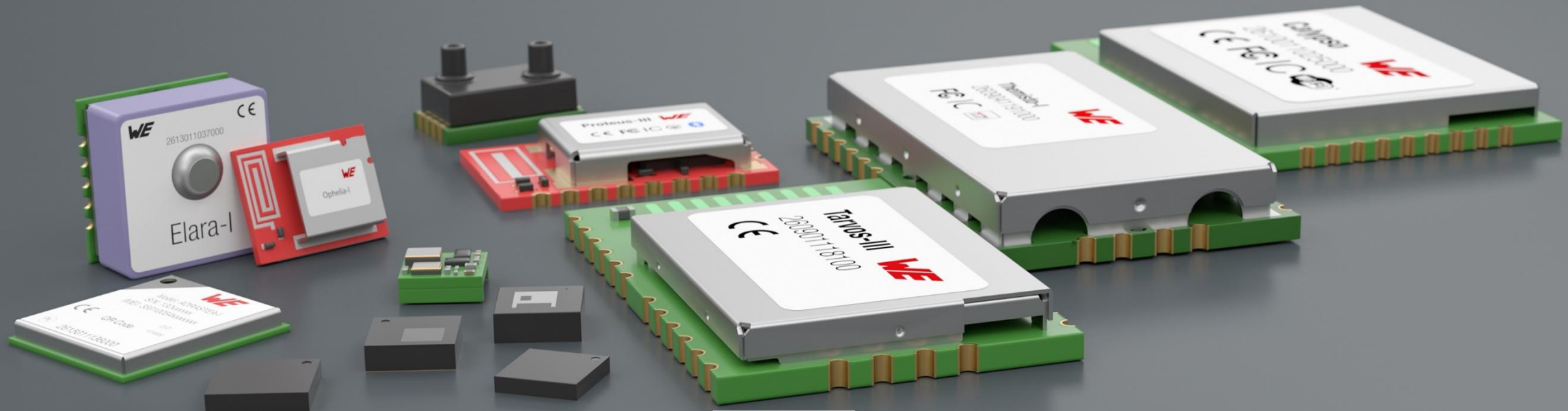


CYBERSECURITY-REGULIERUNGEN (RED) EN18031 & CRA

Kevin Elert
Business Development Manager

AGENDA

- Bedeutung der Cybersecurity im IoT
- Komplexität beim Aufbau eines IoT-Systems
- RED-Delegierter Rechtsakt zur Cybersecurity (EN 18031)
- Praktische Umsetzung der regulatorischen Anforderungen
- Wie WIR (*WE*) sichere IoT-Produkte ermöglichen
- Cyber Resilience Act

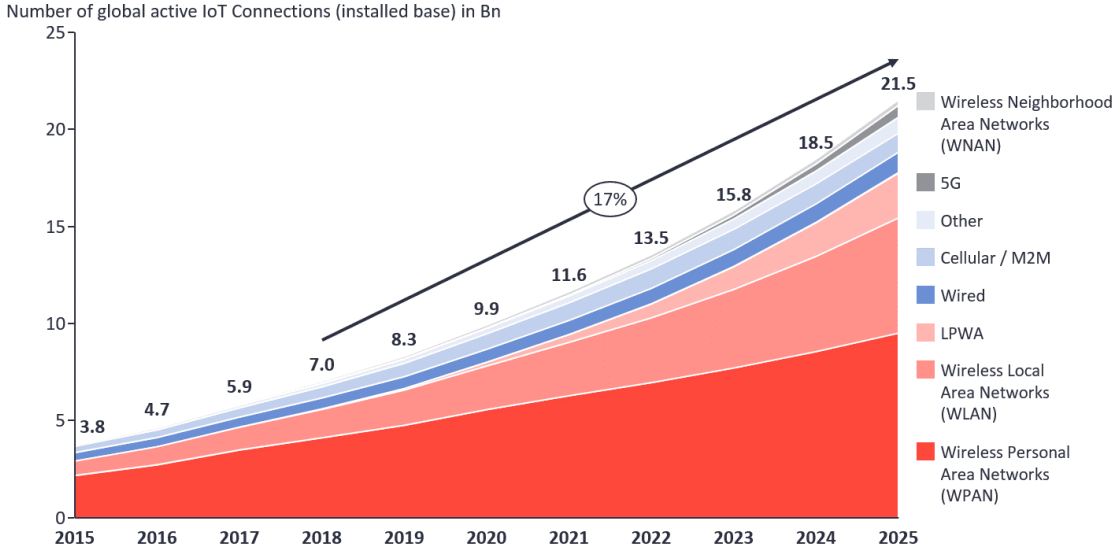
DIE NOTWENDIGKEIT VON CYBERSECURITY

WARUM IST SECURITY BEI IOT WICHTIG?

IOT ANALYTICS

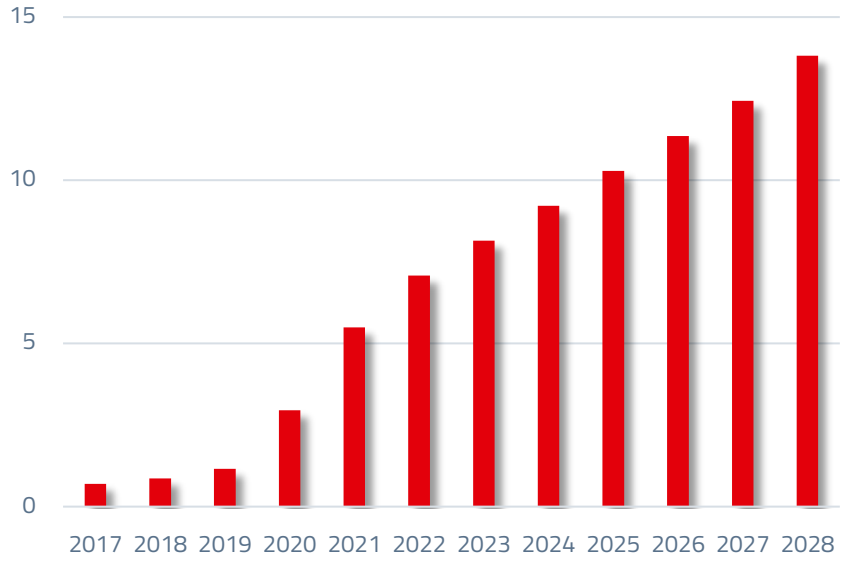
Insights that empower you to understand IoT markets

Global Number of Connected IoT Devices



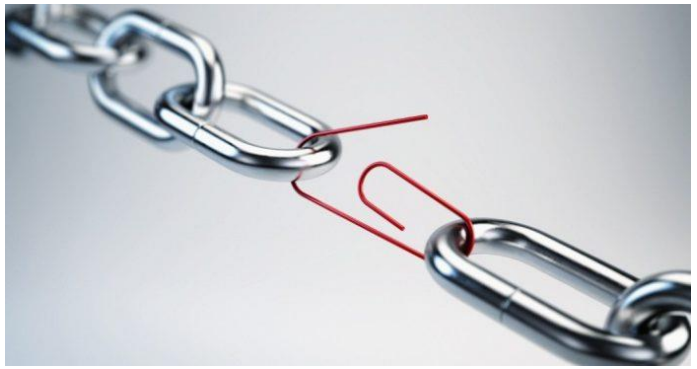
Note: IoT Connections do not include any computers, laptops, fixed phones, cellphones or tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes Ethernet and Fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G; LPWAN includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-fi and related protocols; WNAN includes non-short range mesh; Other includes satellite and unclassified proprietary networks with any range.
Source: IoT Analytics Research 2018

Global Cybercrime impact, Billion US$ (Source : Statista)



WARUM IST SECURITY BEI IOT WICHTIG?

„Angreifer nutzten das smarte Wasserthermometer in einem Aquarium, um sich Zugang zum Netzwerk zu verschaffen. Danach entdeckten sie die High-Roller-Datenbank, zogen die Daten über das Netzwerk zurück durch das Thermostat und luden sie in die Cloud hoch.“



Hackers exploit casino's smart thermometer to steal database info

Nothing is safe.

By Kellen Beck on April 15, 2018

CYBERSECURITY IN IOT ANWENDUNGEN

Warum ist Cybersecurity so komplex?

KOMPLEXITÄT EINES IOT-SYSTEMS

Benutzerschnittstelle
- Datenvisualisierung
- Steuerung und Bedienung

Datenplattform
- Datenaggregation
- Datenanalyse
- Datenaufbereitung und -darstellung

Gateway
- Vebrindung zum Internet
- Edge computing (dezentrale Datenverarbeitung)

Drahtlose Konnektivität
- Sichere Datenübertragung
- Flexibilität und Reichweite

Sensoren und Aktuatoren
- Erfassung physikalischer Umgebungsgrößen
- Digitalisierung von Messwerten
- Ausführen von Aktionen (Aktorik)

Cloud

Gateway

Sensor /Aktuator | Sensor /Aktuator | ... | Sensor /Aktuator

Entwurfskriterien

Cloud Bereich
- Hohe Rechenleistung
- Skalierbarkeit
- Sicherheit
- Flexibilität
- Datenverarbeitung (KI & ML)

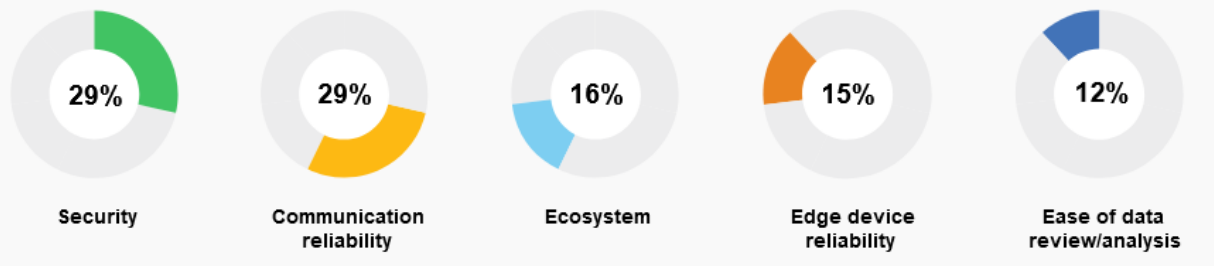
Sicherheit

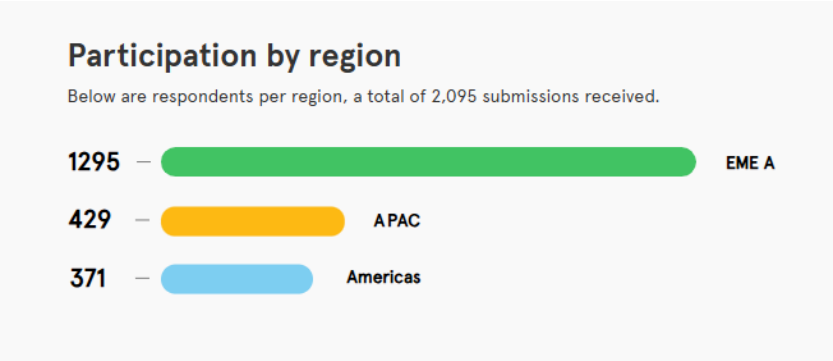
Embedded Bereich
- Geringe Rechenleistung
- Kompakte Bauweise
- Niedriger Energieverbrauch
- Große Reichweite
- Kein oder geringer Installationsaufwand

CYBERSECURITY IST WICHTIG – ABER ICH MÖCHTE KEINE ZEIT ODER GELD DAFÜR INVESTIEREN!

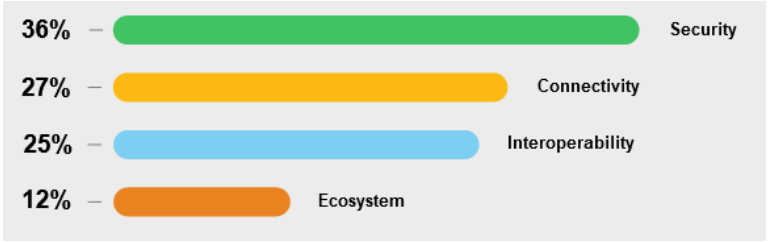
UMFRAGEERGEBNISSE

Was ist der wichtigste Aspekt bei der Entwicklung von IoT-Lösungen?





Was ist Ihre größte Sorge bei der Implementierung von IoT?

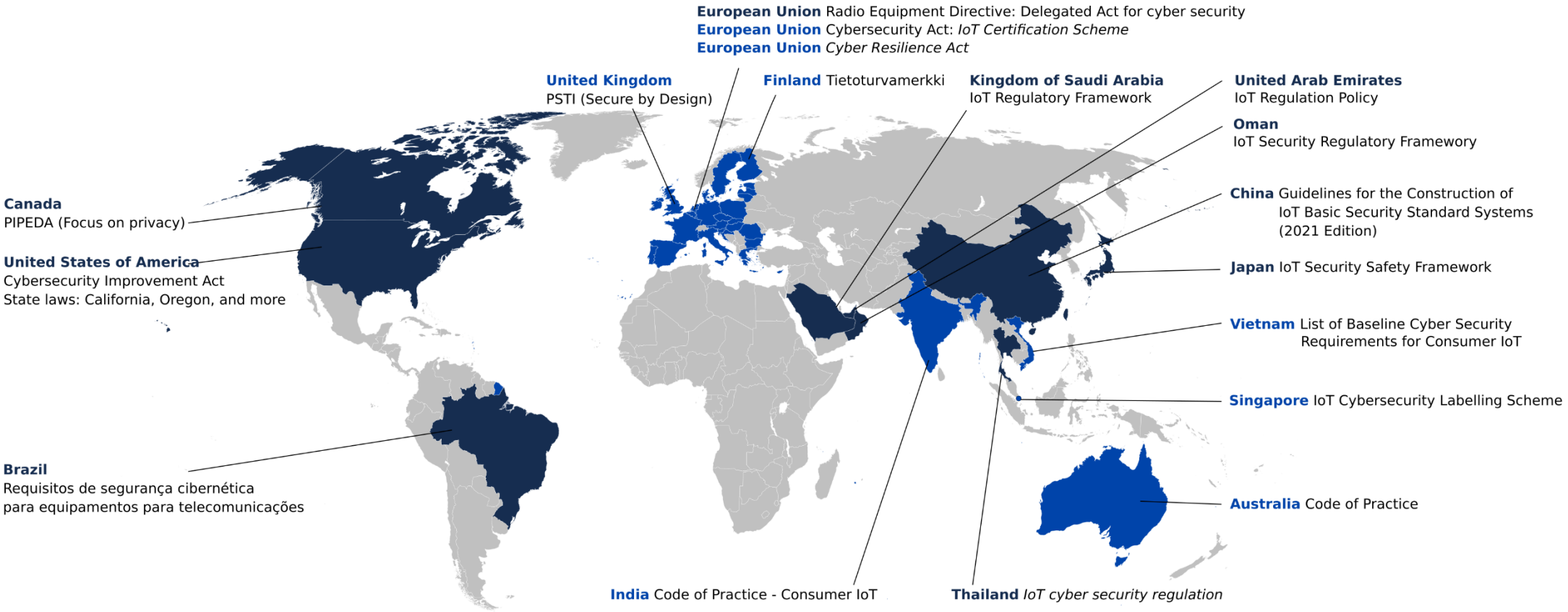


Quelle: https://uk.farnell.com/iot-trends-2021

REGULIERUNGSRAHMEN DER CYBERSECURITY

IOT REGULIERUNGSRAHMEN DER CYBERSECURITY

Worldwide

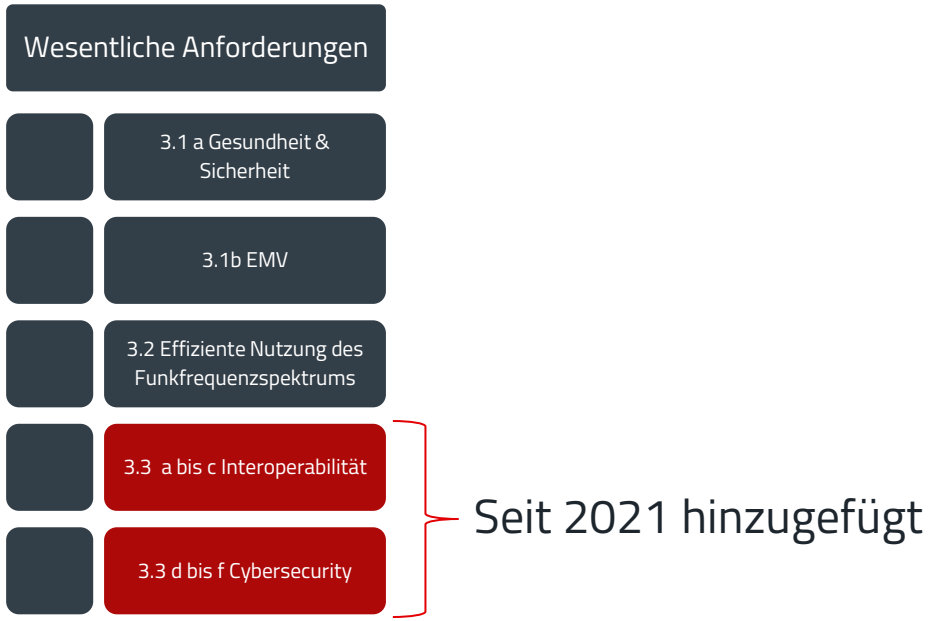


Source - Cetome GitHub Repository :https://github.com/cetome/panorama

RADIO EQUIPMENT DIRECTIVE

- **Offiziell „2014/53/EU“ (Radio Equipment Directive – „RED“) –**
  Seit dem 13.06.2016 im gesamten Europäischen Wirtschaftsraum (EWR) bindend.

- Gilt für alle Funkgeräte.



ZEITLEISTE

Jan 2022
- 2022/30/EU Veröffentlicht
- Artikel 3.3(d), (e) and (f) Durchgesetzt

Feb 2022
Übergangsfrist aktiviert

Jan 2025
Harmonisierte Norm veröffentlicht

Aug 2025
Artikel 3.3(d), (e) and (f) Verpflichtend

Aktuelle Frist
01.08.2025!

HARMONISIERTER STANDARD

- **CEN/CENELEC** hat das Mandat erhalten, die Standards zu erarbeiten
- Drei Standards sind mit bestimmten Einschränkungen harmonisiert:
  - 3.3 (d) -> EN 18031-1:2024
  - 3.3 (e) -> EN 18031-2:2024
  - 3.3 (f) -> EN 18031-3:2024

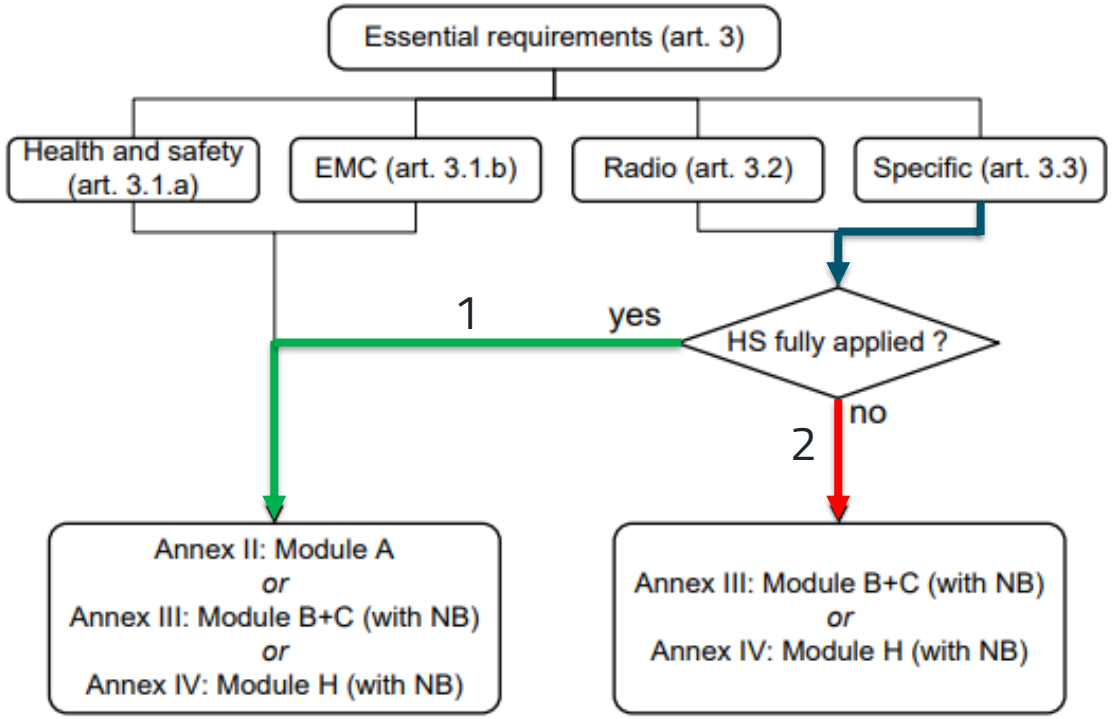
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500138

RED-DELEGIERTER RECHTSAKT FÜR CYBERSECURITY

Pflicht für alle Funkgeräte

3.3 d Netzwerkschutz	▪ Verhinderung von Netzwerkmissbrauch, der zu einer Dienstverschlechterung führt ▪ Alle Geräte, die direkt oder über ein mit dem **Internet verbundenes Gerät kommunizieren können**
3.3 e Datenschutz	▪ Schützt personenbezogene Daten und verbessert die Privatsphäre der Nutzer ▪ Gilt für **alle Geräte**, die über das Internet kommunizieren **und personenbezogene Daten**, **Verkehrsdaten** und/oder **Standortdaten** verarbeiten
3.3 f Betrugsschutz	▪ Betrugsschutz ▪ Gilt für **alle Geräte**, die direkt oder über ein mit dem Internet verbundenes Gerät kommunizieren und den **Transfer von Geld, Geldwerten** oder **virtuellen Währungen ermöglichen**

WIE ERREICHT MAN KONFORMITÄT?



Die drei harmonisierten Standards haben Einschränkungen!

1

- Selbsterklärung
- Harmonisierte Norm notwendig!!!

2

- EU Baumusterprüfung
- Notified body (NB) / Benannte Stelle
- Basierend auf EN 18031-1,2,3

EINSCHRÄNKUNGEN BEI DER HARMONISIERUNG VON EN 18031

Unsere Interpretation

1. Diese Standards (**EN 18031-1, -2, -3:2024**) dürfen nicht zur Konformitätserklärung genutzt werden, wenn Hersteller es dem Nutzer nicht ermöglicht ein Passwort zu setzen oder zu verwenden (**siehe Abschnitte 6.2.5.1 und 6.2.5.2**).

2. **EN 18031-2:2024** darf nicht zur Konformitätserklärung genutzt werden, wenn keine elterliche oder betreuende Kontrolle implementiert ist (**siehe Abschnitte 6.1.3, 6.1.4, 6.1.5 und 6.1.6**).

3. Die Mechanismen gemäß **Abschnitt 6.3.2.4 von EN 18031-3:2024** sind nicht ausreichend, um den Umgang mit finanziellen Vermögenswerten abzudecken, und können daher nicht zur Konformitätserklärung genutzt werden.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500138

EN 18031-1:2024

Zusammengefasste Anforderungen

Access control mechanism (ACM)

- Um unbefugten Zugriff zu verhindern

Authentication mechanism (AUM)

- Mindestens ein Faktor muss für die Authentifizierung verwendet werden

Secure update mechanism (SUM)

- Ein sicherer Mechanismus zur Softwareaktualisierung muss implementiert werden

Secure storage mechanism (SSM)

- Netzwerk- und Sicherheitsressourcen müssen sicher auf dem Gerät gespeichert werden

Secure communication mechanism (SCM)

- Sichere Kommunikation muss für den Austausch von Netzwerk- und Sicherheitsressourcen genutzt werden

Resilience mechanism (RLM)

- Mechanismen zur frühzeitigen Erkennung von Distributed-Denial-of-Service-Angriffen müssen implementiert werden

EN 18031-1:2024

Zusammengefasste Anforderungen

Network monitoring mechanism (NMM)

- Mechanismen zur Abwehr von Denial-of-Service-Angriffen müssen implementiert werden

Traffic control mechanism (TCM)

- Mechanismen zur Steuerung und Begrenzung des Netzwerkverkehrs implementieren.

Confidential cryptographic keys (CCK)

- Mindest-Sicherheitsstärke von Schlüsseln: 112 Bit

General equipment capabilities (GEC)

- Das Gerät darf keine bekannten, ausnutzbaren Schwachstellen enthalten.
- Begrenzung der Exposition von Diensten über verbundene Netzwerkschnittstellen
- Dokumentation optionaler Schnittstellen und Dienste
- Entfernung nicht benötigter Schnittstellen
- Eingabeverifizierung

Cryptography (CRY)

- Bewährte Verfahren für Kryptografie anwenden

TERMINOLOGIE

Begriffe in den Standards

- „Assets“ können folgende Typen umfassen:

Essential requirements	EN 18031-1 RED 3.3 (d)	EN 18031-2 RED 3.3 (e)	EN 18031-3 RED 3.3 (f)
Security asset	☑	☑	☑
Network asset	☑	☒	☒
Privacy asset	☒	☑	☒
Financial asset	☒	☒	☑

- **„Mechanism“** – Methoden zur Umsetzung von Sicherheitsmaßnahmen

- **„Entities“** – Nutzer, Software, Netzwerkpartner …

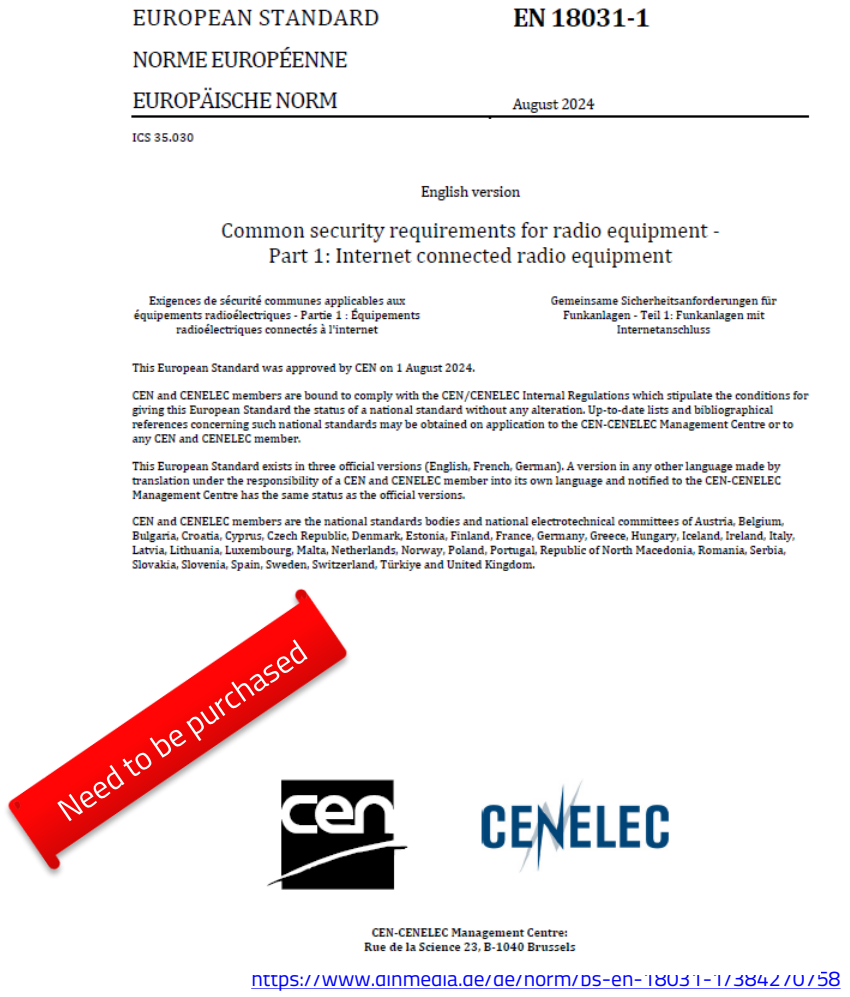
BEISPIEL 2

Raspberry Pi

Abkürzung	Mechanismus	EN 18031-1	EN 18031-2	EN 18031-3
ACM	Mechanismus der Zugangskontrolle	☑	☑	☑
AUM	Mechanismus zur Authentifizierung	☑	☑	☑
SUM	Sicherer Aktualisierungsmechanismus	☑	☑	☑
SSM	Sicherer Speichermechanismus	☑	☑	☑
SCM	Mechanismus für sichere Kommunikation	☑	☑	☑
RLM	Ausfallsicherheits-Mechanismus	☑	☒	☒
LGM	Mechanismus zur Protokollierung	☒	☑	☑
NMM	Mechanismus zur Netzwerküberwachung	☑	☒	☒
DLM	Mechanismus zur Löschung von Daten	☒	☑	☒
TCM	Mechanismus zur Verkehrskontrolle	☑	☒	☒
UNM	Mechanismus zur Benachrichtigung der Benutzer	☒	☑	☒
CCK	Vertrauliche kryptografische Schlüssel	☑	☑	☑
GEC	Allgemeine Ausstattungsmerkmale	☑	☑	☑
CRY	Kryptographie	☑	☑	☑

START HERE!

- Definieren Sie klar den vorgesehenen **Einsatzzweck** Ihres Produkts
- Prüfen Sie, ob Ihr Funkgerät über das Internet **kommuniziert**
- Kontaktieren Sie Ihr **akkreditiertes Labor**
  und/oder
- **Erwerben Sie die Standards** (sie sind nicht kostenlos verfügbar)
- **Führen Sie eine Cybersecurity-Risikobewertung durch** – Dies umfasst die Identifikation von Assets, Entitäten, Schnittstellen und Mechanismen
- Arbeiten Sie die **Entscheidungsbäume** im Standard durch und führen Sie die konzeptionelle sowie funktionale Bewertung durch
- **Dokumentieren** Sie das Ergebnis Ihrer Bewertung
- **Informieren** Sie Ihre **Endnutzer** über Cybersecurity-Best Practices



EUROPEAN STANDARD **EN 18031-1**

NORME EUROPÉENNE

EUROPÄISCHE NORM August 2024

ICS 35.030

English version

Common security requirements for radio equipment -
Part 1: Internet connected radio equipment

Exigences de sécurité communes applicables aux équipements radioélectriques - Partie 1 : Équipements radioélectriques connectés à l'internet

Gemeinsame Sicherheitsanforderungen für Funkanlagen - Teil 1: Funkanlagen mit Internetanschluss

This European Standard was approved by CEN on 1 August 2024.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

Need to be purchased

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

https://www.dinmedia.de/de/norm/ds-en-18031-1/384270758

BEISPIELE

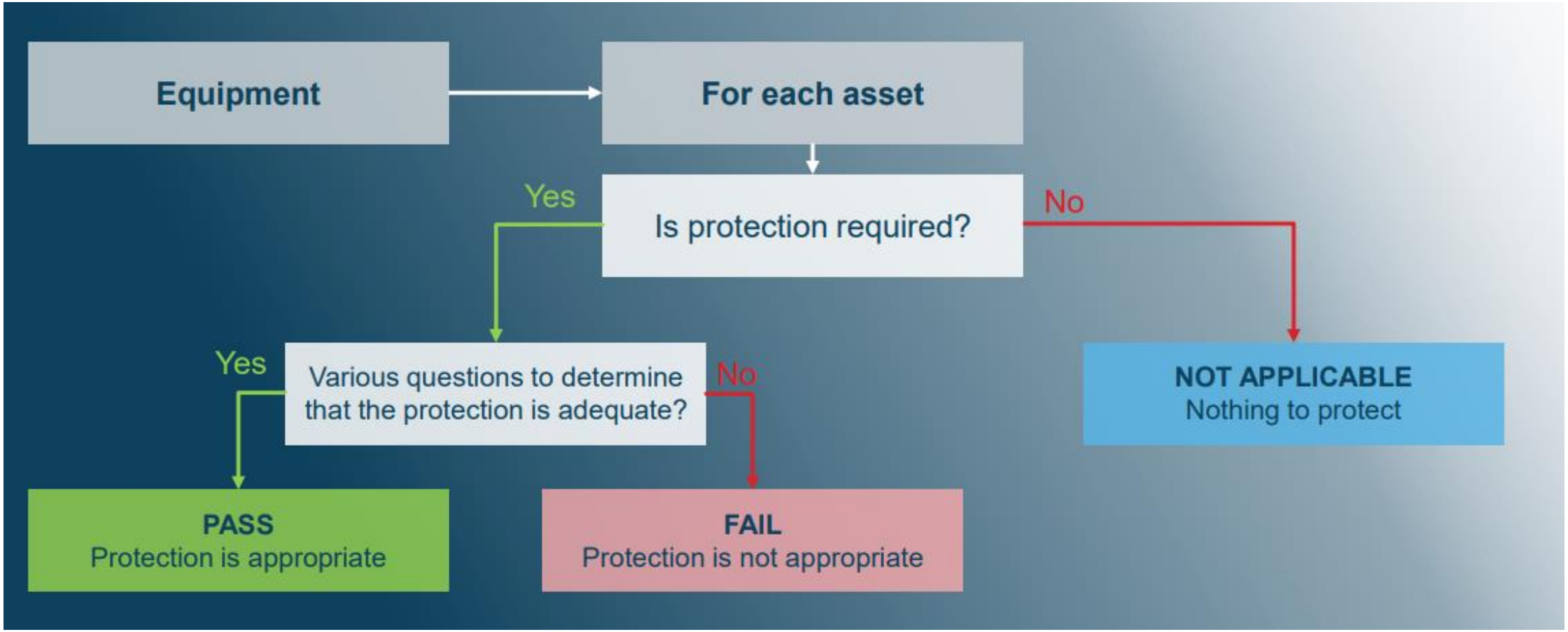
BEISPIEL 1

Walkie-Talkie

- Beeinflusst das Internet? ✗
- Persönliche Daten auf dem Gerät? ✗
- Finanzdaten auf dem Gerät? ✗

Insellösung!

DECISION TREES



BEISPIEL 1

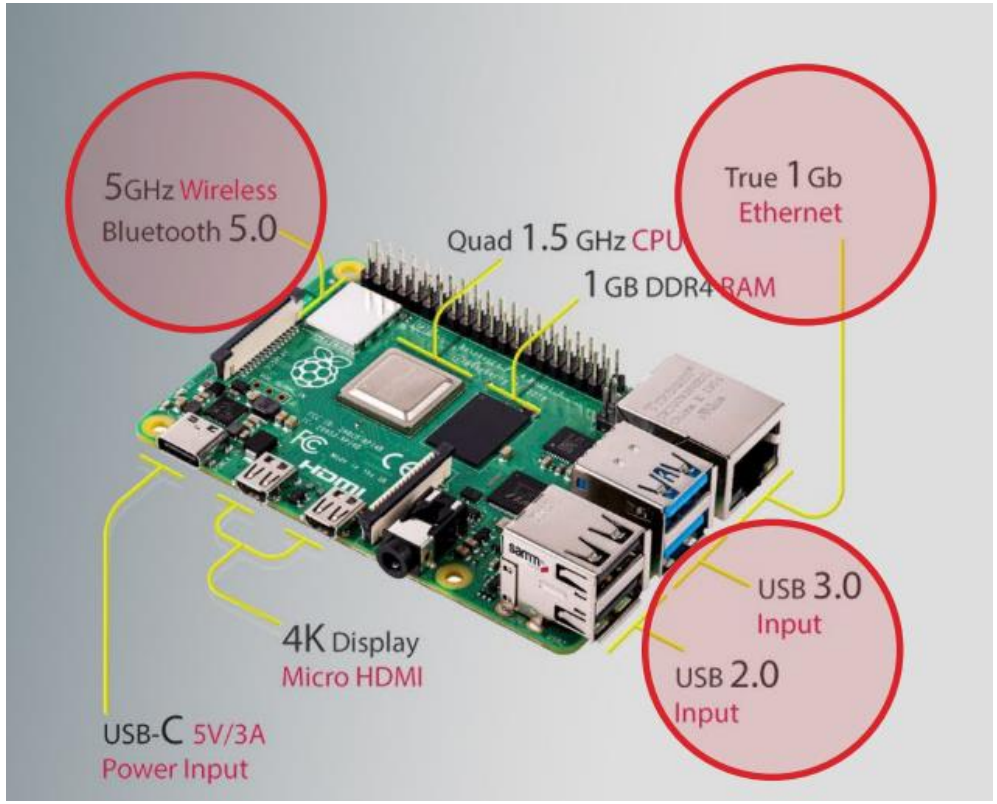
Walkie-Talkie

Requirements	Specification/conditons	Compliance verfied by
(d) Radio equipment does not **harm the network** or its functioning nor misuses network resources, thereby causing an unacceptable degradation of service	d) **Not applicable**: The DUT is only able to communicate via the following interfaces and protocols: 1. Bluetooth Low Energy 4.0: Using for first installations, updates and process data communication. The communication is done using protocols which does not exchange data with the internet either directly or of an intermediate equipment. The DUT is not capable itself to communicate over the internet. 2. profibus: Profibus is used to monitor and control the connected devices. The communication is done using protocols which does not exchange data with the internet either directly or of an intermediate equipment. The DUT is not capable itself to communicate over the internet.	
e) Radio equipment incorporates safeguards to ensure that the **personal data** and privacy of the user and of the subscriber are protected	e) **Not applicable**: The DUT does not pose a risk to the user's privacy, as it does not store or process any personal data.	
(f) Radio equipment supports certain features ensuring protection from **fraud**	f) **Not applicable**: The DUT cannot pose a risk of fraud because it does not store or process financial data.	

BEISPIEL 2

Raspberry-Pi

- Beeinflusst das Internet? ✓
- Persönliche Daten auf dem Gerät? ✗
- Finanzdaten auf dem Gerät? ✗

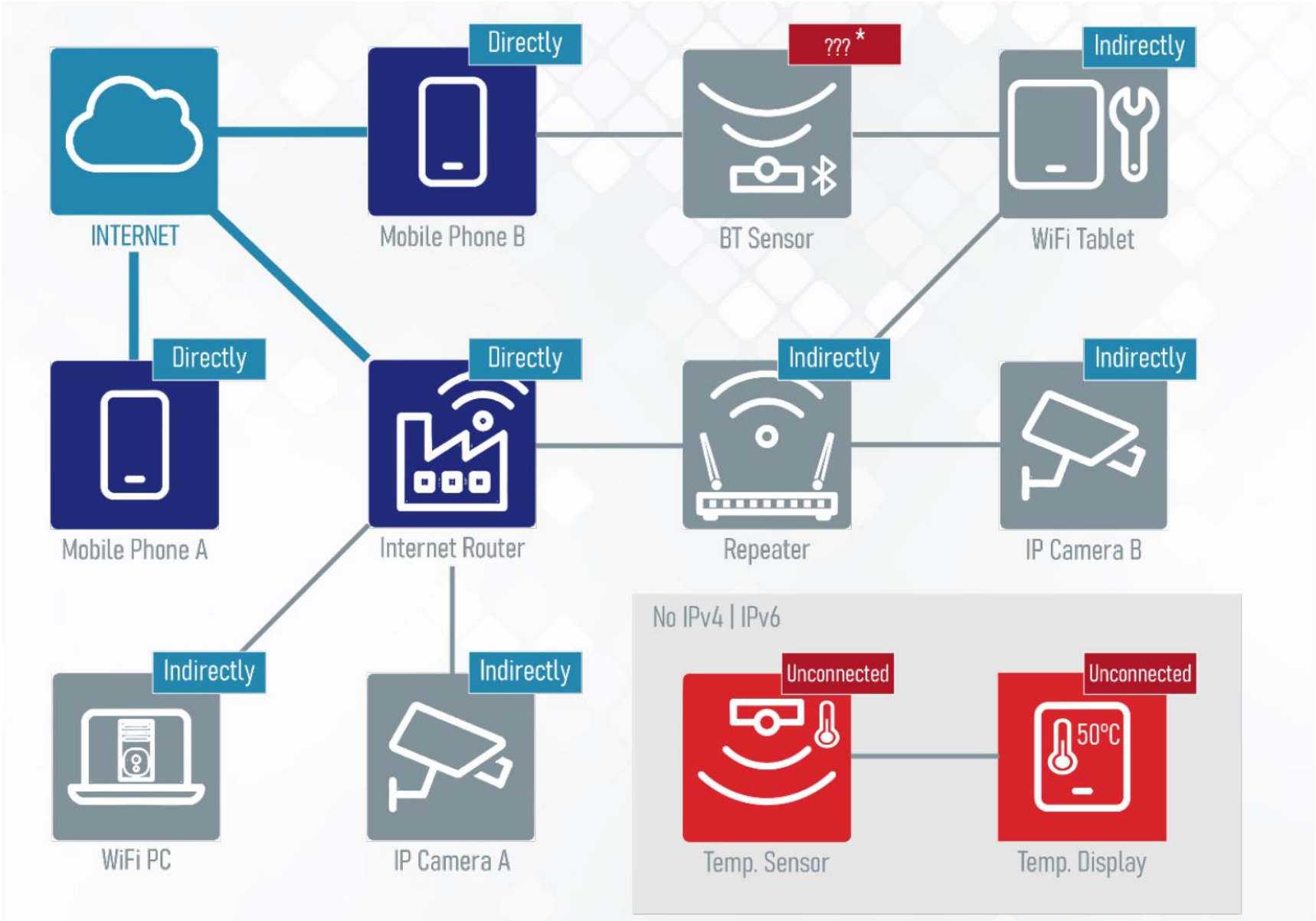


BEISPIEL 2

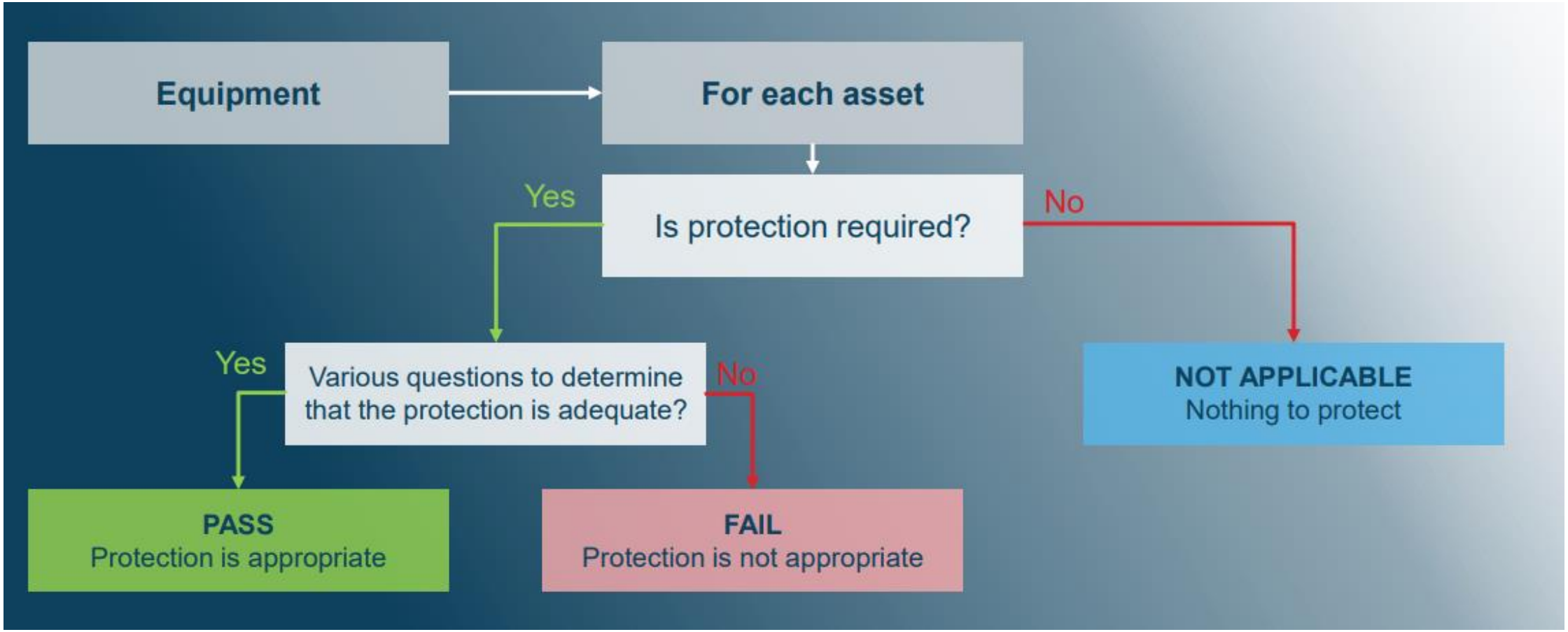
Raspberry Pi

Requirements	Specification/conditons	Compliance verfied by
(d) Radio equipment does not harm the network or its functioning nor misuses network resources, thereby causing an unacceptable degradation of service	**d) Applicable:** The DUT is communicated via the following interfaces and protocols: 1. WLAN 802.11b: Using for first installations, updates and process data communication. The communication is done via TCP/IP.	EN18031-1
e) Radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected	**e) Not applicable:** The DUT does not pose a risk to the user's privacy, as it does not store or process any personal data.	
(f) Radio equipment supports certain features ensuring protection from fraud	**f) Not applicable:** The DUT cannot pose a risk of fraud because it does not store or process financial data.	

DIREKT / INDIREKT



DECISION TREES



CYBERSECURITY-RISIKOBEWERTUNG

BEDROHUNGSMODELLIERUNG UND SICHERHEITSANALYSEN

- **Asset : Was muss geschützt werden?**
  - Geräte-ID
  - Firmware
  - Zugangsdaten (Passwörter, Zertifikate etc.)
  - Biometrische Daten

- **Ziel: Was soll erreicht werden?**
  - Authentizität
  - Integrität
  - Datenschutz
  - Vertraulichkeit

- **Bedrohungen: Wogegen muss geschützt werden?**
  - **Remote-Angreifer:** Software, Netzwerk
  - **Lokale/physische Angreifer:** Software, Netzwerk, Hardware
  - **Gerätespezifische Angreifer:** Diebstahl des Geräts, Manipulation der Stromversorgung
  - **Weitere Angreifer:** Insider-Angriff, Hochentwickelte Hardware-Angriffe

- **Mechanismus: Wie wird das erreicht?**
  - Zwei-Faktor-Authentifizierung
  - Datenverschlüsselung
  - Sichere Firmware Updates
  - Signaturprüfung
  - Validierung von Eingabedaten

CYBERSECURITY RISK ASSESSMENT

- Was wird geschützt?
- Wovor wird geschützt?
- Was soll erreicht werden?
- Was wird benötigt, um dies zu erreichen?

Asset	Asset	Asset
Cloud Zugangsdaten	Firmware	Wireless link
Bedrohung	Bedrohung	Bedrohung
Remote-Softwareangriffe	Remote-Softwareangriffe	Remote-Softwareangriffe
Sicherheitsziel	Sicherheitsziel	Sicherheitszie
Authentifizierung	Integrität	Authentizität & Integrität
Sicherheitsmechanismen	Sicherheitsmechanismen	Sicherheitsmechanismen
Sicherer Speicher	Sicheres FW-Update	Datenverschlüsselung

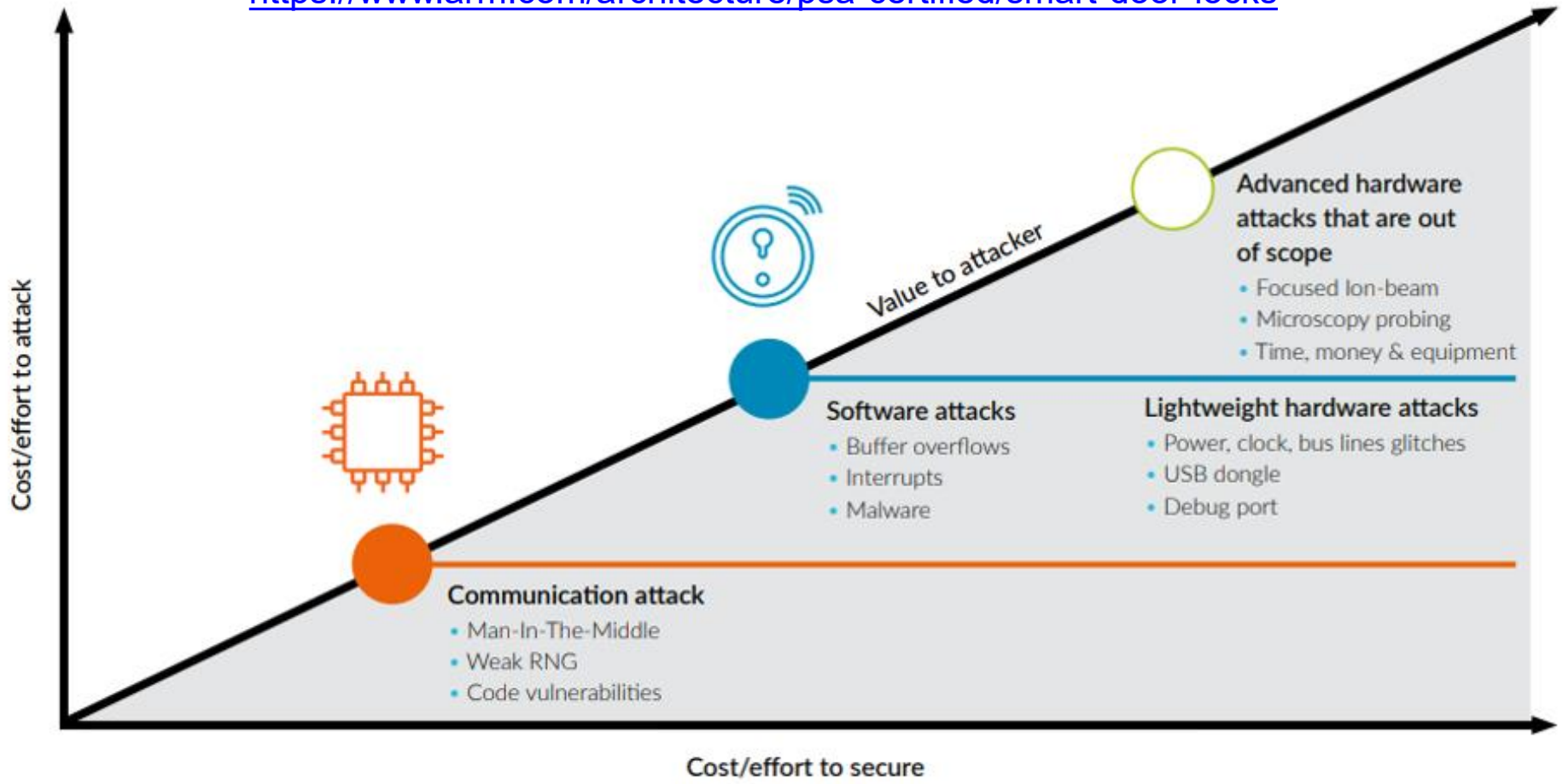
https://www.arm.com/architecture/psa-certified/smart-door-locks

THREAT MODELLING –STRIDE MODELL

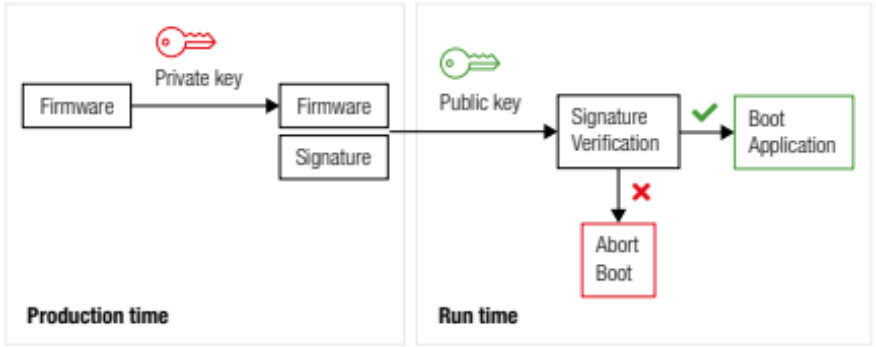
- **S** – Spoofing – Vortäuschen einer falsche Identität (z.B. gestolene Zugangsdaten)
- **T** – Tampering – Manipulation von Daten oder Code (z.B. Firmware-Veränderung)
- **R** – Repudiation – Abstreiten von Aktionen ohne Nachweisbarkeit (fehlender Log-in)
- **I** – Information disclosure - Unbefugte Offenlegung von Sensiblen Informationen
- **D** – Denial-of-Service – Störung oder Blockierung von Diensten oder Systemressourcen
- **E** – Elevation-of-Privilege – Erlangen höherer Rechte durch Ausnutzen von Schwachstellen

KOMPROMISSE / ABWÄGUNGEN

https://www.arm.com/architecture/psa-certified/smart-door-locks

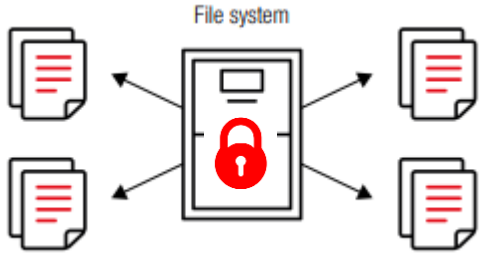


GÄNGIGE MINIMALE-SICHERHEITSFUNKTIONEN

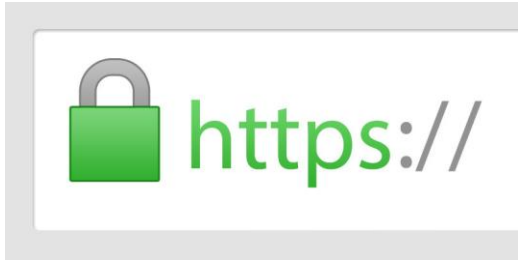


Sichere Produktion

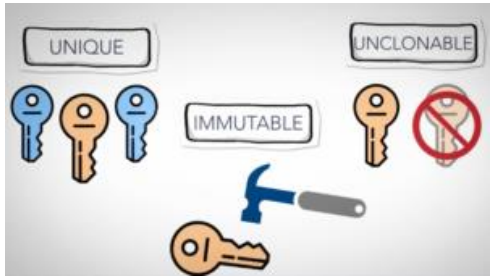
Sicheres booten



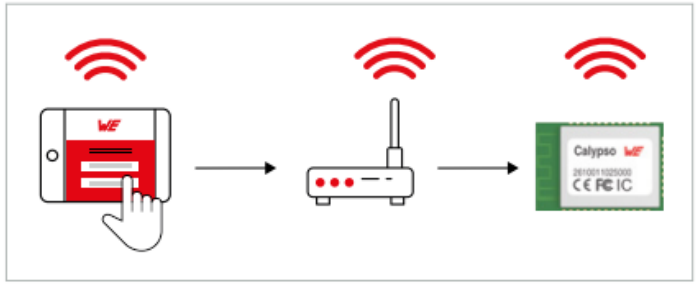
Vertrauliche Datenablage



Sichere Verbindung



Sicherer root of trust



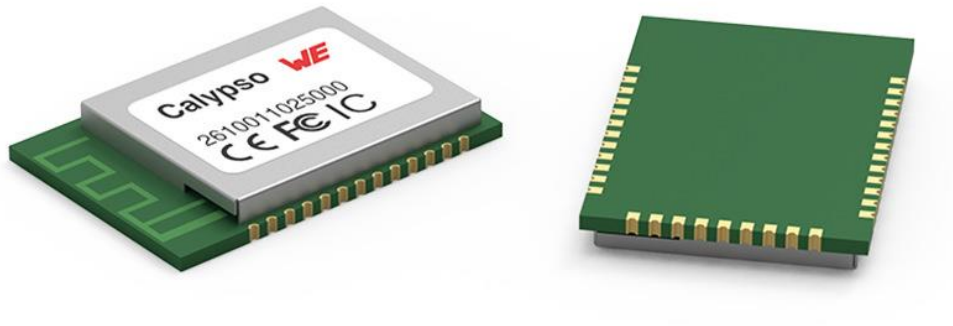
Sicheres FOTA

Physische Sicherheit

WIE SETZEN WIR DIES PRAKTISCH IN UNSEREM ENDGERÄT UM?

CALYPSO WI-FI MODUL

Secure IoT ready



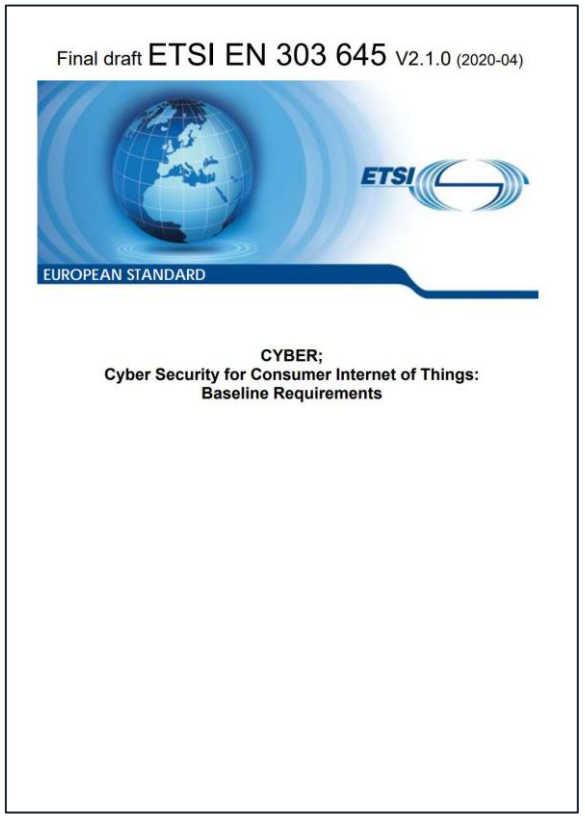
- ✓ 10-Byte nicht manipulierbare, eindeutige Geräte-ID
- ✓ Sicherer Bootvorgang (Secure Boot)
- ✓ **Sicherer Datenablage** – Verschlüsseltes Dateisystem zur Speicherung von Zertifikaten und anderen Anmeldeinformationen
- ✓ Sichere Wi-Fi-Verbindung – WPA3
- ✓ Secure socket – TLSv1.2
- ✓ Hardware-beschleunigte Krypto-Engine
- ✓ Sicheres Firmware-Update über die Luft (FOTA)

Wi Fi CERTIFIED

CE FC IC

Eine solide Grundlage für eine sichere Endanwendung!

GUTE DOKUMENTATION



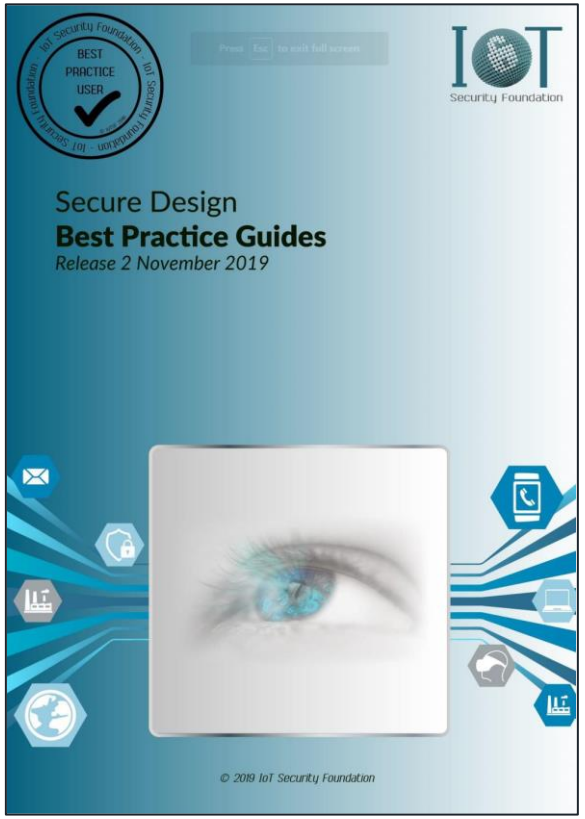
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

IEC 62443-3-3

Industrial communication networks – Network and system security

Part3-3: System security requirements and security levels

https://www.vde-verlag.de/normen/0800628/din-en-iec-62443-3-3-vde-0802-3-3-2020-01.html



https://iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2_Digitalv3.pdf

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

CYBER RESILIENCE ACT

CYBER RESILIENCE ACT IN DER EU

- **Verpflichtende Cybersicherheitsstandards:** Hersteller sind verpflichtet, die Cybersicherheit über den gesamten Lebenszyklus von Produkten mit digitalen Elementen sicherzustellen.
- **Anwendungsbereich:** Gilt für alle Produkte, die direkt oder indirekt mit einem anderen Gerät oder Netzwerk verbunden sind – mit bestimmten Ausnahmen.
- **CE-Kennzeichnung:** Produkte müssen die **CE-Kennzeichnung** tragen, um die Einhaltung der Cybersicherheitsanforderungen zu bestätigen.
- **Lebenszykluspflege:** Hersteller sind verpflichtet, **Sicherheitsupdates und Wartung** für ihre Produkte während des gesamten Lebenszyklus bereitzustellen.
- **Umsetzungszeitraum:** Die **Hauptpflichten gelten ab dem 11. Dezember 2027**

WELCHE RISIKEN SOLL DER VORSCHLAG ADRESSIEREN?

Marktanfälligkeit

- Angriffe breiten sich innerhalb von Minuten über Grenzen hinweg aus.
- Unzureichende Sicherheit ist die aktuelle Marktnorm.

Vernachlässigung durch Hersteller

- Kein langfristiger Support oder Sicherheitsupdates..
- Minimaler Antrieb, in „Security by Design“ (Sicherheit durch Systemarchitektur) zu investieren.

Belastung der Verbraucher

- Benutzern fehlen die Informationen, um Geräte sicher einzurichten.
- Die Kosten für Sicherheitsvorfälle trägt der Verbraucher.

ANWENDUNGSBEREICH DES CRA

- Gilt für alle Produkte mit digitalen Elementen (PDEs):
  - **Embedded devices** (IoT, industrielle Steuerungen)
  - **Software und Firmware**
  - **Vernetzte Maschinen und Anlagen**
- Umfasst **EU-Hersteller, Händler** und **Importe** aus der ganzen Welt.
- Schließt einige branchenspezifische Produkte aus (z. B. Medizinprodukte, Automobilbranche, Schifffahrt).

WAS SCHREIBT DER CRA VOR?

Grundlegende Cybersicherheitsanforderungen

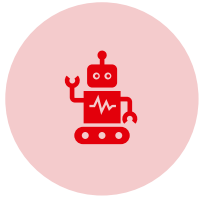
Teil I – Sicherheitsanforderungen für Produkte

- Standardmäßig sichere Konfiguration ohne bekannte ausnutzbare Schwachstellen
- Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Daten
- Zugriffskontrolle, Verschlüsselung und Minimierung von Angriffsflächen
- Widerstandsfähigkeit gegen Denial-of-Service-Angriffe
- Sichere Update-Mechanismen, einschließlich standardmäßig aktivierter automatischer Sicherheitsupdates

Teil II – Anforderungen an den Umgang mit Schwachstellen

- Systematische Identifizierung und Dokumentation von Schwachstellen, auch in Drittanbieter-Komponenten (SBOM)
- Rechtzeitige Entwicklung und Bereitstellung von kostenlosen Sicherheitspatches
- Regelmäßige Tests und Überprüfungen der Produktsicherheit
- Richtlinien zur öffentlichen Offenlegung und koordiniertes Schwachstellenmanagement

ZENTRALE HERSTELLERPFLICHTEN



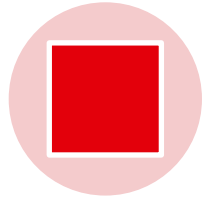
Cybersicherheit in den gesamten **Produktlebenszyklus** integrieren: Design, Entwicklung, Produktion, Wartung, Ende der Lebensdauer.

Cybersicherheits-Risikobewertungen durchführen und Ergebnisse dokumentieren.

Sicherheitsupdates während der gesamten Produktlebensdauer bereitstellen.

Schwachstellen und Vorfälle umgehend **melden**.

Konformitätsbewertung durchführen & **CE-Kennzeichnung** erhalten.



Informationen und Anweisungen für den Benutzer bereitstellen, um eine sichere Nutzung des Produkts zu gewährleisten.

CRA – ZEITPLAN

Dec 2024

Der CRA wird in der EU geltendes Recht. 36-monatige Übergangsfrist.

Sept 2026

Artikel 14 tritt in Kraft und schreibt Meldepflichten an die ENISA vor.

DEC 2027

Der CRA ist vollständig auf alle Geräte mit digitalen Elementen anwendbar.

WAS PASSIERT MIT NICHT KONFORMEN PRODUKTEN?

- **Marktüberwachung**: Behörden zur Durchsetzung der Konformität (Einhaltung der Richtlinien).
- **Strafen**: Geldbußen und Einschränkungen bei Nichteinhaltung.
  - Bis zu 15 Mio. € oder 2,5 % des weltweiten Jahresumsatzes bei Nichterfüllung der grundlegenden Cybersicherheitsanforderungen.
  - Bis zu 10 Mio. € oder 2 % des Umsatzes bei sonstigen Pflichtverletzungen.
  - Bis zu 5 Mio. € oder 1 % des Umsatzes für die Bereitstellung falscher oder unvollständiger Informationen an die Behörden.
- **Maßnahmen**: Rücknahme oder Rückruf nicht konformer Produkte vom Markt.
- **Rechtliche Konsequenzen**: Mögliche rechtliche Schritte gegen nicht konforme Hersteller.
- **Rufschädigung**: Nichteinhaltung kann dem Ruf der Marke schaden.

Stock Image, Microsoft Office

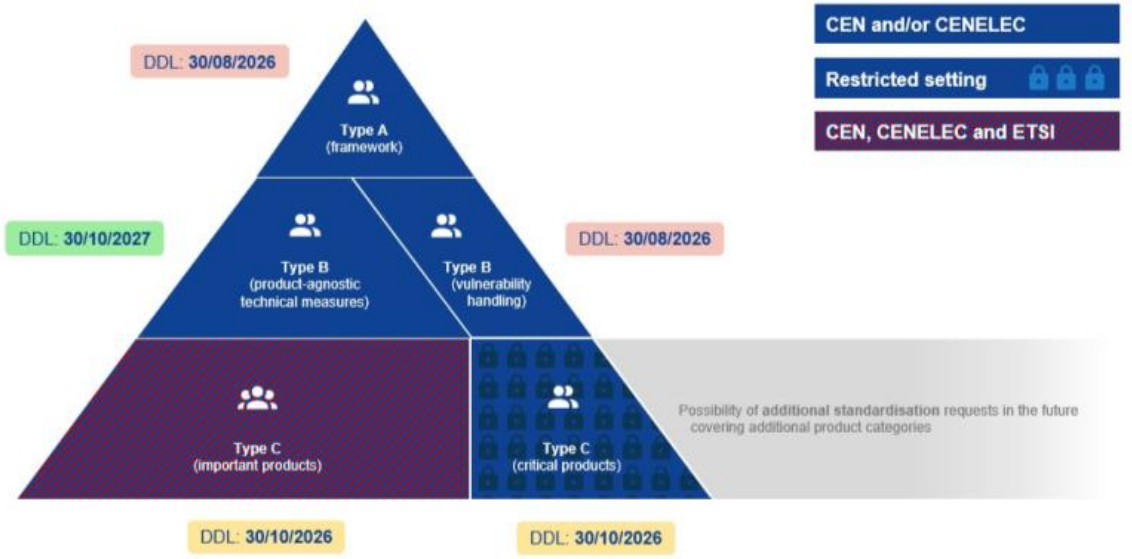
PRODUKTKLASSIFIZIERUNG UND KONFORMITÄT

Kategorie	Risiko	Konformität	Beispiele
Standard (Default)	Niedrig	Selbsterklärung	Smart-Home-Geräte, Drucker, Bluetooth-Lautsprecher, Media-Player-Softwareanwendungen
Klasse I	Wichtig	Selbsterklärung, sofern eine harmonisierte Norm anwendbar ist	Eigenständige & eingebettete Browser, Passwort-Manager, Betriebssysteme (OS), Boot-Manager, Router, Modems
Klasse II	Wichtig	Bewertung durch Dritte *(Prüfung durch externe Stelle)*	Hypervisoren, Firewalls, manipulationssichere Mikrocontroller (MCUs) und Prozessoren
Kritische Klasse	Kritisch	Bewertung durch Dritte *(Prüfung durch externe Stelle)*	Smart-Meter-Gateways, Smartcards, Hardware mit Sicherheitsmodulen (Security Boxes)

DIE STANDARDISIERUNGSLANDSCHAFT FÜR DEN CRA

- **Typ A: Rahmenstandards**
  - Define principles, terms or framework conditions
  - prEN 40000-1-1 (Vocabulary)
  - prEN 40000-1-2 (Principles for Cyber Resilience)
- **Typ B: Horizontale Standards**
  - Product-agnostic CRA requirements
  - prEN 40000-1-3 (Vulnerability Handling)
  - prEN 40000-1-4 (Generic Security Requirements)
- **Typ C: Vertikale (Product-Specific) Standards**
  - EN 304 6xx Series

https://www.stan4cra.eu/



WAS IST EIN PRODUKT MIT DIGITALEN ELEMENTEN? WANN FÄLLT ES UNTER DEN CRA?

- Ein Produkt mit digitalen Elementen ist „ein Software- oder Hardwareprodukt und seine Fern-Datenverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die separat in Verkehr gebracht werden“ (Artikel 3 Absatz 1).

- Dies umfasst eigenständige Software-Apps, separat verkaufte Firmware, Hardware im Bundle mit Software (wie Drucker mit Treibern) sowie Hardwarekomponenten wie Sensoren, integrierte Schaltkreise und IoT-Geräte.

- Anwendungsbereich des CRA – drei Bedingungen müssen erfüllt sein:
  - es ist ein Produkt mit digitalen Elementen,
  - es wird in Verkehr gebracht, und
  - es verfügt über eine direkte oder indirekte Verbindung zu einem Gerät oder Netzwerk..

- Eine **physische Verbindung** nutzt elektrische, optische, mechanische Schnittstellen, Kabel oder Funkwellen (USB, Ethernet, WLAN, Bluetooth, NFC). Eine **logische Verbindung** ist eine virtuelle Datenverbindung über eine Softwareschnittstelle (z. B. ein Browser, der eine HTTPS-Verbindung aufbaut, oder ein E-Mail-Client, der IMAP nutzt). Eine **indirekte Verbindung** liegt vor, wenn ein Produkt sich nicht selbst verbindet, sondern auf einem Host-System läuft, das dies tut (z. B. ein Offline-Texteditor auf einem vernetzten Betriebssystem). Produkte ohne jegliche Konnektivität (z. B. ein einfacher Taschenrechner) fallen nicht in den Geltungsbereich des CRA.

- PDEs (Produkte mit digitalen Elementen), die vor dem 11. Dezember 2027 in Verkehr gebracht werden, fallen nicht unter den CRA, es sei denn, sie erfahren nach dem 11. Dezember 2027 eine **wesentliche Änderung**. Die **Meldepflichten** (Artikel 14) für aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle gelten jedoch für alle Produkte im Anwendungsbereich, auch für solche, die vor diesem Datum in Verkehr gebracht wurden..

WAS BEDEUTET „INVERKEHRBRINGEN“ (PLACING ON THE MARKET)?

- **Inverkehrbringen (Placing on the market)** - Definition: „Inverkehrbringen“ bezeichnet den Zeitpunkt, an dem ein Produkt ***erstmalig auf dem EU-Markt*** **bereitgestellt** wird. Dies geschieht durch einen Hersteller oder einen Importeur und bezieht sich auf jedes einzelne Produkt, nicht auf einen Typ oder ein Modell. Sobald ein Produkt in Verkehr gebracht wurde, kann es weiterverkauft oder in der Lieferkette weitergegeben werden, ohne dass dies erneut als „Inverkehrbringen“ gilt. Beispiel: Ein Hersteller in Deutschland produziert eine Charge smarter Thermostate. Wenn diese Thermostate zum ersten Mal an einen Händler in Frankreich verkauft werden, werden sie „in Verkehr gebracht“. Einige Anforderungen des CRA gelten auch für Produkte, die auf dem Markt bereitgestellt werden, nachdem sie in Verkehr gebracht wurden. Dies wird als „Bereitstellung auf dem Markt“ bezeichnet. (BSI TR 03183-1)
- **Bereitstellung auf dem Markt (Making available on the market)** - Definition: „Bereitstellung auf dem Markt“ bezeichnet jede Abgabe eines Produkts für den Vertrieb, den Verbrauch oder die Verwendung auf dem EU-Markt im Rahmen einer Geschäftstätigkeit, sei es gegen Entgelt oder unentgeltlich. Dies bezieht sich **auf** ***jede einzelne Abgabe eines Produkts für den Vertrieb, den Verbrauch oder die Verwendung auf dem EU-Markt*** und umfasst jede Weitergabe eines Produkts, einschließlich Verkauf, Leasing, Vermietung oder unentgeltlicher Abgabe. Dies gilt für die gesamte Lieferkette, nachdem das Produkt in Verkehr gebracht wurde. Beispiel: Wenn ein Händler in Frankreich das smarte Thermostat an einen Einzelhändler verkauft und der Einzelhändler es an einen Endverbraucher verkauft, ist jede dieser Transaktionen eine „Bereitstellung auf dem Markt“. Zusammenfassend lässt sich sagen: Inverkehrbringen ist die erstmalige Abgabe eines Produkts für den Vertrieb, den Verbrauch oder die Verwendung auf dem EU-Markt, und die Bereitstellung auf dem Markt ist jede nachfolgende Abgabe (Verkauf, Weitergabe usw.) des Produkts auf dem EU-Markt, nachdem es in Verkehr gebracht wurde. (BSI TR 03183-1)

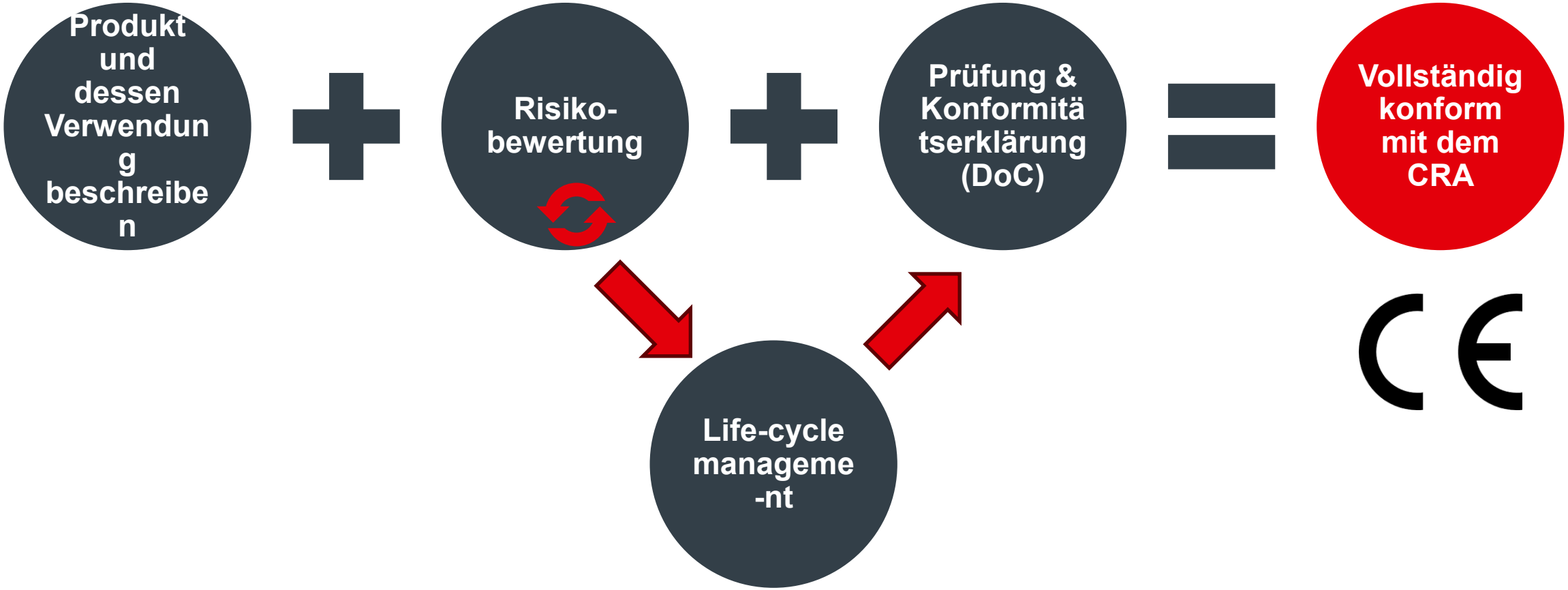
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-0318…

WIE IST DAS ZUSAMMENSPIEL MIT DEN BESTEHENDEN VORSCHRIFTEN?

- NIS2 Richtlinie
  - Der Cyber Resilience Act (CRA) wird die NIS2-Richtlinie ergänzen.
  - Ein verbessertes Cybersicherheitsniveau bei Produkten mit digitalen Elementen würde die Einhaltung von NIS2 erleichtern.

- RED-DA (Delegierte Verordnung zur Funkanlagenrichtlinie) EN18031
  - Der Cyber Resilience Act ist auf die Anforderungen der delegierten RED-Verordnung abgestimmt.
  - Um rechtliche Klarheit zu gewährleisten, wird die delegierte RED-Verordnung daher geändert oder aufgehoben, sobald der CRA anwendbar wird.

WEG ZUR KONFORMITÄT – CRA



CRA FAQ DOCUMENT

https://ec.europa.eu/newsroom/dae/redirection/document/122331

CRA STANDARDIZATION DASHBOARD

Find the latest state of standardization in this link

VIELEN DANK!