Willkommen

Radio Equipment Directive
Cybersecurity

Dietmar Frei , April.2024

Ihr Referent

Dietmar Frei

Leitung
Cybersecurity

- +49 5235 9500-15
- Frei.dietmar@phoenix-testlab.de

Frohmensch, Querdenker, Bastler, Technik-Begeisterter und jahrelang Head of Customer Communications bei Phoenix Testlab.
Seit 2025 Leitung Cybersecurity, bald im Ruhestand

Hobbies:
Basteln, Segeln, Dräxeln, Tennis, Tüfteln, Welt bereisen

AGENDA

Umsetzung der Anforderungen RED Art. 3.3

Risikobewertung

- Arbeiten in Gruppen

EN 18031-X

Security/Network Asset

- Arbeiten in Gruppen

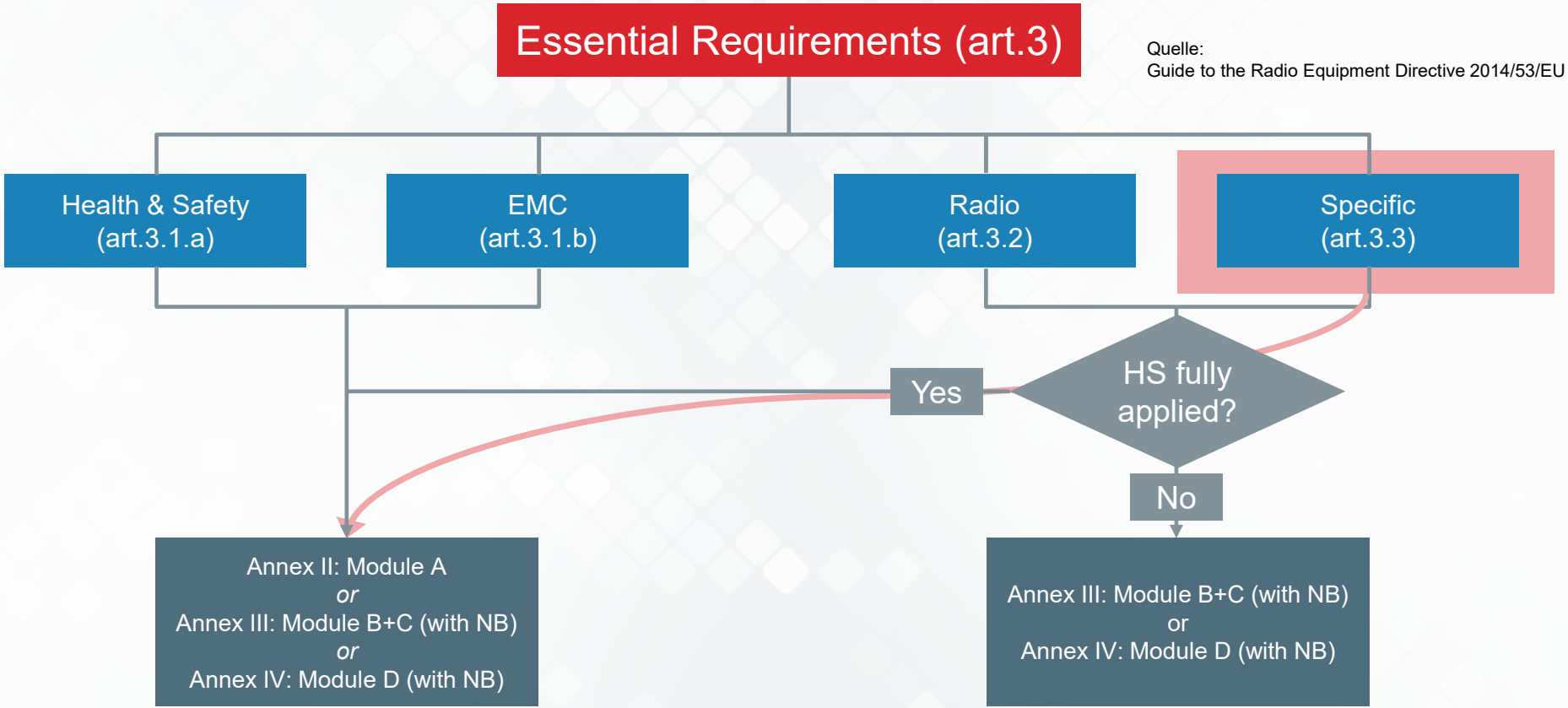
Applicability of access control mechanisms

- Arbeiten in Gruppen

Appropriate access Access control mechanism

Zusammenfassung

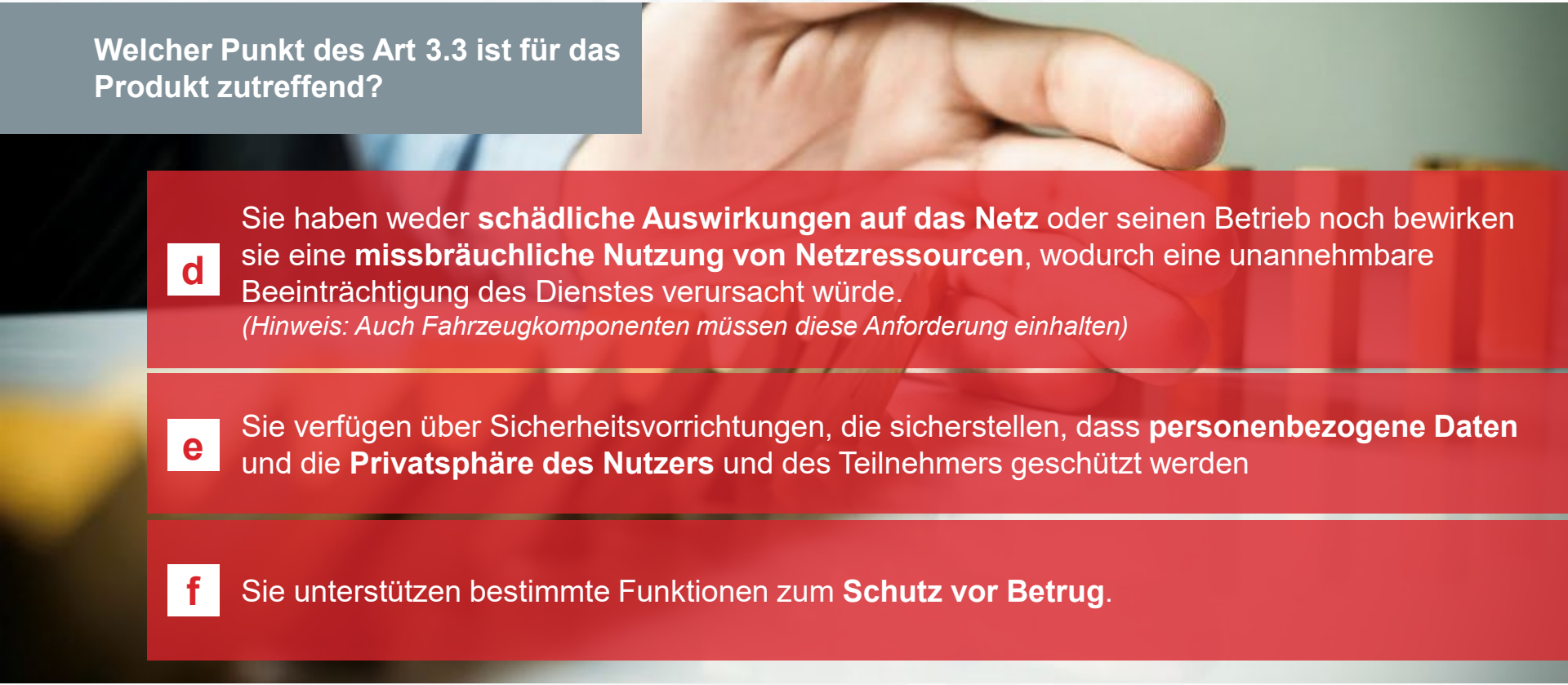
RED Grundlegende Anforderungen Konformitätsbewertung in Artikel 17



Quelle:
Guide to the Radio Equipment Directive 2014/53/EU

Erster Schritt Risikobewertung

Welcher Punkt des Art 3.3 ist für das Produkt zutreffend?

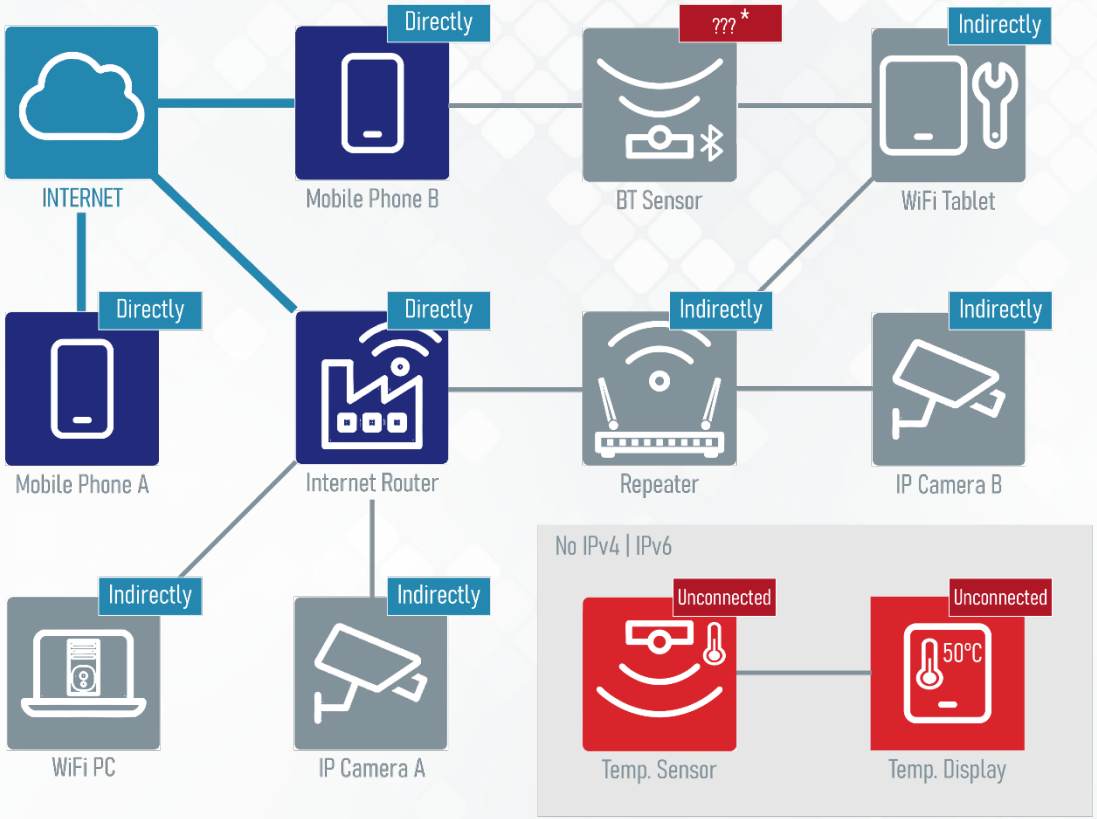


d Sie haben weder **schädliche Auswirkungen auf das Netz** oder seinen Betrieb noch bewirken sie eine **missbräuchliche Nutzung von Netzressourcen**, wodurch eine unannehmbare Beeinträchtigung des Dienstes verursacht würde.
(Hinweis: Auch Fahrzeugkomponenten müssen diese Anforderung einhalten)

e Sie verfügen über Sicherheitsvorrichtungen, die sicherstellen, dass **personenbezogene Daten** und die **Privatsphäre des Nutzers** und des Teilnehmers geschützt werden

f Sie unterstützen bestimmte Funktionen zum **Schutz vor Betrug**.

Direkt oder indirekt verbundene Geräte lt. RED DA



*depends on BT Version / Implementation

Beispiel 1
Fiktives Produkt Sprechfunk

Welcher Punkt des Art 3.3 ist für das Produkt zutreffend?

d **Auswirkungen** auf Netz / Betrieb? **Missbräuchliche Nutzung** von Netzressourcen?

e **Personenbezogene Daten** im Produkt vorhanden ?

f Betrug bezüglich Finanzdaten?

Beispiel 1
Fiktives Produkt Sprechfunk

Sprechfunkgerät **ohne Internetverbindung** und **personenbezogenen Daten** ist laut RED Art. 3.3 d,e,f **nicht zu berücksichtigen**.

In der Risikobewertung ist diese Bewertung zu dokumentieren.

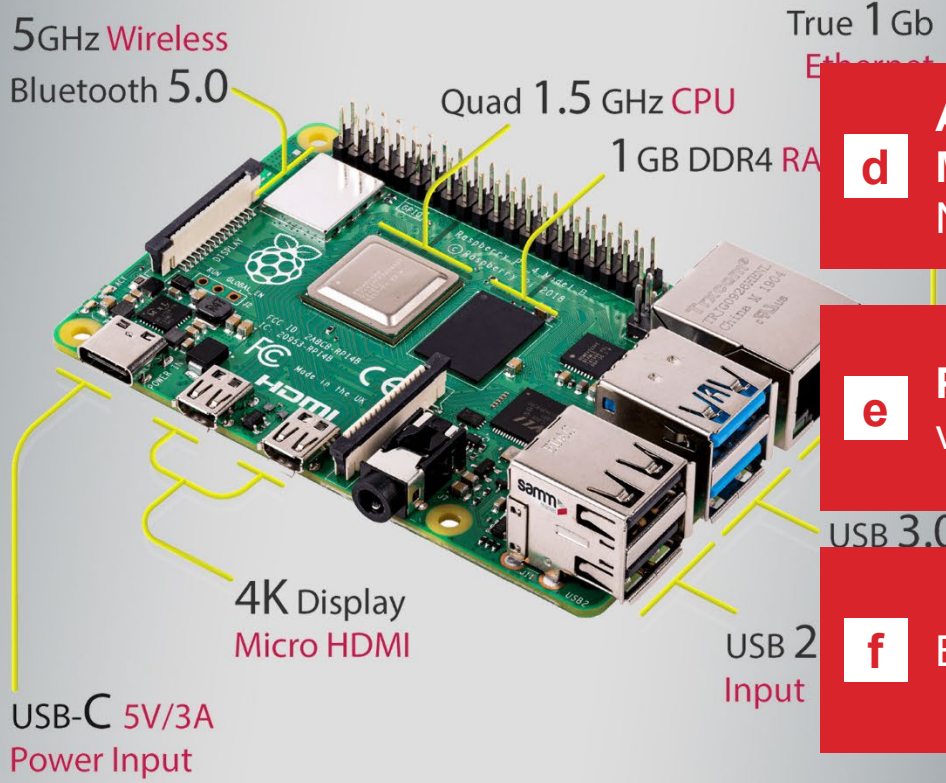
d **Auswirkungen** auf Netz / Betrieb? **Missbräuchliche Nutzung** von Netzressourcen? **Nein.**

e **Personenbezogene Daten** im Produkt vorhanden ? **Nein.**

f Betrug bezüglich Finanzdaten? **Nein.**

→ Insel-Lösung

Beispiel 2
Produkt Raspberry Pi

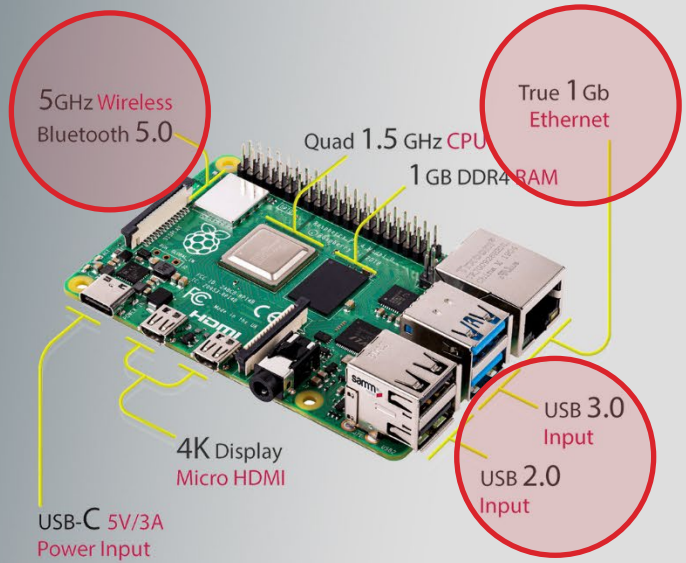


d **Auswirkungen** auf Netz / Betrieb? **Missbräuchliche Nutzung** von Netzressourcen?

e **Personenbezogene Daten** im Produkt vorhanden ?

f Betrug bezüglich Finanzdaten?

Beispiel 2
Produkt Raspberry Pi



Familienzulassung ist abhängig vom **Baumuster**.
Baumuster Anforderung für Familie: RED Art. 3.1a, 3.1.b, 3,2, 3.3 identisch

d **Auswirkungen** auf Netz / Betrieb?
Missbräuchliche Nutzung von Netzressourcen?

Auswirkung auf Netz möglich.
RED Art. 3.3 d ist zu berücksichtigen

e **Personenbezogene Daten** im Produkt vorhanden ?

RED Art. 3.3 e ist zu berücksichtigen, wenn die Anwendung die Speicherung von **personenbezogenen Daten** zulässt.

f Betrug bezüglich Finanzdaten?

RED Art. 3.3 f ist zu berücksichtigen, wenn die Anwendung die Speicherung von **Finanzdaten** erlaubt.

Beispiel Risikobewertung:
Essential Requirements for RED ART. 3.3 d,e,f || Not applicable

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 e) Radio equipment incorporates safeguards to ensure that the **personal data** and privacy of the user and of the subscriber are protected (f) Radio equipment supports certain features ensuring protection from **fraud**	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) **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) **Not applicable**: The DUT cannot pose a risk of fraud because it does not store or process financial data.	

Beispiel Risikobewertung:
Essential Requirements for RED Art 3.3 d,e,f || Applicable

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.	

Quintessenz Risikobewertung

Insel-Lösung möglich

Familienzulassungen sind abhängig vom Baumuster

RISIKOBEWERTUNG

Indirekte Verbindungen zum Netz berücksichtigen

Spricht das Gerät „Internettisch“?

AGENDA

Umsetzung der Anforderungen RED Art. 3.3

Risikobewertung

- Arbeiten in Gruppen

EN 18031-X

Security/Network Asset

- Arbeiten in Gruppen

Applicability of access control mechanisms

- Arbeiten in Gruppen

Appropriate access Access control mechanism

Zusammenfassung

Standard EN 18031-X

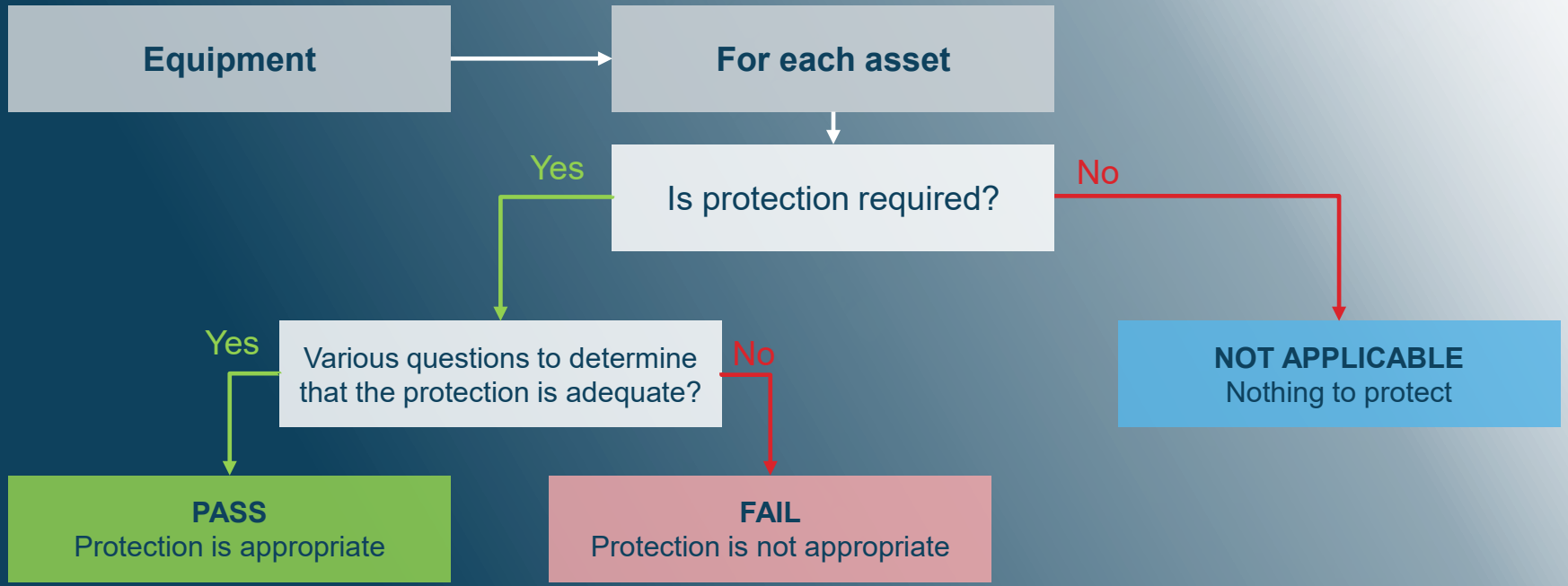
- Um sicherzustellen, dass die Anforderungen aufeinander abgestimmt werden können, wurden Assets als Hauptziele eingeführt, auf die die Anforderungen anzuwenden sind.

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	☒	☒	☑

Anforderungen der EN 18031-X

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	☑	☑	☑

Entscheidungsbäume / Decision Trees



Entscheidungsbäume helfen bei der Beurteilung der Anforderungen bezüglich:

- Anwendbarkeit und Angemessenheit

Die Entscheidungsbäume sind auf jede Security/Network Asset anzuwenden

- (Username, Password, PIN, Network configuration, WLAN Access.)

Kein Bestandteil der Bewertung sind:

- **funktionale Protokolltests**
- **Pen-Tests.**
- **multimediale** oder **hochgradig gezielte/ausgeklügelte Angriffe** und damit die invasive **Analyse von Hard- und Softwaremodulen**.

Die **Testszenarien (TSOs)** zielen auf einen **grundlegenden Aufwand** hinsichtlich **Testtiefe** und **Testumfang** gemäß **Basissicherheitsniveau** ab.