WÜRTH ELEKTRONIK
MORE THAN YOU EXPECT

PHOENIX TESTLAB

Bundesnetzagentur

WEBINAR:

5VOR12
IN DER CYBERSICHERHEIT

VON RED BIS CRA

INFORMATIONEN UND DISKUSSION

WEBINAR:

5VOR12
IN DER CYBERSICHERHEIT

VON RED BIS CRA

INFORMATIONEN UND DISKUSSION

1. **Einführung**
   Holger Bentje, Phoenix Testlab
   Hintergrund, Entstehung und Relevanz von RED-DA und CRA

2. **Konformitäts- und Risikobewertung**
   Dietmar Frei, Phoenix Testlab
   Was ist gefordert? Wo bestehen Unsicherheiten?

3. **Bewertbarkeit aus Sicht der Marktüberwachung**
   Jonas Bünnemann, Bundesnetzagentur
   Einschätzung der Bundesnetzagentur, Umgang mit Bestandssystemen

4. **Umsetzung in der Praxis**
   Adithya Madanahalli, Würth Elektronik
   Wie Funkmodule helfen können, Anforderungen effizient zu erfüllen

5. **Offene Fragerunde und Diskussion**
   Moderation: Michael Lang, Würth Elektronik
   Ihre Fragen, unsere Antworten – moderiert und interaktiv

Willkommen

5 vor 12
in der Cybersecurity
Einführung

Holger Bentje / Operations / 30 Juli 2025

Referent

Holger Bentje

Master Specialist EMC & Radio Technologies
Director Notified Body RED & TCB USA, Canada, Japan

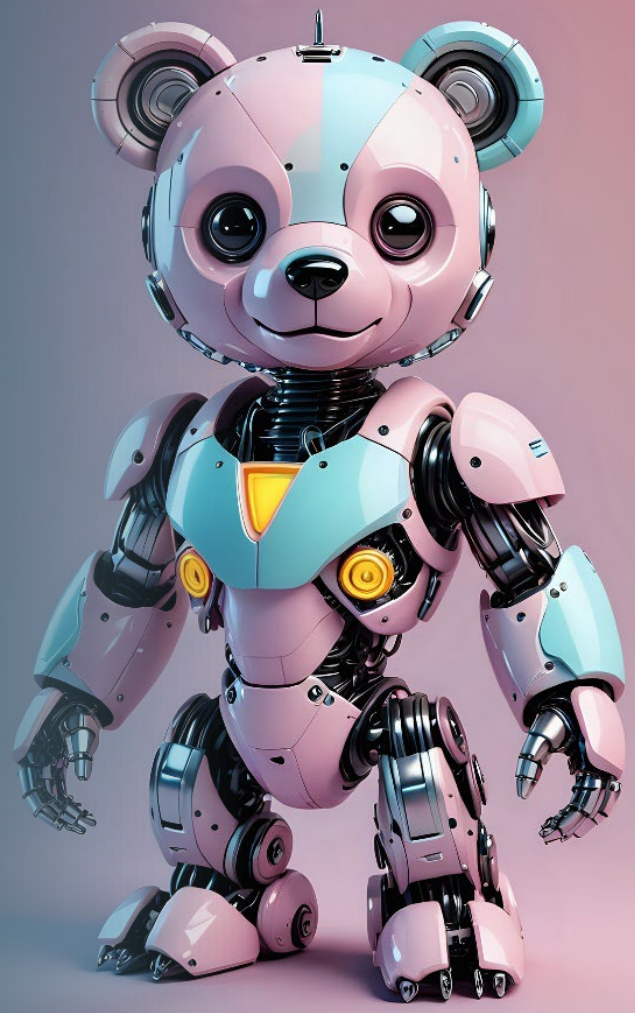
- +49-5235-9500-24
- bentje.holger@phoenix-testlab.de

Das Problem

Im Dezember 2016 führte der Norwegian Consumer Council eine eingehende Analyse mehrerer mit dem Internet verbundener Spielzeuge (Smart Toys) durch.

- Die Ergebnisse deuten auf einen möglichen Mangel beim Schutz der Rechte von Kindern auf Privatsphäre und Sicherheit hin.
- Dank integrierter Lautsprecher, Mikrofone und anderer Sensoren sind vernetzte Spielzeuge "intelligent" und können beispielsweise Sprache interpretieren, was sie in die Lage versetzt, mit dem Kind zu interagieren.
- Außerdem können sie nicht nur Fotos, Videos, Geolokalisierungsdaten und Daten im Zusammenhang mit dem Spielerlebnis aufzeichnen, sondern auch Herzfrequenz, Schlafgewohnheiten oder andere biometrische Daten.
- Sie können auch mit Telefonen und Tablets oder direkt mit dem Internet verbunden werden.

Die Fähigkeit dieser Produkte, Informationen aufzuzeichnen, zu speichern und weiterzugeben, gab Anlass zu Bedenken in Bezug auf ihre Sicherheit und den Schutz der Privatsphäre.



Source: EC Impact Assessment Report.pdf

Regulatorische Initiative

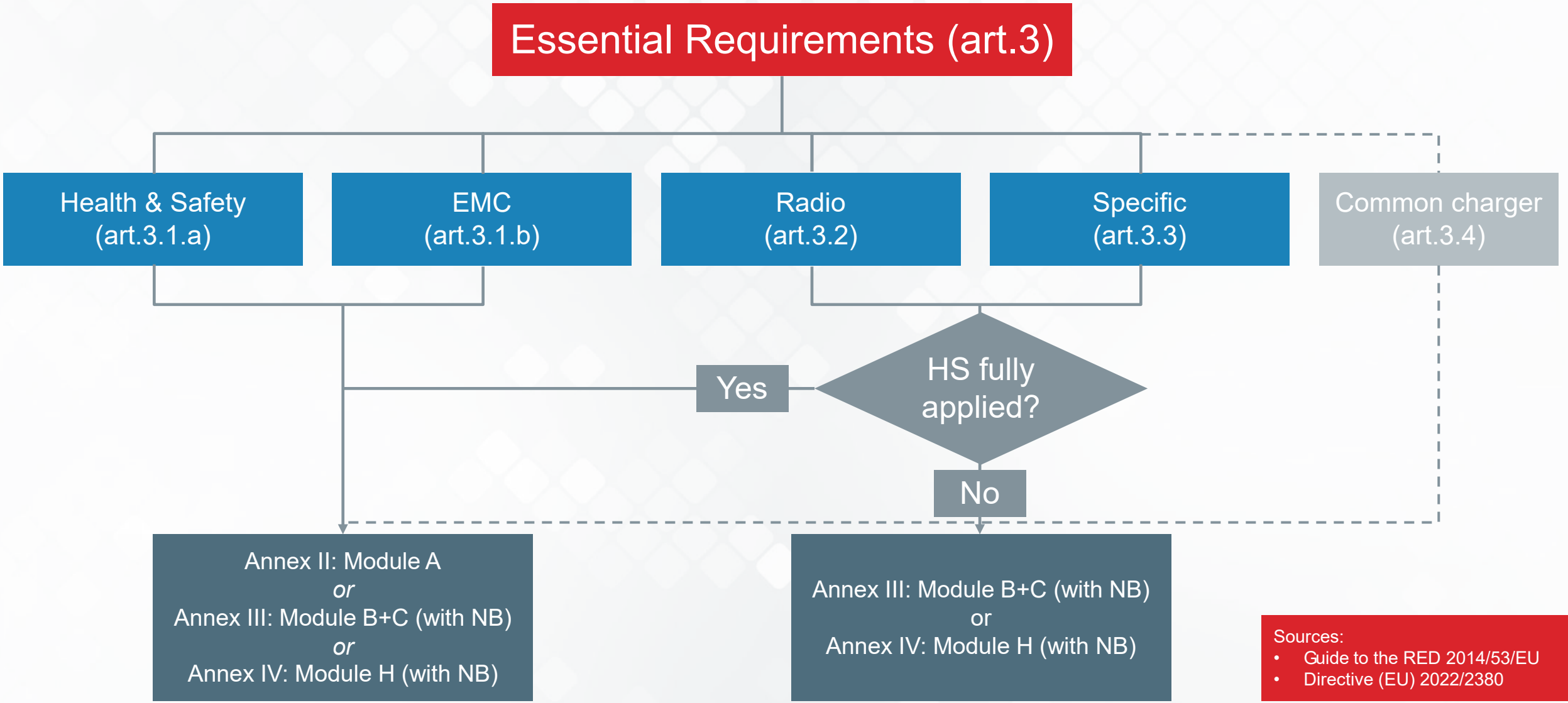
Am 7. Februar 2018 wurde von der Europäischen Kommission eine Sondersitzung des "Telecommunication Conformity Assessment and Market Surveillance Committee" (TCAM) organisiert, um die Möglichkeit der Nutzung des Artikel 3(3) der Funkanlagenrichtlinie (RED) zu prüfen.

Source: EC Impact Assessment Report.pdf

Funkanlagenrichtlinie (RED)

- Die Funkanlagenrichtlinie 2014/53/EU ("RED") legt einen Rechtsrahmen für das Inverkehrbringen von Funkanlagen auf dem europäischen Binnenmarkt fest.
- Sie definiert verbindliche Marktzugangsbedingungen für Produkte und ermöglicht es den Mitgliedstaaten, Korrekturmaßnahmen für nicht konforme Geräte zu ergreifen.
- Bei der RED handelt es sich um eine Gesetzgebung nach dem neuen Konzept, bei der nur “wesentliche Anforderungen” (essential requirements) festgelegt werden. Die Hersteller müssen nachweisen, dass die technischen Lösungen in ihren Produkten mit dem Gesetz übereinstimmen.
- Alle mit dem Internet verbundenen Funkanlagen, einschließlich IoT-Produkte mit Funkschnittstellen und Wearables, wie z. B. Smart Watches, fallen in den Anwendungsbereich dieser Richtlinie.

RED-Aspekte = Essential Requirements = Risiken!



Sources:
- Guide to the RED 2014/53/EU
- Directive (EU) 2022/2380

Die Lösung

- Bestimmte optionale Anforderungen der RED könnten über delegierte Rechtsakte zur Anwendung gebracht werden.
- Die RED hat das Potenzial, das gewünschte grundlegende Sicherheitsniveau zu erreichen.
  - Schnell: es muss keine neue Verordnung erlassen werden
  - Effektiv: unsichere Geräte werden durch Marktdurchsetzung vom europäischen Markt verbannt
  - Angemessen: Selbsteinschätzung der Basisanforderungen durch den Hersteller möglich
- Jeder delegierte Rechtsakt nach Artikel 3(3) wird die entsprechenden grundlegenden Anforderungen für bestimmte Kategorien von Funkanlagen anwendbar machen.
- Nur für Funkanlagen, die nach dem 1. August 2025 in Verkehr gebracht werden, gelten die neuen grundlegenden Anforderungen.
- Die Delegierte Verordnung (EU) 2022/30 (RED DA) legt die grundlegenden Anforderungen der RED fest.

Funkanlagenrichtlinie und Cybersecurity

Obwohl die RED das Wort "Cybersecurity" nicht erwähnt, beziehen sich einige ihrer grundlegenden Anforderungen in Artikel 3 (3) auf Elemente der Cybersicherheit, wie z. B.

Artikel 3.3 (d)
Schutz des Netzes

Artikel 3.3 (e)
Schutz der Privatsphäre und personenbezogener Daten

Artikel 3.3 (f)
Schutz vor Betrug

Der nächste Schritt: CRA

- Die Cybersicherheitspolitik der EU wird schrittweise umgesetzt.
- In einem ersten Schritt werden Hersteller ihre Produkte an die Delegierte Verordnung zur RED und anschließend an den Cyber Resilience Act (CRA) anpassen.
- Die harmonisierten Normen zur Unterstützung der delegierten Verordnung werden weiterentwickelt und um CRA-Anforderungen ergänzt.
- Das Cybersicherheitsniveau von Produkten in der EU wird schrittweise verbessert werden.
- Der Cyber Resilience Act wird die Weiterentwicklung des delegierten Rechtsakts zur RED sein.
  - Anwendungsbereich: Alle digitalen Produkte, einschließlich Hardware und Software, nicht beschränkt auf Funkanlagen.
  - Lebenszyklus im Fokus: Gilt für den gesamten Lebenszyklus des Produkts und nicht nur für das erste Inverkehrbringen.
- Der CRA wurde im Amtsblatt der EU als Verordnung (EU) 2024/2847 veröffentlicht.
  - Veröffentlicht am 20.11.2024
  - In-Kraft-Treten am 10.12.2024
  - Meldepflichten ab 11.09.2026
  - Inkrafttreten ab 11.12.2027

DANKE

5 vor 12
in der Cybersecurity

5 vor 12
in der Cybersecurity

Alle Inhalte in dieser Präsentation, insbesondere Texte, Fotografien und Grafiken sind urheberrechtlich geschützt und alle in dieser Präsentation enthaltenen Strategien, Modelle, Konzepte und Schlussfolgerungen sind ebenfalls geistiges Eigentum von Phoenix Testlab, sofern dies nicht anders, zum Beispiel durch Quellenangaben, gekennzeichnet ist.
Alle in dieser Präsentation enthaltenen Informationen sind vertraulich zu behandeln. Es ist ohne vorherige schriftliche Genehmigung durch Phoenix Testlab untersagt, diese Präsentation ganz oder auszugsweise zu kopieren, zu verändern, zu vervielfältigen, zu veröffentlichen, zu verbreiten oder in einer sonstigen Weise Dritten zugänglich zu machen.

All contents in this presentation, in particular texts, photographs and graphics, are protected by copyright and all strategies, models, concepts and conclusions contained in this presentation are also the intellectual property of Phoenix Testlab, unless otherwise indicated, for example by references.
All information contained in this presentation is to be treated as confidential. It is prohibited to copy, modify, reproduce, publish, distribute or make this presentation available to third parties in any other way, either in whole or in part, without the prior written permission of Phoenix Testlab.

WÜRTH ELEKTRONIK MORE THAN YOU EXPECT

PHOENIX TESTLAB

Bundesnetzagentur

WEBINAR:

5VOR12
IN DER CYBERSICHERHEIT

VON RED BIS CRA

INFORMATIONEN UND DISKUSSION

1. **Einführung**
   Holger Bentje, Phoenix Testlab
   Hintergrund, Entstehung und Relevanz von RED-DA und CRA

2. **Konformitäts- und Risikobewertung**
   Dietmar Frei, Phoenix Testlab
   Was ist gefordert? Wo bestehen Unsicherheiten?

3. **Bewertbarkeit aus Sicht der Marktüberwachung**
   Jonas Bünnemann, Bundesnetzagentur
   Einschätzung der Bundesnetzagentur, Umgang mit Bestandssystemen

4. **Umsetzung in der Praxis**
   Adithya Madanahalli, Würth Elektronik
   Wie Funkmodule helfen können, Anforderungen effizient zu erfüllen

5. **Offene Fragerunde und Diskussion**
   Moderation: Michael Lang, Würth Elektronik
   Ihre Fragen, unsere Antworten – moderiert und interaktiv

Willkommen

5vor12 in der Cybersicherheit

Dietmar Frei , Juli.2025

Your speaker

Dietmar Frei

Management
Cybersecurity

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

Frohmensch, lateral thinker, tinkerer, technology enthusiast and Head of Customer Communications at Phoenix Testlab for many years.
Head of Cybersecurity since 2025, soon to retire

Hobbies:
Handicrafts, sailing, playing tennis, tinkering, traveling the world

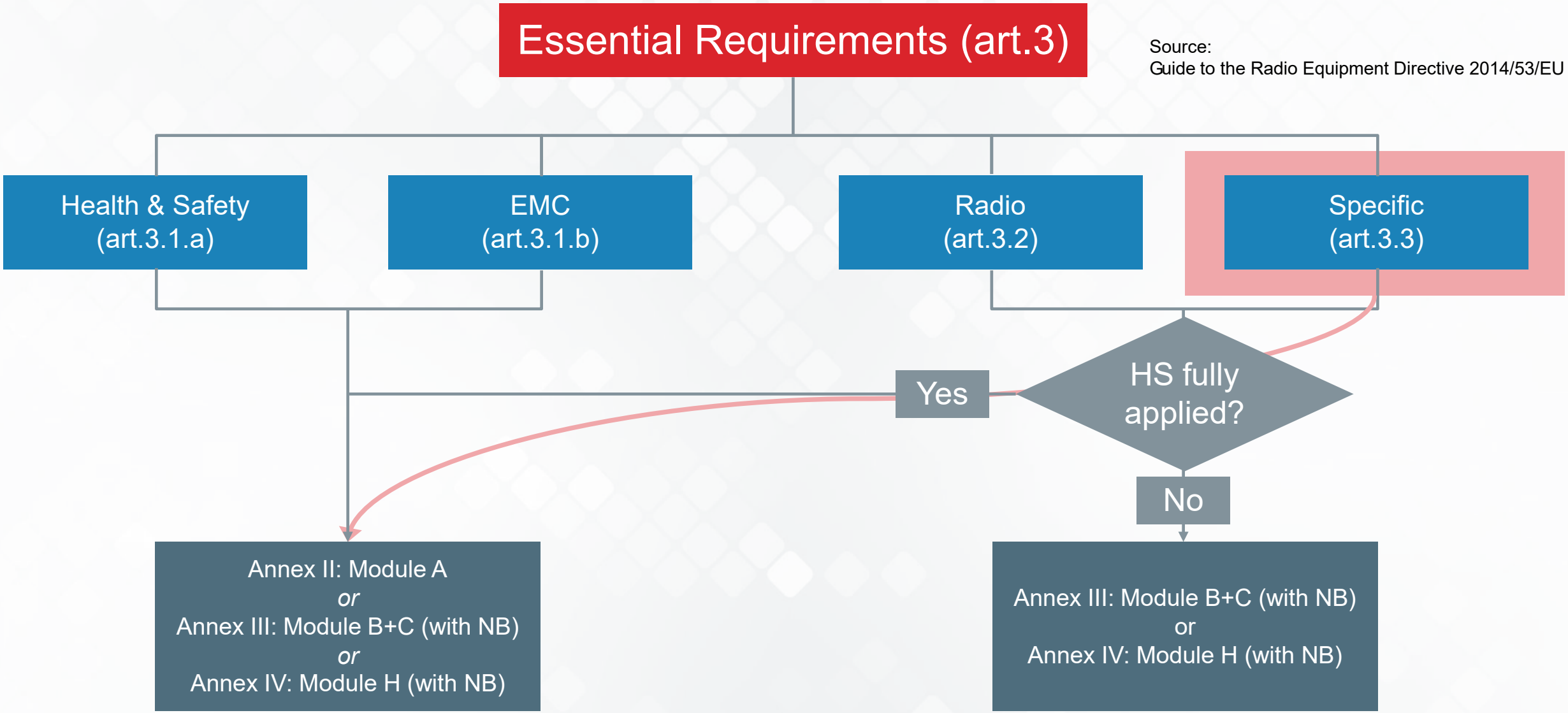
AGENDA

Implementation of the RED requirements Art. 3.3
- Risk Assessment
- Decleration of Conformity

EN 18031-X
- Security/Network Asset Requirements

Summary

RED Essential requirements Conformity assessment in item 17



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

First step risk assessment

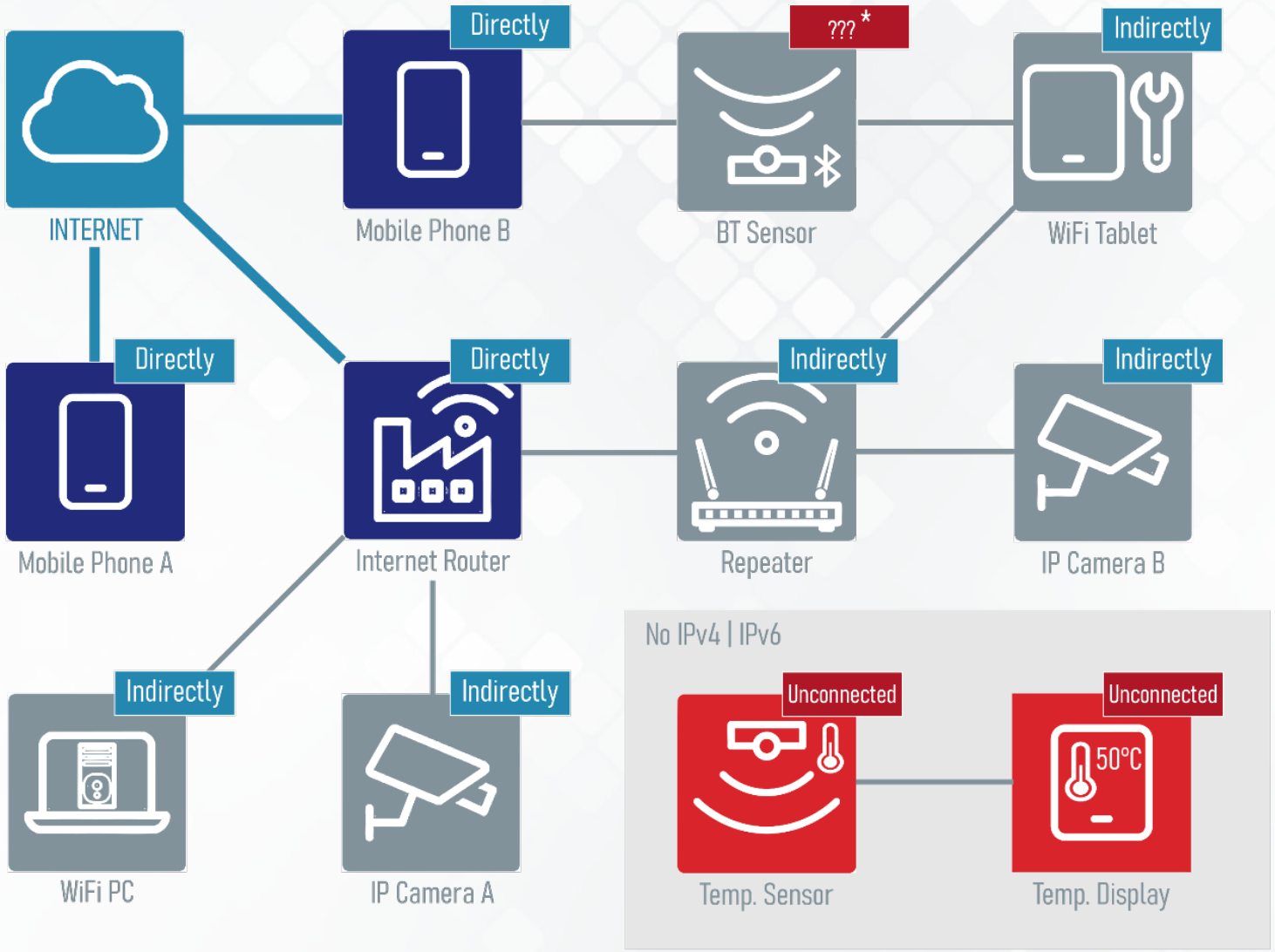
Which point of Art 3.3 is applicable to the product?

d They do not have **a harmful effect on the network** or its operation, nor do they cause **misuse of network resources**, which would cause an unacceptable degradation of service.
(Note: vehicle components must also comply with this requirement)

e They have security measures in place to ensure that **personal data** and the **privacy of the user** and subscriber are contactor protected

f They support certain **fraud protection** functions.

Directly or indirectly connected devices according to RED DA



*depends on BT Version / Implementation

© Feb 2025, Phoenix Testlab GmbH

Example risk assessment:
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.	

Example risk assessment:
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.	

Declaration of Conformity

- Parts of the Document
  - Radio equipment/product/model no/brand name ….
  - Name and address of manufacturer
  - Type of Product
  - Which declaration is involved, fulfills the requirements
  - Compliance verfied by
    - …..
    -EN18031-1, EN18031-2, EN18031-3 Aug. 2024
  - Notified body
  - Description of accessories and components, including software which allow the radio equipment to operate
  - Additional information

  - Date and Signature

Standard EN 18031-X

- To ensure that the requirements can be harmonized, assets have been introduced as the main targets to which the requirements are to be applied.

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	☒	☒	☑

Requirements of EN 18031-X

Abbreviation	Mechanism	EN 18031-1	EN 18031-2	EN 18031-3
ACM	Access control mechanism	☑	☑	☑
AUM	Mechanism for authentication	☑	☑	☑
SUM	Secure update mechanism	☑	☑	☑
SSM	Secure storage mechanism	☑	☑	☑
SCM	Mechanism for secure communication	☑	☑	☑
RLM	Fail-safe mechanism	☑	☒	☒
LGM	Mechanism for logging	☒	☑	☑
NMM	Network monitoring mechanism	☑	☒	☒
DLM	Mechanism for deleting data	☒	☑	☒
TCM	Traffic control mechanism	☑	☒	☒
UNM	Mechanism for notifying users	☒	☑	☒
CCK	Confidential cryptographic keys	☑	☑	☑
GEC	General equipment features	☑	☑	☑
CRY	Cryptography	☑	☑	☑

AGENDA

Implementation of the RED requirements Art. 3.3
- Risk Assessment
- Decleration of Conformity

EN 18031-X
- Security/Network Asset Requirements

Summary

Summary

- Risk Assessment
- Declaration of Conformity including EN18031-x
- Using EN18031-x Standards

WÜRTH ELEKTRONIK MORE THAN YOU EXPECT

PHOENIX TESTLAB

Bundesnetzagentur

WEBINAR:

5VOR12
IN DER CYBERSICHERHEIT

VON RED BIS CRA

INFORMATIONEN UND DISKUSSION

1. **Einführung**
   Holger Bentje, Phoenix Testlab
   Hintergrund, Entstehung und Relevanz von RED-DA und CRA

2. **Konformitäts- und Risikobewertung**
   Dietmar Frei, Phoenix Testlab
   Was ist gefordert? Wo bestehen Unsicherheiten?

3. **Bewertbarkeit aus Sicht der Marktüberwachung**
   Jonas Bünnemann, Bundesnetzagentur
   Einschätzung der Bundesnetzagentur, Umgang mit Bestandssystemen

4. **Umsetzung in der Praxis**
   Adithya Madanahalli, Würth Elektronik
   Wie Funkmodule helfen können, Anforderungen effizient zu erfüllen

5. **Offene Fragerunde und Diskussion**
   Moderation: Michael Lang, Würth Elektronik
   Ihre Fragen, unsere Antworten – moderiert und interaktiv

Bundesnetzagentur

Cybersicherheit

Bestandsregelung und Risikobewertung

Jonas Bünnemann
Referat 411 Marktüberwachung nach EMVG und FuAG

Themen

- Bestandsregelung
  - Importe von außerhalb des EWR
  - Funkanlagen hergestellt im EWR

- Risikobewertung

Bestandsregelung

Innerhalb und außerhalb des EWR

Importe von außerhalb des EWR

- Entscheidend ist der Zeitpunkt des ersten Inverkehrbringens
  - Importe → Einfuhrdatum (Abschluss des Zollverfahrens)
  - Produktionsdatum uninteressant

- Abschluss des Zollverfahrens ohne Konformität nach Cybersicherheitsaspekten nach dem 01.08.2025 ?
  - Funkanlage zum freien Warenverkehr angemeldet und freigegeben
  - JA: Funkanlage erstmalig in Verkehr gebracht („bereitgestellt“)
    - Unerheblich zu welchem Zeitpunkt die Funkanlagen verkauft werden
  - NEIN: Kein Import der Funkanlagen nach dem 01.08.2025

Funkanlagen hergestellt im EWR

- Entscheidend ist Zeitpunkt des ersten Inverkehrbringens
  - Funkanlage bereits im Verkaufslager?
  - Produktionsdatum als Indiz

- Wann darf die Funkanlage in das Verkaufslager?
  - Abgeschlossenes und bestandenes Konformitätsbewertungsverfahren

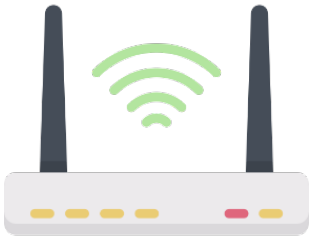
- Nach **01.08.2025**:
  - Neues Konformitätsbewertungsverfahren nötig
  - Weiter produzierte Anlagen ohne Anpassung nicht mehr vertriebsfähig

Risikobewertung

Risikobewertung

- Orientierung an Risikobewertung der EU zur Produktsicherheit

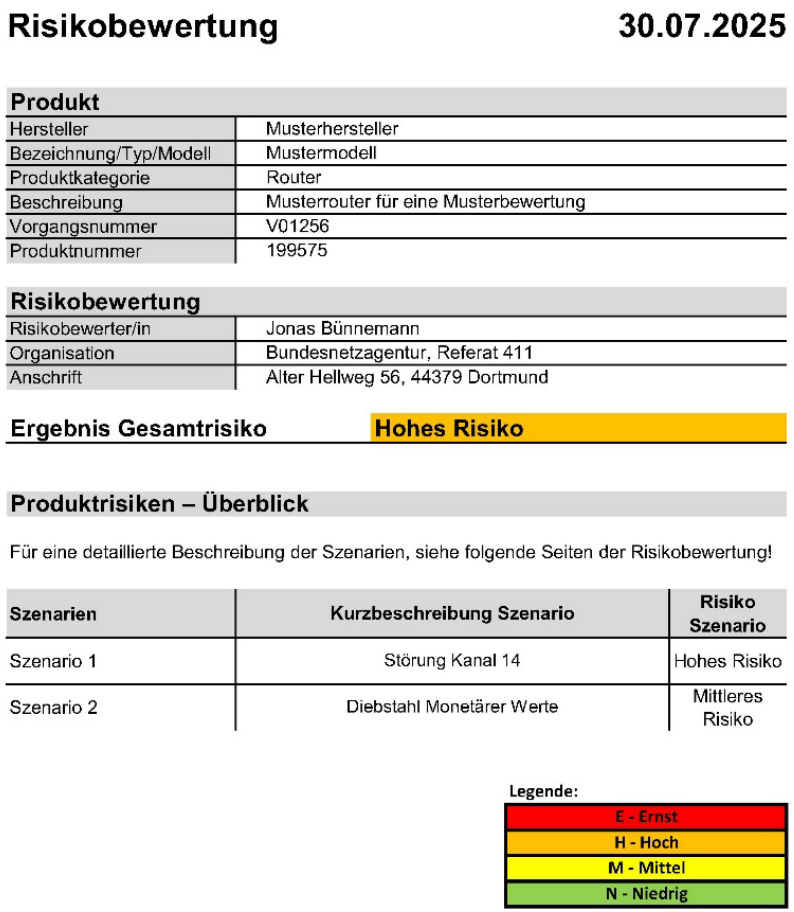
- Folgende Bewertung als Beispiel
  - Layout entspricht zukünftigen Bewertungsbögen der BNetzA
  - Inhalte nur beispielhaft, ohne Anspruch auf Richtigkeit



Risikobewertung

- Verschiedene Szenarien pro Bewertung möglich
  - Max. fünf Schritte pro Szenario

- Ermittlung des Einzel- und Gesamtrisikos
  - Einzelrisiko pro Szenario
  - Gesamtrisiko = höchstes Einzelrisiko



Risikobewertung **30.07.2025**

Produkt	
Hersteller	Musterhersteller
Bezeichnung/Typ/Modell	Mustermodell
Produktkategorie	Router
Beschreibung	Musterrouter für eine Musterbewertung
Vorgangsnummer	V01256
Produktnummer	199575

Risikobewertung	
Risikobewerter/in	Jonas Bünnemann
Organisation	Bundesnetzagentur, Referat 411
Anschrift	Alter Hellweg 56, 44379 Dortmund

Ergebnis Gesamtrisiko **Hohes Risiko**

Produktrisiken – Überblick

Für eine detaillierte Beschreibung der Szenarien, siehe folgende Seiten der Risikobewertung!

Szenarien	Kurzbeschreibung Szenario	Risiko Szenario
Szenario 1	Störung Kanal 14	Hohes Risiko
Szenario 2	Diebstahl Monetärer Werte	Mittleres Risiko

Legende:

E - Ernst
H - Hoch
M - Mittel
N - Niedrig

Risikobewertung - Beispielszenario

- Produktgefahr
  - Beschreibung der Gefahrenparameter
- Verbraucher
  - Beschreibung der betroffenen Nutzer
- Schweregrad
  - Schwere des Schadens
- Wahrscheinlichkeit der Schritte zum Risiko
  - Beschreibung des Szenarios

Risikobewertung **30.07.2025**

Szenario 1	Störung Kanal 14		Hohes Risiko
	1. Produktgefahr		
	Gefahrenart	Zugriff auf Netwerk	
	Schadensart	Beeinträchtigung des Netzes	
	2. Verbraucher		
	Nutzergruppe	Kinder	
	Beschreibung	Kinder zwischen 8 und 14 Jahren (Gefährdete Verbraucher)	
	3. Schweregrad		
	Schweregrad	3	
	4. Wahrscheinlichkeit der Schritte zur Verletzung		
Schritt/e	Beschreibung, wie der Schritt zum angegebenen Schaden führt		Wahrschein-lichkeit
Schritt 1	Zugriff auf Netzwerk via Standardpasswort des Routers		0,05
Schritt 2	Wahl eines in Deutschland unzulässigen Kommunikationskanals (WLAN Kanal 14)		0,08
Schritt 3	Störung medizinischer Geräte im Kinderkrankenhaus		0,05

Gesamtwahrscheinlichkeit Szenario	0,0002000
Risikostufe	Hoch

Kontakt

Jonas Bünnemann
Referat 411
marktueberwachung@BNetzA.de

Bundesnetzagentur

WÜRTH ELEKTRONIK MORE THAN YOU EXPECT

PHOENIX TESTLAB

Bundesnetzagentur

WEBINAR:

5VOR12
IN DER CYBERSICHERHEIT

VON RED BIS CRA

INFORMATIONEN UND DISKUSSION

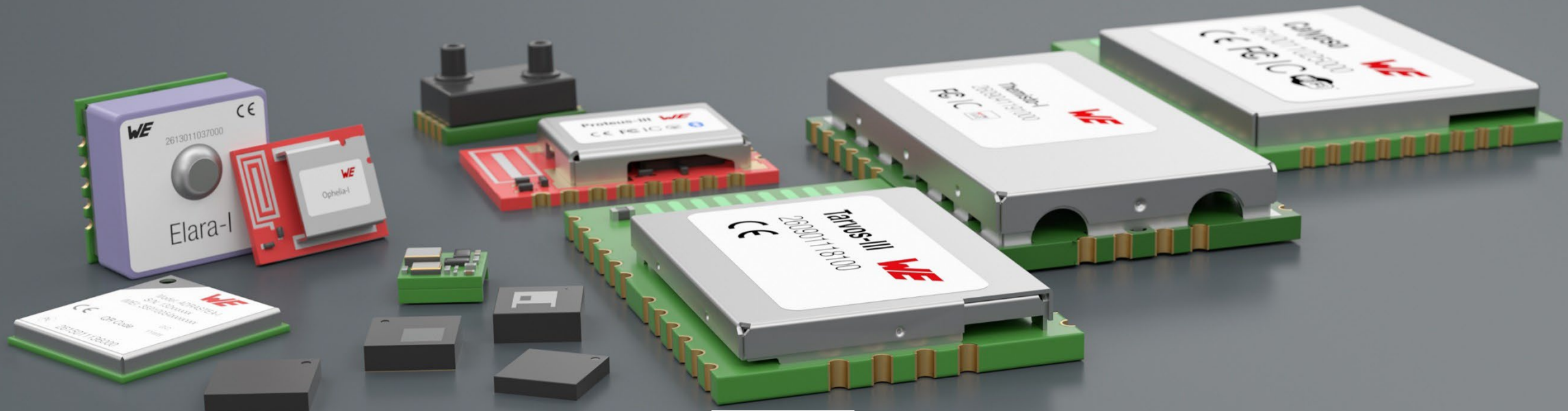
1. **Einführung**
   Holger Bentje, Phoenix Testlab
   Hintergrund, Entstehung und Relevanz von RED-DA und CRA

2. **Konformitäts- und Risikobewertung**
   Dietmar Frei, Phoenix Testlab
   Was ist gefordert? Wo bestehen Unsicherheiten?

3. **Bewertbarkeit aus Sicht der Marktüberwachung**
   Jonas Bünnemann, Bundesnetzagentur
   Einschätzung der Bundesnetzagentur, Umgang mit Bestandssystemen

4. **Umsetzung in der Praxis**
   Adithya Madanahalli, Würth Elektronik
   Wie Funkmodule helfen können, Anforderungen effizient zu erfüllen

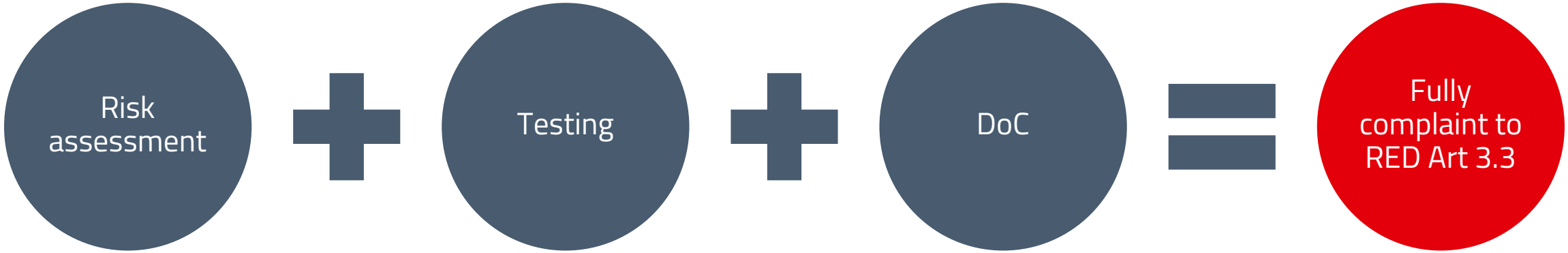
5. **Offene Fragerunde und Diskussion**
   Moderation: Michael Lang, Würth Elektronik
   Ihre Fragen, unsere Antworten – moderiert und interaktiv



Practical tips to RED-DA conformity

Adithya Madanahalli

YOUR CYBERSECURITY COMPLIANCE JOURNEY



CYBERSECURITY RISK ASSESSMENT

CYBER SECURITY RISK ASSESSMENT

- **Asset : What do we need to protect?**
  - Device ID
  - Firmware
  - Credentials (passwords, certificates etc.)
  - Biometric data
- **Threats : What are we protecting against?**
  - Remote attackers : Software, Network
  - Local/physical attackers: Software, Network, Hardware
  - Device specific attackers: Device theft, Battery compromise
  - Other attackers: Insider attack, Advanced hardware attack
- **Objective : What do we want to achieve?**
  - Authenticity
  - Integrity
  - Privacy
  - Confidentiality
- **Mechanism : How do we achieve it?**
  - 2-factor authentication
  - Data encryption
  - Secure firmware updates
  - Signature verification
  - Data input checks

CYBERSECURITY RISK ASSESSMENT

What is being protected?

What are we protecting against?

What do we want to achieve?

What is required to achieve it ?

Asset	Threat	Security objective	Security mechanism
Cloud credentials	Remote software attacks	Authenticity	Secure storage
Firmware	Remote software attacks	Integrity	Secure firmware update
Wireless link	Remote network attacks	Authenticity & Integrity	Data encryption

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

EN18031

Terms used in the standards

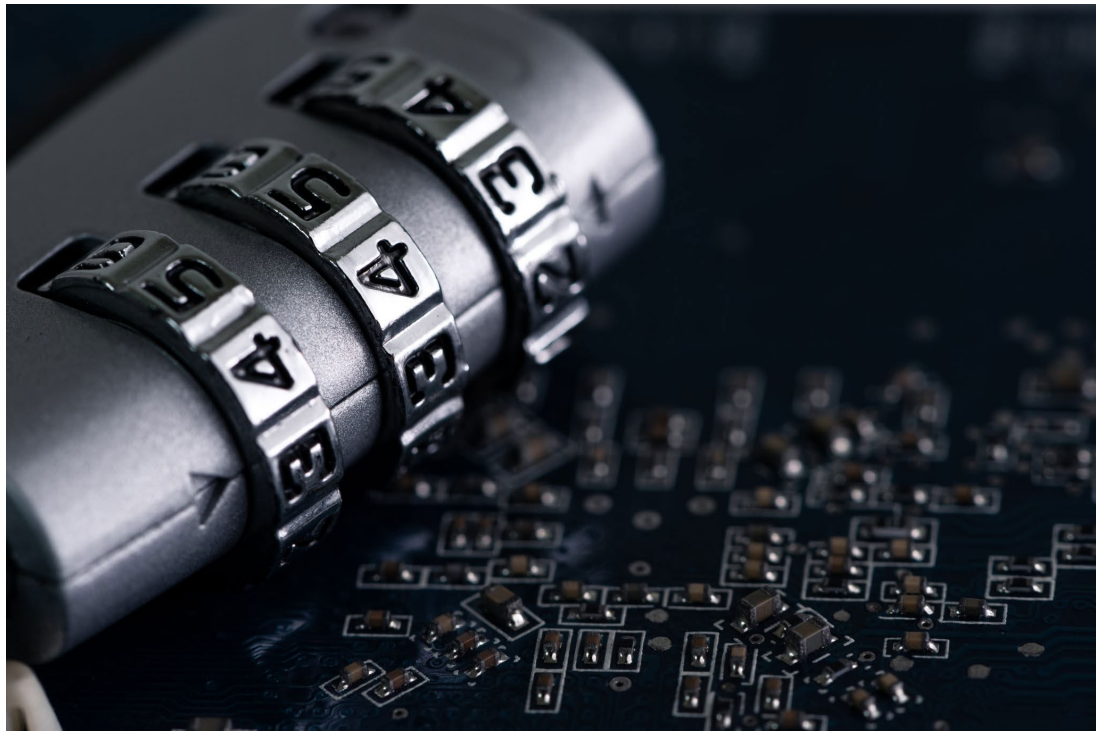
- “Assets” can be of the following types:

Requirement	3.3.d	3.3.e	3.3.f
Security asset	X	X	X
Network asset	X		
Privacy asset		X	
Financial asset			X

- “Mechanism” – Methods that can be used to apply security measures
- “Entities” – User, software, network peer …

WHAT ARE NETWORK ASSETS?

- Definition as per standard
  - Network functions
  - Network function configuration
- Classification
  - Confidential: Disclosure can harm the network.
  - Sensitive: Manipulation can harm the network.
- Examples of Network Functions
  - Protocol Implementations (e.g., TCP/IP stack, BlueZ)
  - Client Applications (e.g., DNS client, update services)
  - Server Applications/Daemons (e.g., FTP server, MQTT broker)
- Example of Network function configuration
  - /etc/dhcp/dhcpclient.conf (DHCP client)
- How to identify network assets?
  - Manually
  - Automated tools – for example EMBA, FACT



WHAT ARE SECURITY ASSETS?

- Definition as per standard
  - Security functions
  - Security function configuration
- Classification
  - Confidential: Disclosure can harm the network.
  - Sensitive: Manipulation can harm the network.
- Examples of Security Functions
  - Cryptographic libraries (e.g., Mbed TLS, OpenSSL)
  - SSH/VPN clients and servers
  - Firewalls
- Example of Security function parameters
  - Sensitive: Public keys, certificates, config files
  - Confidential & Sensitive: Passwords, private keys, tokens
- How to identify network assets?
  - Manually
  - Automated tools – for example EMBA, FACT

WHAT ARE PRIVACY ASSETS?

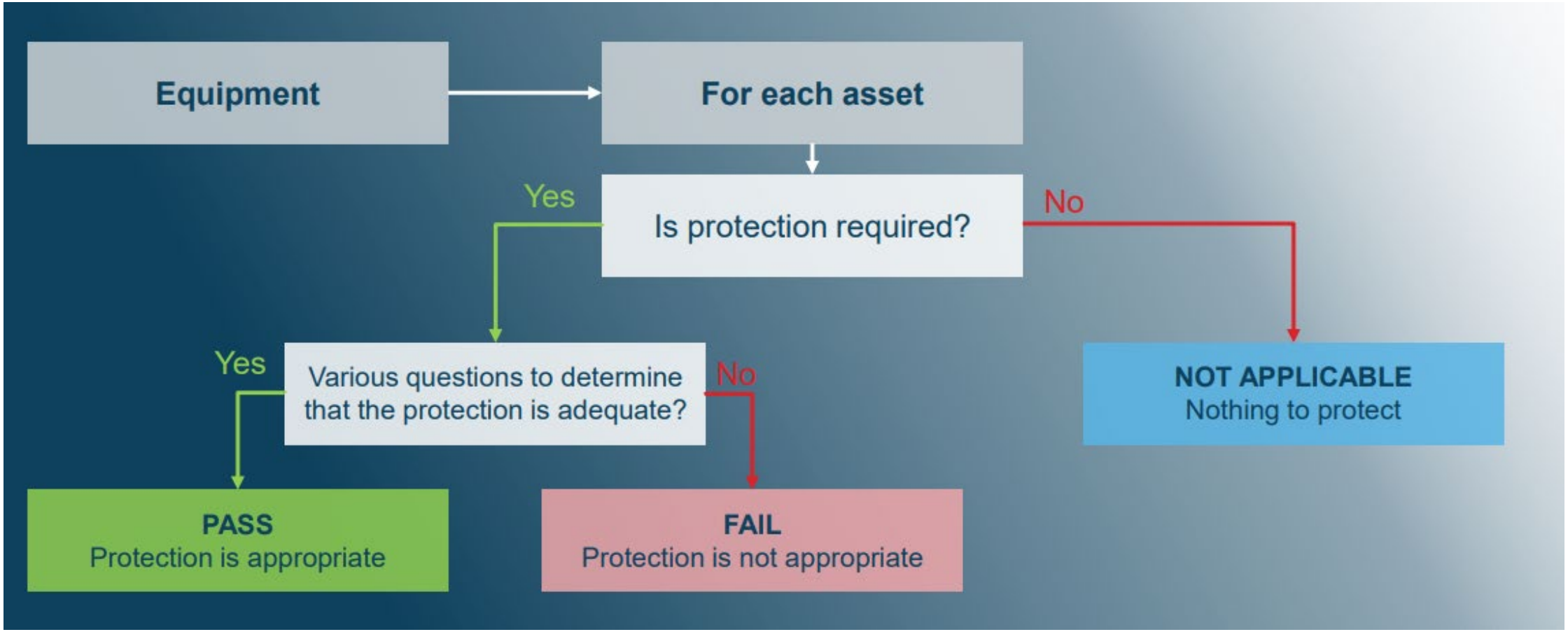
- Definition as per standard
  - Personal information
  - Traffic data
  - Location data

- Examples
  - Name, Email, Address, IP address, GPS location
  - Time stamped location data
  - Log data
  - Biometric data

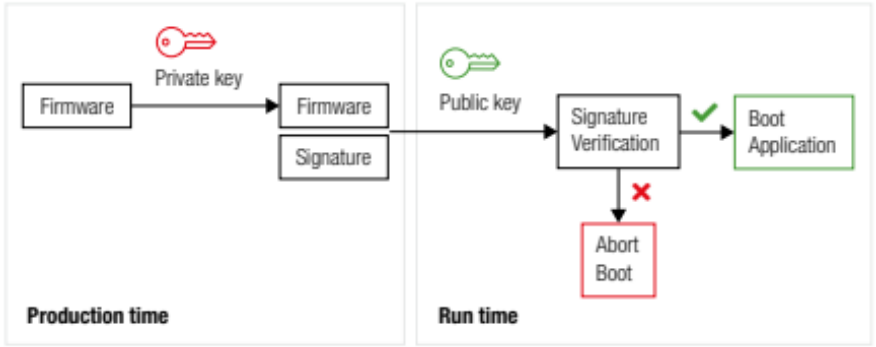
- Operations on personal data
  - Collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

- How to identify network assets?
  - Manually
  - Automated tools – for example bearer

DECISION TREES

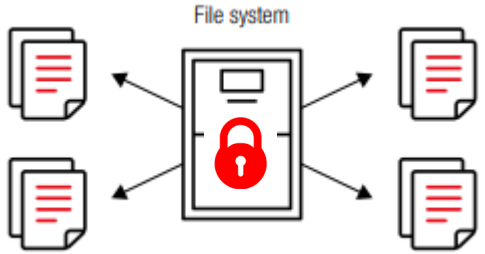


COMMON MINIMUM-SECURITY REQUIREMENTS

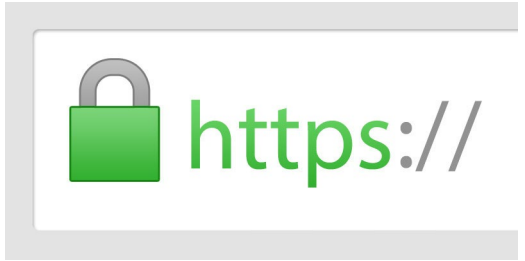


Secure production

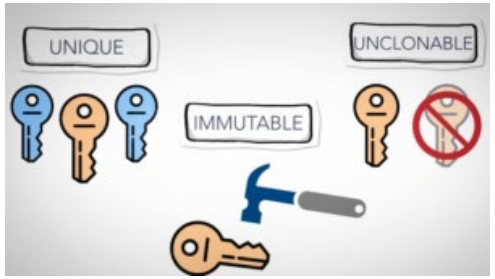
Secure boot



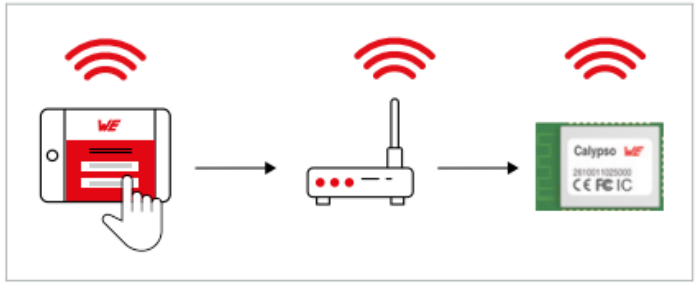
Secure storage



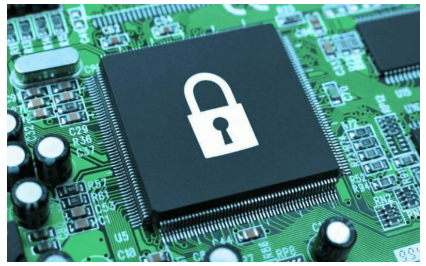
Secure connection



Secure root of trust



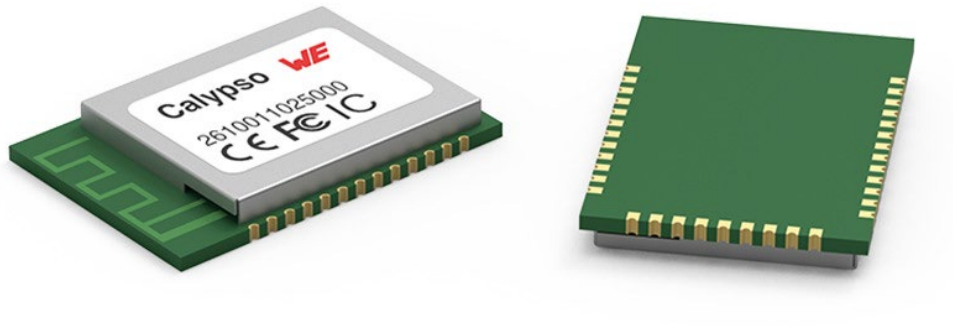
Secure FOTA



Physical security

CALYPSO WI-FI MODULE

Secure IoT ready



- ✓ 10 byte non-tamperable unique device ID
- ✓ Secure boot
- ✓ Secure storage – Encrypted file system to store certificates and other credentials
- ✓ Secure Wi-Fi connection – WPA3
- ✓ Secure socket – TLSv1.2
- ✓ Hardware accelerated crypto engine
- ✓ Secure Firmware over the air update

Wi Fi CERTIFIED

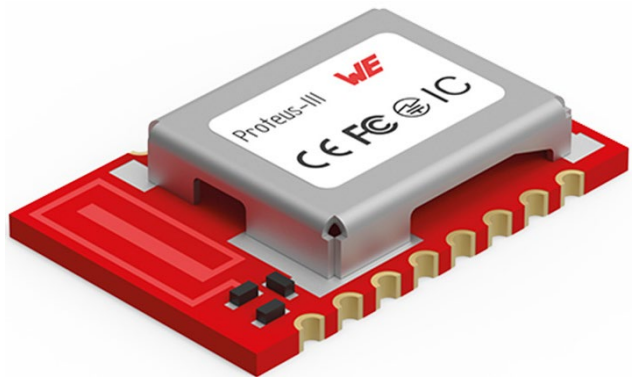
CE FC IC

A good basis for secure end application !!!

PROTEUS-III BLUETOOTH® LE 5.1 MODULE

Secure IoT ready

- ✓ Non-tamperable unique device ID
- ✓ Secure boot
- ✓ Secure BLE connection - LESC
- ✓ Hardware accelerated crypto engine
- ✓ Secure Firmware over the air update

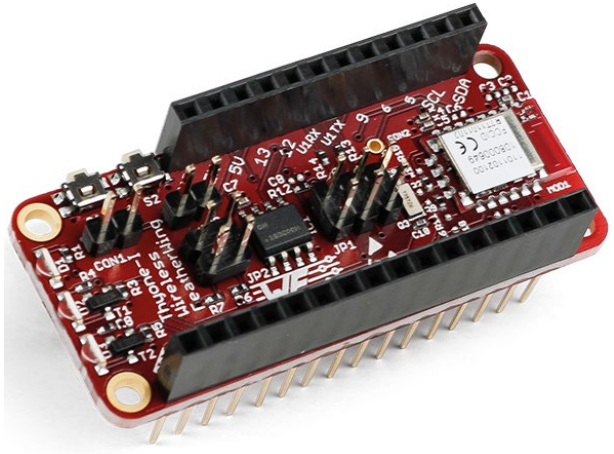


A good basis for secure end application !!!

THYONE-I WIRELESS MODULE

Secure IoT ready

Microchip
ATECC608B



2.4 GHz Proprietary
Wireless connectivity

- Nano SIM size
- Low power
- Range up to 750 m
- Broadcast, Multicast , Unicast
- Mesh capable

Cryptographic co-processor

- 72 bit UDID
- Secure key storage
- AES-128
- SHA256
- ECDH, ECC
- Secure boot

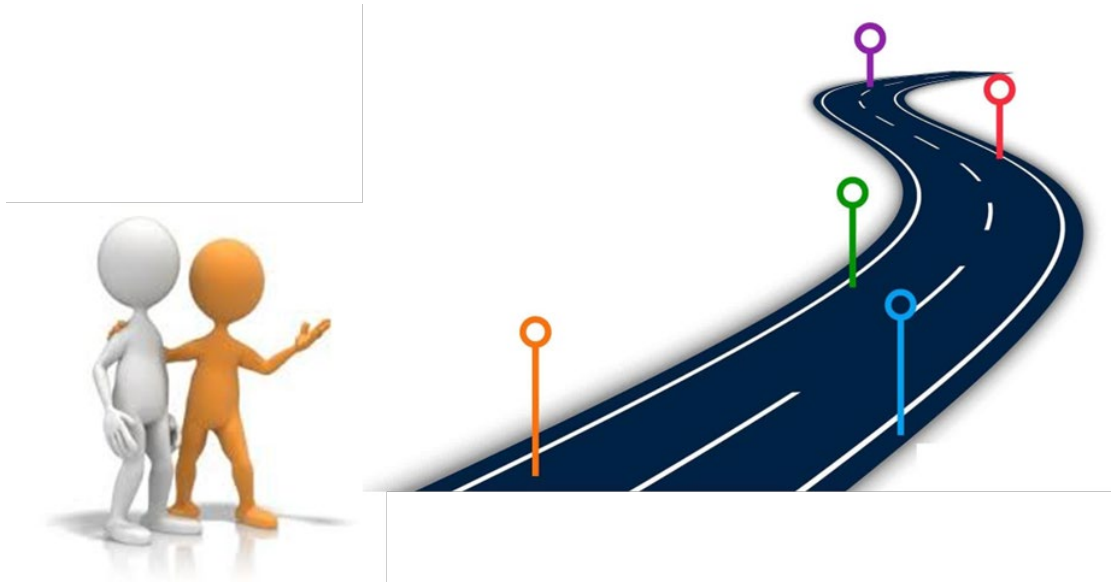
IIoT ready wireless
connectivity

A good basis for secure end application !!!

CYBERSECURITY COMPLIANCE WITH WE RADIO MODULES

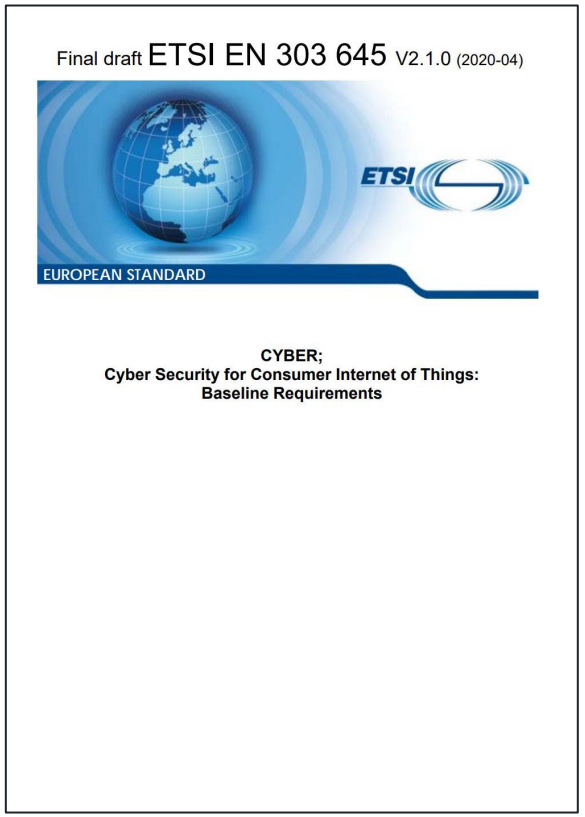
Our value addition

- Pre-filled templates for risk assessment
- List of network and security assets for your use cases
- Information regarding changes via the PCN process
- Prompt security updates subject to availability
- Expert consultation at your door-step



THANK YOU!

GOOD DOCUMENTATION



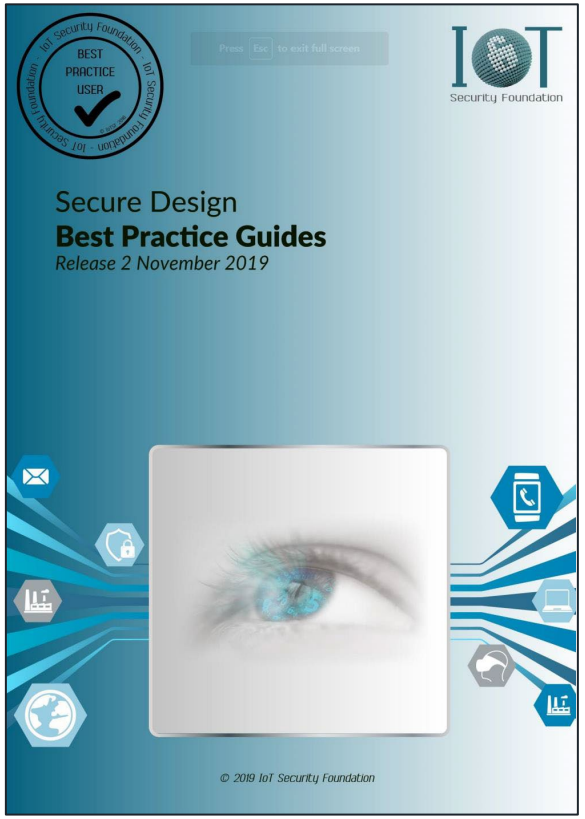
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

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

WÜRTH ELEKTRONIK MORE THAN YOU EXPECT

PHOENIX TESTLAB

Bundesnetzagentur

WEBINAR:

5VOR12
IN DER CYBERSICHERHEIT

VON RED BIS CRA

INFORMATIONEN UND DISKUSSION

1. **Einführung**
   Holger Bentje, Phoenix Testlab
   Hintergrund, Entstehung und Relevanz von RED-DA und CRA

2. **Konformitäts- und Risikobewertung**
   Dietmar Frei, Phoenix Testlab
   Was ist gefordert? Wo bestehen Unsicherheiten?

3. **Bewertbarkeit aus Sicht der Marktüberwachung**
   Jonas Bünnemann, Bundesnetzagentur
   Einschätzung der Bundesnetzagentur, Umgang mit Bestandssystemen

4. **Umsetzung in der Praxis**
   Adithya Madanahalli, Würth Elektronik
   Wie Funkmodule helfen können, Anforderungen effizient zu erfüllen

5. **Offene Fragerunde und Diskussion**
   Moderation: Michael Lang, Würth Elektronik
   Ihre Fragen, unsere Antworten – moderiert und interaktiv

WÜRTH ELEKTRONIK
MORE THAN YOU EXPECT

PHOENIX TESTLAB

Bundesnetzagentur

WEBINAR:

5VOR12
IN DER CYBERSICHERHEIT

VON RED BIS CRA

INFORMATIONEN UND DISKUSSION

FEEDBACK ZUM WEBINAR:

WÜRTH ELEKTRONIK
MORE THAN YOU EXPECT

PHOENIX TESTLAB

Bundesnetzagentur

WEBINAR:

5VOR12
IN DER CYBERSICHERHEIT

VON RED BIS CRA

INFORMATIONEN UND DISKUSSION

AUFZEICHNUNG DIESER VERANSTALTUNG IN WENIGEN TAGEN ONLINE

WÜRTH ELEKTRONIK
MORE THAN YOU EXPECT

PHOENIX TESTLAB

Bundesnetzagentur

WEBINAR:

5VOR12 IN DER CYBERSICHERHEIT

VIELEN DANK FÜR IHRE TEILNAHME!

AUF WIEDERSEHEN!