WÜRTH ELEKTRONIK
MORE THAN YOU EXPECT

PHOENIX TESTLAB

Bundesnetzagentur

WEBINAR:

CYBERSECURITY AT THE ELEVENTH HOUR

FROM RED TO CRA

INFORMATION AND DISCUSSION

WEBINAR:

CYBERSECURITY AT THE ELEVENTH HOUR

FROM RED TO CRA

INFORMATION AND DISCUSSION

1. **Introduction**
   Holger Bentje, Phoenix Testlab
   Background, origin, and relevance of RED-DA and CRA

2. **Conformity and Risk Assessment**
   Tobias Vogler, Phoenix Testlab
   What's required? Where are the uncertainties?

3. **Evaluability from a Market Surveillance Perspective**
   Jonas Bünnemann, Bundesnetzagentur
   Insights from the Federal Network Agency,
   handling legacy systems

4. **Practical Implementation**
   Adithya Madanahalli, Würth Elektronik
   How wireless modules can support compliance efficiently

5. **Open Q&A and Discussion** –
   Moderation: Michael Lang, Würth Elektronik
   Your questions, our answers – moderated and interactive

Welcome

Time is running out!

Introduction

Holger Bentje / Operations / 30 July 2025

Speaker

Holger Bentje

Master Specialist EMC & Radio Technologies

Director Notified Body RED & TCB USA, Canada, Japan

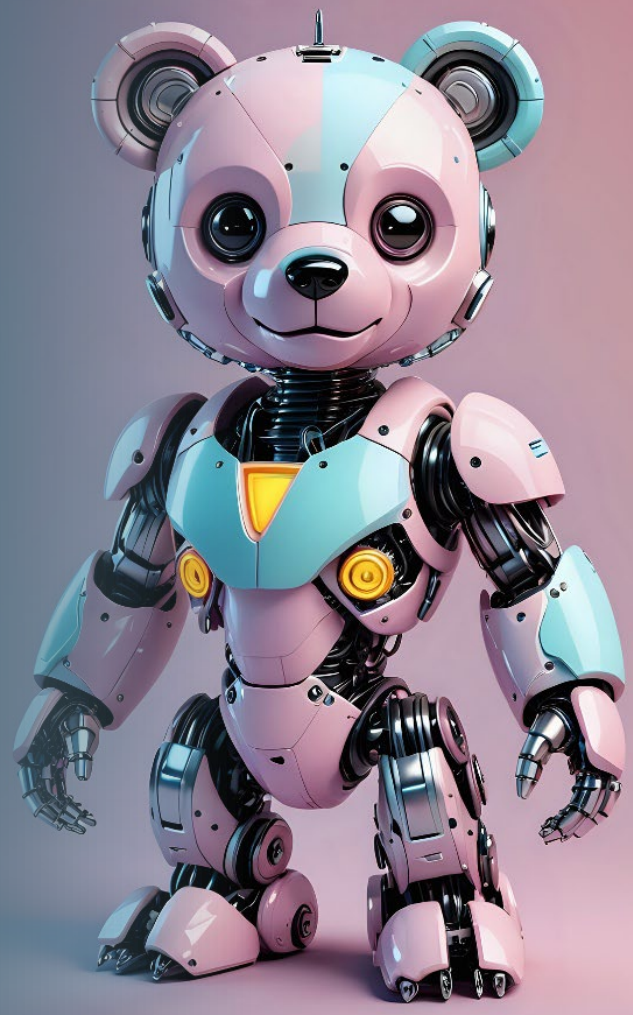
- +49-5235-9500-24
- bentje.holger@phoenix-testlab.de

The Problem

In **December 2016**, the Norwegian Consumer Council conducted an in-depth analysis of several internet-connected toys.

- Its findings point to a possible lack in the protection of children's rights to privacy and security.
- Thanks to integrated speakers, microphones and other sensors, inter-connected toys are "smart" and can for instance interpret speech, which makes them capable of interacting with the child
- They may also record not only photos, videos, geolocalisation data, data linked to the play experience, but also heartrate, sleeping habits or other biometrical data.
- They can also be connected to phones and tablets or directly to the internet.

The ability of these products to record, store and share information raises concerns related to their safety, security and privacy.



Source: EC Impact Assessment Report.pdf

Regulatory Initiative

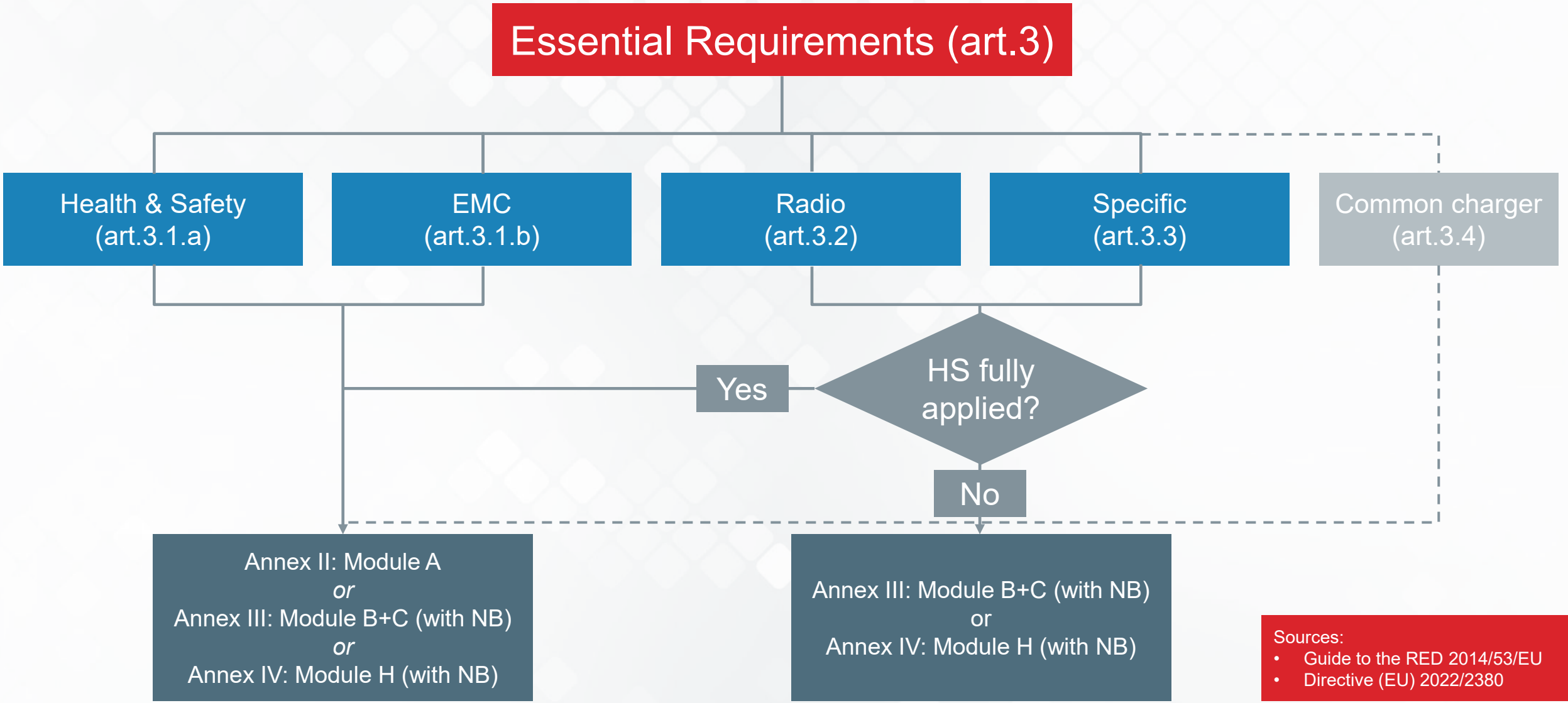
On 7 February 2018 a special “Telecommunication Conformity Assessment and Market Surveillance Committee” (TCAM) meeting was organized by the European Commission with a view on the possible extent of the applicability of Article 3.3 of the Radio Equipment Directive (RED).

Source: EC Impact Assessment Report.pdf

Radio Equipment Directive (RED)

- The Radio Equipment Directive 2014/53/EU (“RED”) establishes a **regulatory framework** for placing radio equipment on the European Market.
- It concerns mandatory **market access conditions** of products and allows Member States to take corrective measures on non-compliant equipment.
- The RED is a new approach legislation, where only **essential requirements** are defined.
  Manufacturers are requested to demonstrate how the technical solutions in their products comply with the law.
- All **internet-connected** radio equipment, including Internet of Things (IoT) with a radio interfaces and wearables, such as smart watches, fall under the Directive’s scope.

RED-Aspects = Essential Requirements = Risks!



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

The Solution

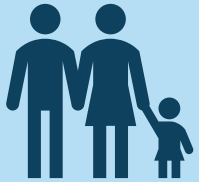
- Certain RED requirements could be made applicable via delegated acts.
- The RED has the potential to reach the desired basic level of security.
  - Fast: no new regulation must be adopted
  - Effective: insecure equipment to be banned from the European market by market enforcement
  - Proportionate: self-assessment of the base line requirements by the manufacturer
- Any delegated act under Article 3(3) will make applicable the corresponding essential requirements for specific categories of radio equipment.
- Only radio equipment placed on the market after 1 August 2025 will be subject to the new essential requirements.
- Delegated Regulation (EU) 2022/30 specifies the essential requirements of the RED.

Radio Equipment Directive and Cybersecurity

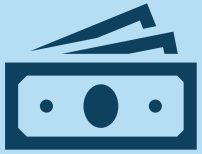
In the specific case of “cybersecurity”, although the RED does not mention the word, some of its essential requirements in Article 3.3 concern elements of it, such as…

Article 3.3 (d)
the protection of the networks

Article 3.3 (e)
the protection of privacy and personal data



Article 3.3 (f)
the protection against fraud



The next Steps

- The EU's cybersecurity policy has been implemented gradually.
- In a first step, manufacturers will adapt their products to the Delegated Regulation to the RED and then to the Cyber Resilience Act (CRA)
- The harmonized standards in support of the Delegated Regulation will be reused and supplemented by the CRA.
- The cybersecurity level of products in the EU will be gradually improved.
- The Cyber Resilience Act will be the evolution of the delegated act on RED.
  - Scope: All digital products, including hardware and software, not limited to radio equipment.
  - Lifetime: Applies to the entire life cycle of the product and not just the initial placing on the market.
- CRA has been published in the Official Journal of the EU as (EU) 2024/2847.
  - Published: 20.11.2024
  - Entry into force: 10.12.2024
  - Reporting obligations from: 11.09.2026
  - Effective date from: 11.12.2027

THANK YOU

Time is running out!

Time is running out!

WEBINAR:

CYBERSECURITY AT THE ELEVENTH HOUR

FROM RED TO CRA

INFORMATION AND DISCUSSION

1. **Introduction**
   Holger Bentje, Phoenix Testlab
   Background, origin, and relevance of RED-DA and CRA

2. **Conformity and Risk Assessment**
   Tobias Vogler, Phoenix Testlab
   What's required? Where are the uncertainties?

3. **Evaluability from a Market Surveillance Perspective**
   Jonas Bünnemann, Bundesnetzagentur
   Insights from the Federal Network Agency,
   handling legacy systems

4. **Practical Implementation**
   Adithya Madanahalli, Würth Elektronik
   How wireless modules can support compliance efficiently

5. **Open Q&A and Discussion** –
   Moderation: Michael Lang, Würth Elektronik
   Your questions, our answers – moderated and interactive

Welcome

Cybersecurity at the eleventh hour

Conformity and Risk Assessment

Tobias Vogler / Cyber Security / July 2025

Public

Your speaker

Tobias Vogler

Section Manager
Cyber Security

- +49 5235 9500-249
- vogler.tobias@phoenix-testlab.de

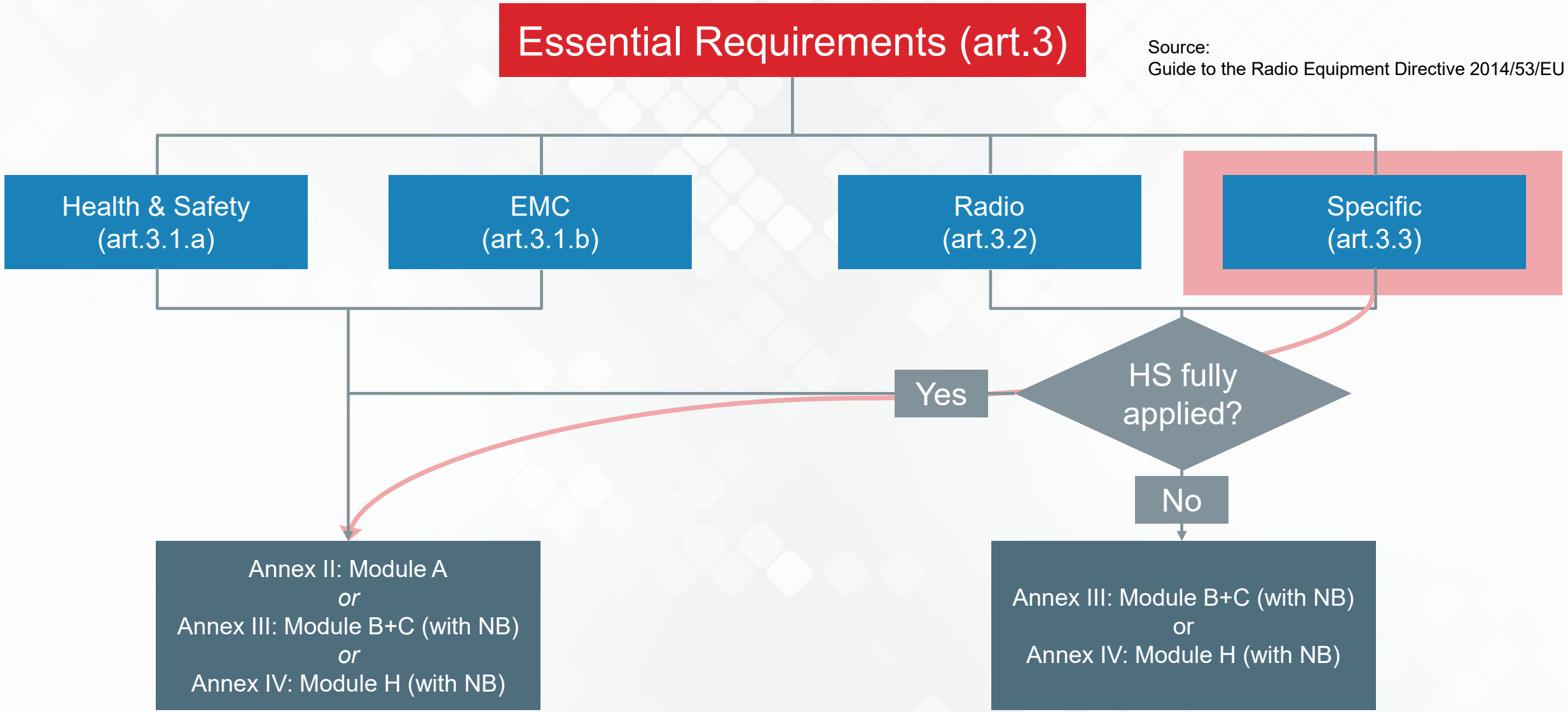
AGENDA

Implementation of the RED requirements Art. 3.3
- Risk Assessment
- Declaration 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

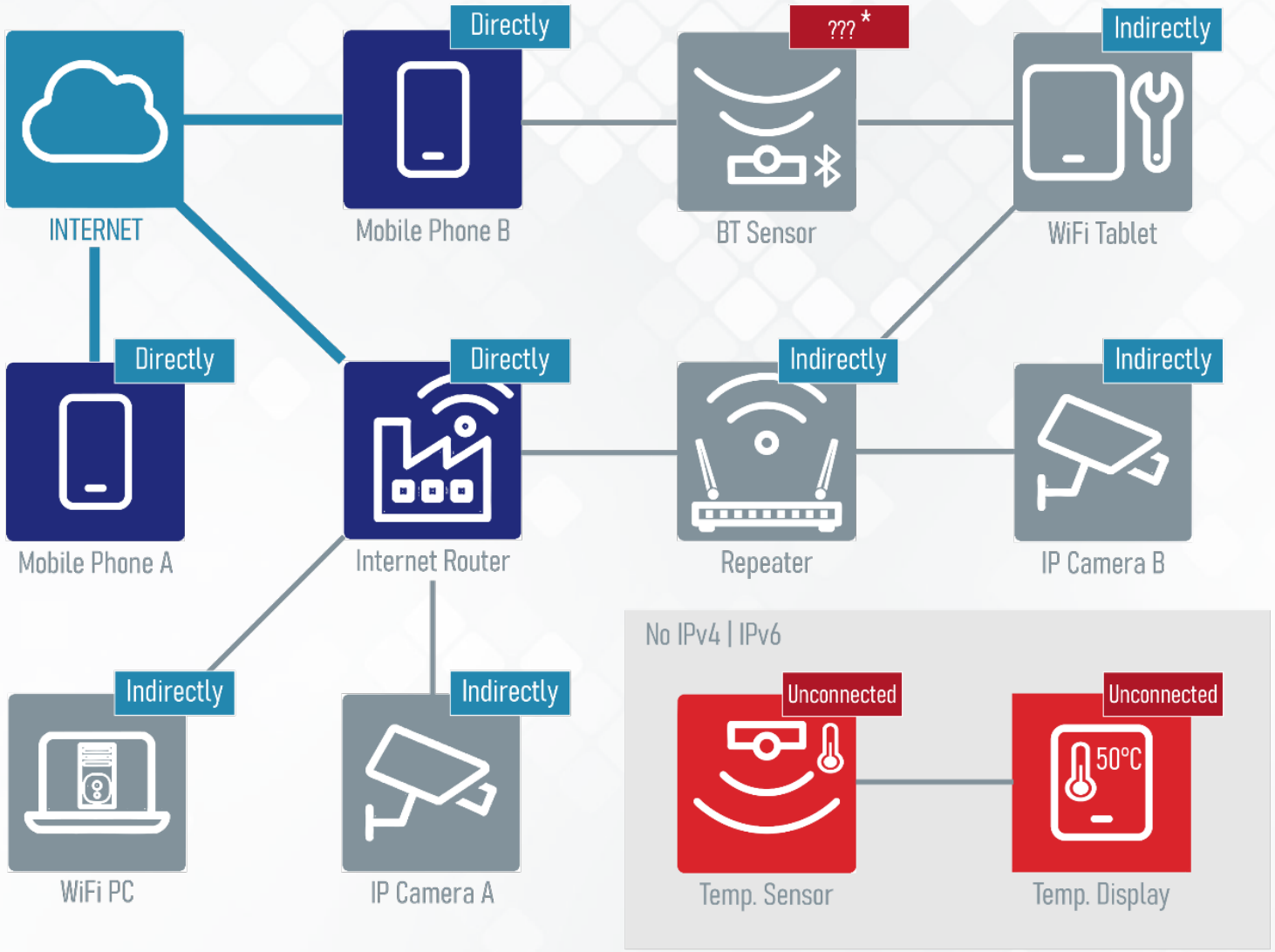
Which point of Art 3.3 is applicable to the product?

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

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 verified by
    - …..
    - EN18031-1 / EN18031-2 / EN18031-3 (lastest version: 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	☑	☑	☑

Summary

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

Public

Internal

WÜRTH ELEKTRONIK
MORE THAN YOU EXPECT

PHOENIX TESTLAB

Bundesnetzagentur

WEBINAR:

CYBERSECURITY AT THE ELEVENTH HOUR

FROM RED TO CRA

INFORMATION AND DISCUSSION

1. **Introduction**
   Holger Bentje, Phoenix Testlab
   Background, origin, and relevance of RED-DA and CRA

2. **Conformity and Risk Assessment**
   Tobias Vogler, Phoenix Testlab
   What's required? Where are the uncertainties?

3. **Evaluability from a Market Surveillance Perspective**
   Jonas Bünnemann, Bundesnetzagentur
   Insights from the Federal Network Agency,
   handling legacy systems

4. **Practical Implementation**
   Adithya Madanahalli, Würth Elektronik
   How wireless modules can support compliance efficiently

5. **Open Q&A and Discussion** –
   Moderation: Michael Lang, Würth Elektronik
   Your questions, our answers – moderated and interactive

Bundesnetzagentur

Cybersecurity

Stock regulation and risk assessment

Jonas Bünnemann
Referat 411 Market Surveillance, EMC and RED

Topics

- Stock regulation
  - Outer EEA (European Economic Area) imports
  - Radio equipment produced in the EEA
- Risk assessment

Stock regulation

Regarding Outer EEA imports & inner EEA prodcuction of radio equipment

Outer EEA imports of radio equipment

- Radio equipment needs to comply with 2014/53/EU standards, the time of the market lunch is crucial!
  - For imports → the import date (completion of costume procedures)
  - The date of production is not relvant!

- Products that completed the costume procedures after 01.08.2025 WITHOUT conformity regarding cybersecurity:
  - Radio equipment registered and released for free movement of goods
  - YES: the specific radio equipment is released into the market for the first time
    - No matter *when* the specific radio equipment will be sold
  - NO: No import of radio equipment released after the 01.08.2025

Radio equipment produced in EEA

- Again: the decisive factor is the time of market lunch
  - Is the radio equipment already stored in sales warehouse?
  - Date of production could be an indicator

- When is radio equipment allowed to be stored in sales warehouse?
  - Completed & passed conformity assessment procedure

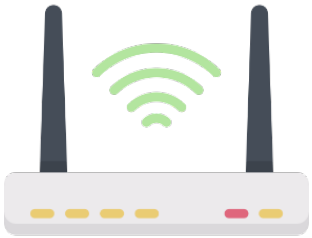
- After **01.08.2025**:
  - A new conformity assessment procedure is required!
  - Systems that are still being produced are no longer marketable!

Risk assessment

Risk assessment

- Orientation towards the EU risk assessment regarding product saftey

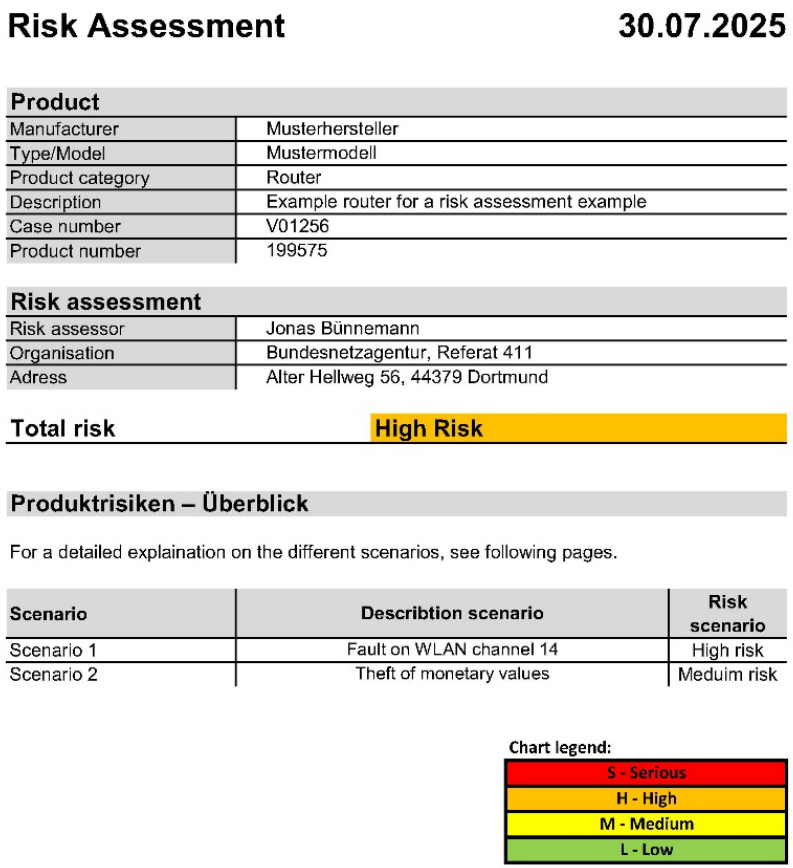
- Example for risk assessment:
  - Layout looks like future evaluation form of the BNetzA
  - Contents pose as an example, no claim to accuracy!



Risk assessment

- Different scenarios possible per evaluation
  - five steps max. per scenario

- Assessment of individual and overall risk
  - Individual risk per scenario
  - Overall risk = highest individual risk



Risk Assessment **30.07.2025**

Product	
Manufacturer	Musterhersteller
Type/Model	Mustermodell
Product category	Router
Description	Example router for a risk assessment example
Case number	V01256
Product number	199575

Risk assessment	
Risk assessor	Jonas Bünnemann
Organisation	Bundesnetzagentur, Referat 411
Adress	Alter Hellweg 56, 44379 Dortmund

Total risk **High Risk**

Produktrisiken – Überblick

For a detailed explaination on the different scenarios, see following pages.

Scenario	Describtion scenario	Risk scenario
Scenario 1	Fault on WLAN channel 14	High risk
Scenario 2	Theft of monetary values	Meduim risk

Chart legend:

- S - Serious
- H - High
- M - Medium
- L - Low

Risk assessment - Examples

- Danger of product
  - Description of danger parameters
- User
  - Description of affected user
- Severity
  - Severity of damage
- Probability that the steps towards the risk will occur
  - Scenario description

Risk Assessment **30.07.2025**

Scenario 1	Fault on WLAN channel 14		High Risk
	1. Product hazard		
	Hazard group	Access to network	
	Hazard type	Network disruption	
	2. Consumer		
	User type	Older children	
	Description	8 to 14 years (Vulnerable consumers)	
	3. Severity of the harm		
	Injury level	3	
	4. Probability of the steps to injury		
Step/s	Description on how the step leads to the harm		Wahrschein-lichkeit
Step 1	Network access via standard router password		0,05
Step 2	Setup changes to use channel 14, in Germany reserved for hospital communications		0,08
Step 3	Disruption of hospital equipment		0,05

Overall probability	0,0002000
Risc of this scenario	High

Kontakt

Jonas Bünnemann
Referat 411
marktueberwachung@BNetzA.de

Bundesnetzagentur

WÜRTH ELEKTRONIK
MORE THAN YOU EXPECT

PHOENIX TESTLAB

Bundesnetzagentur

WEBINAR:

CYBERSECURITY AT THE ELEVENTH HOUR

FROM RED TO CRA

INFORMATION AND DISCUSSION

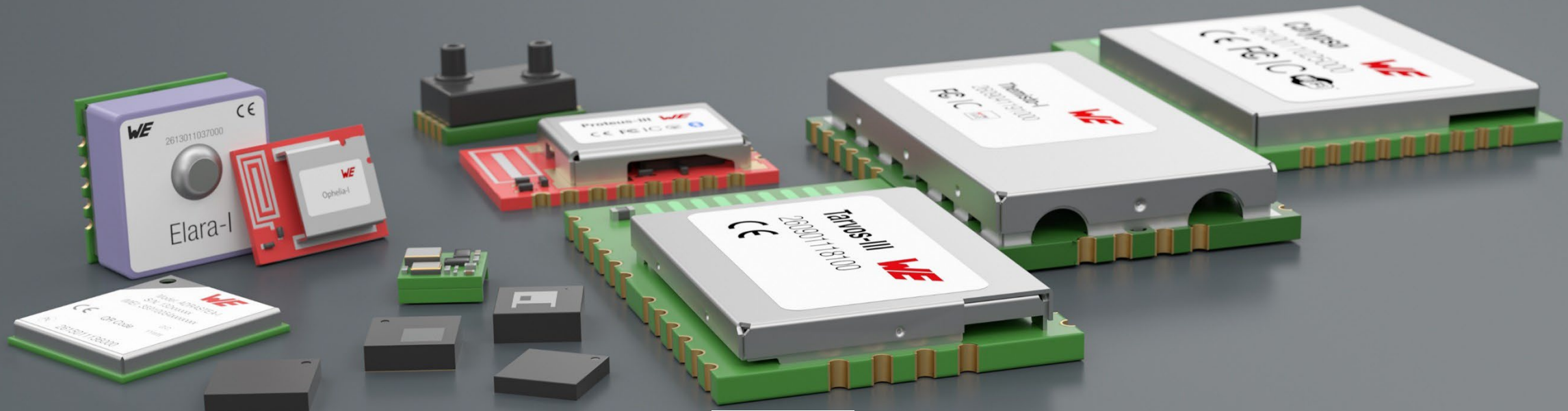
1. **Introduction**
   Holger Bentje, Phoenix Testlab
   Background, origin, and relevance of RED-DA and CRA

2. **Conformity and Risk Assessment**
   Tobias Vogler, Phoenix Testlab
   What's required? Where are the uncertainties?

3. **Evaluability from a Market Surveillance Perspective**
   Jonas Bünnemann, Bundesnetzagentur
   Insights from the Federal Network Agency, handling legacy systems

4. **Practical Implementation**
   Adithya Madanahalli, Würth Elektronik
   How wireless modules can support compliance efficiently

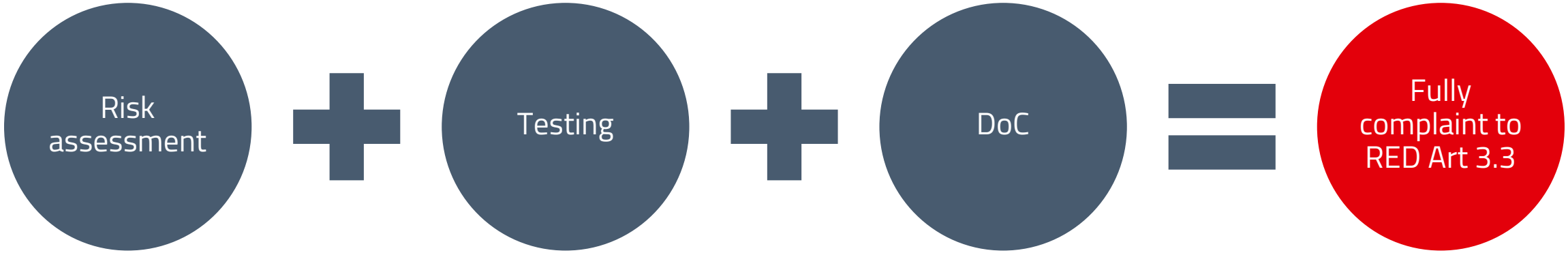
5. **Open Q&A and Discussion** –
   Moderation: Michael Lang, Würth Elektronik
   Your questions, our answers – moderated and interactive



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

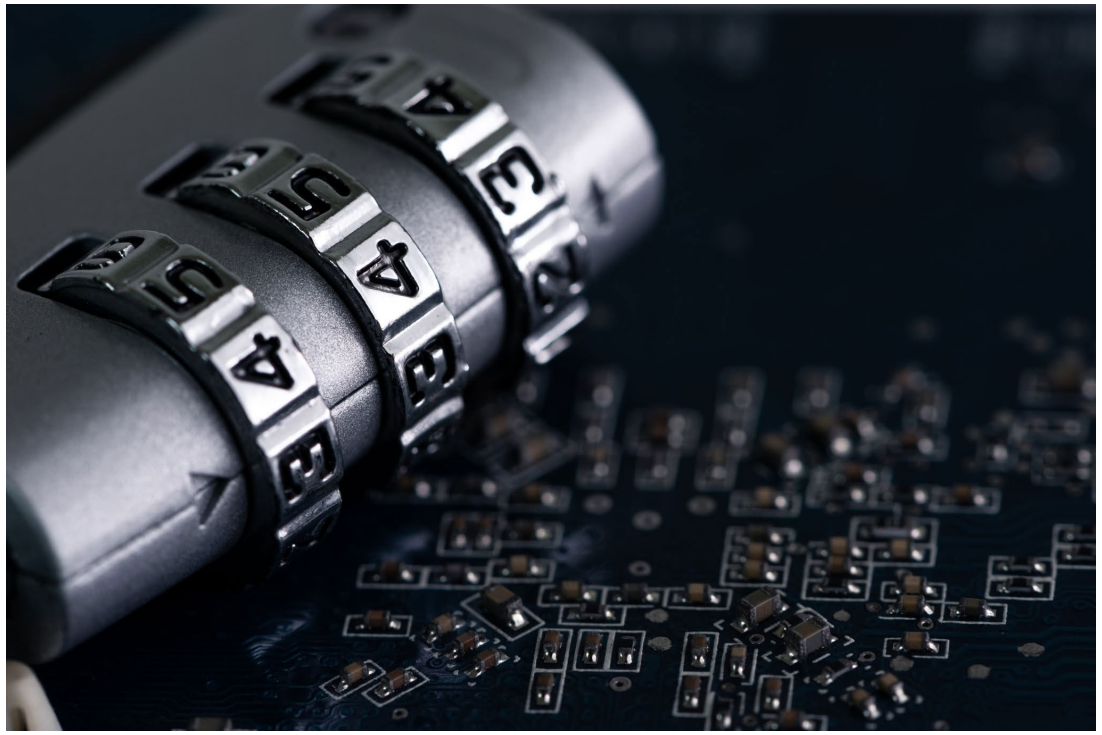
- “Assets” can be of the following types:

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?

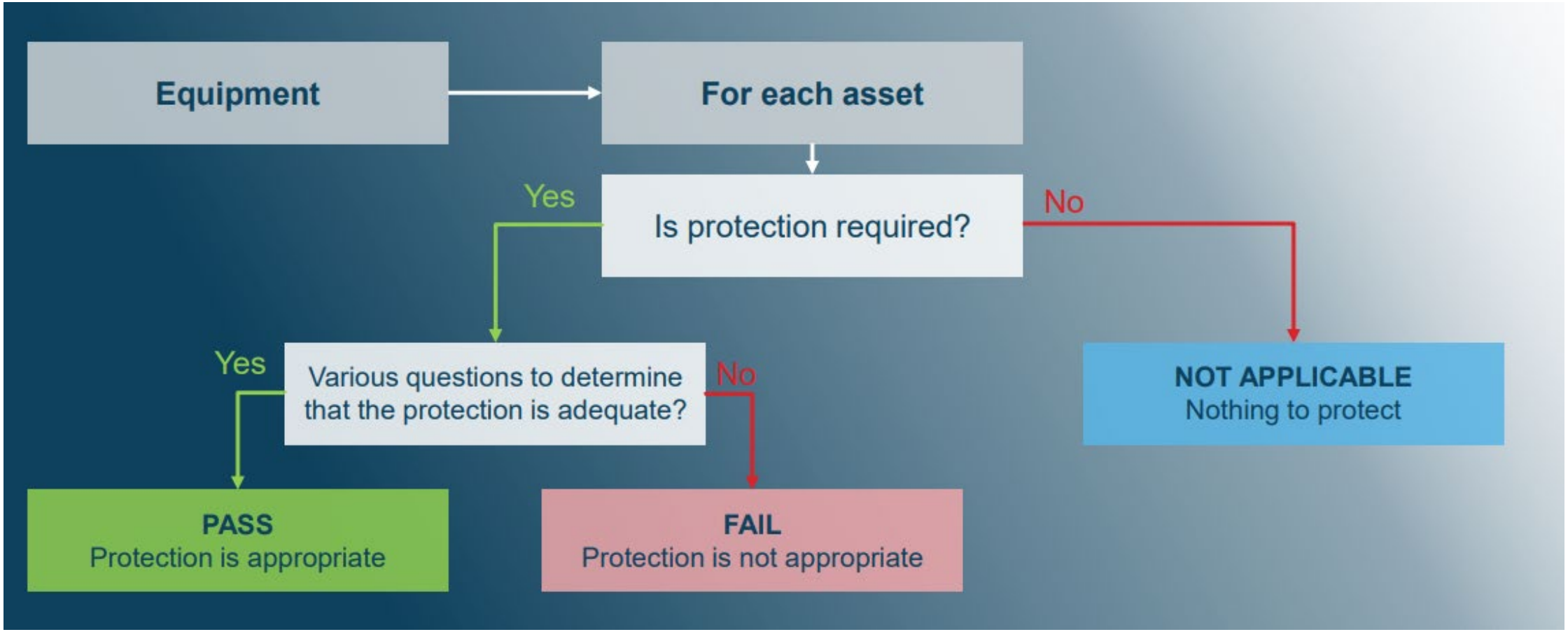
- Definition as per standard
  - Personal information
  - Traffic data
  - Location data

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

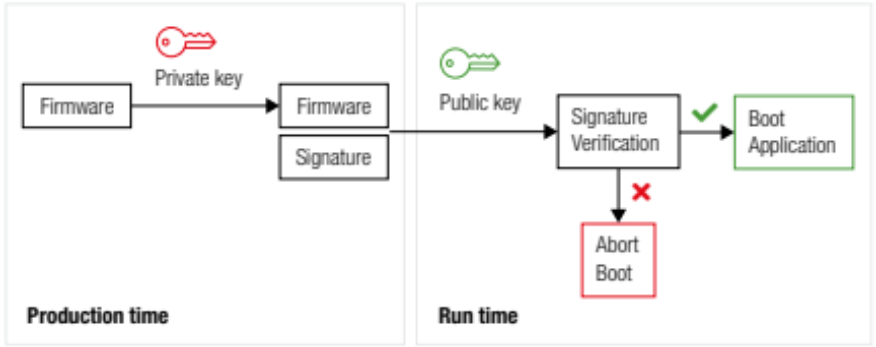
- Operations on personal data
  - Collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

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

DECISION TREES

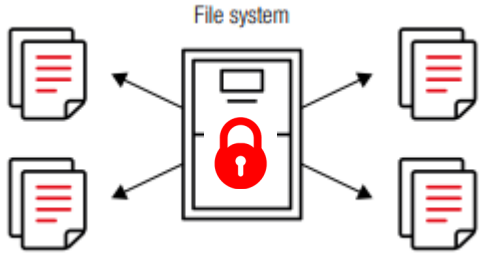


COMMON MINIMUM-SECURITY REQUIREMENTS

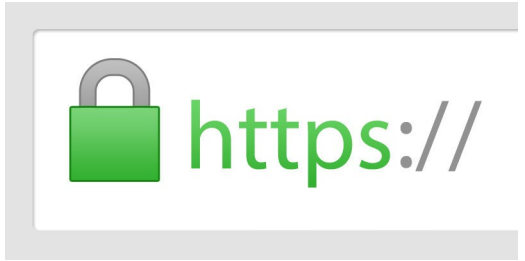


Secure production

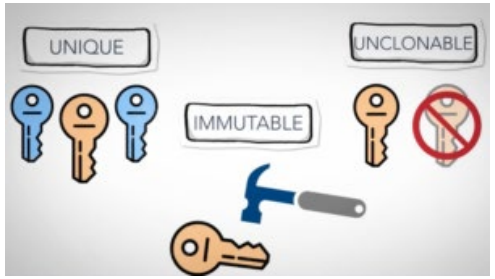
Secure boot



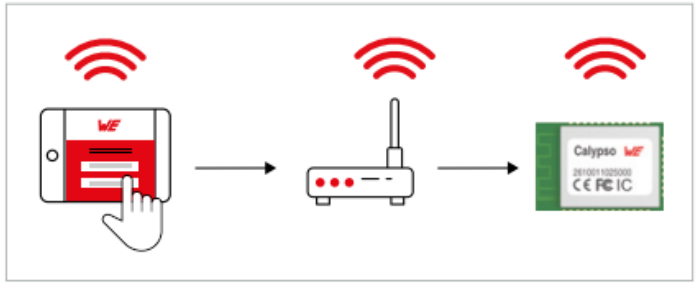
Secure storage



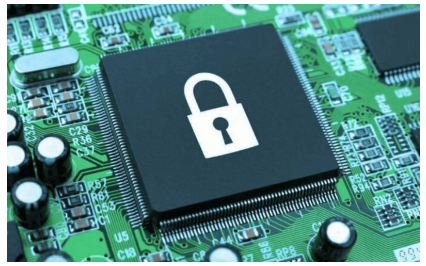
Secure connection



Secure root of trust



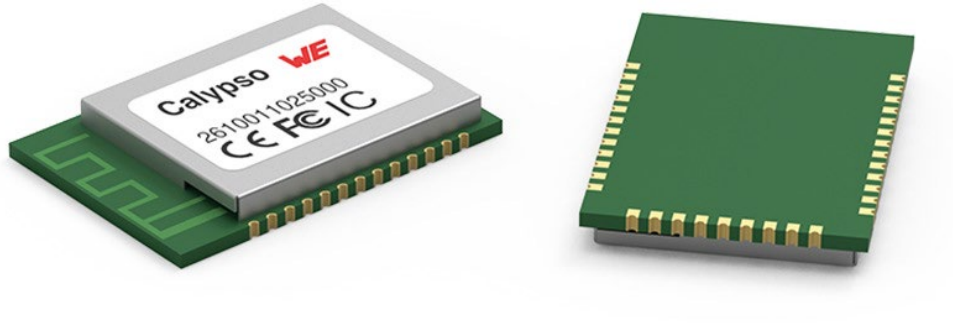
Secure FOTA



Physical security

CALYPSO/CORDELIA-I 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

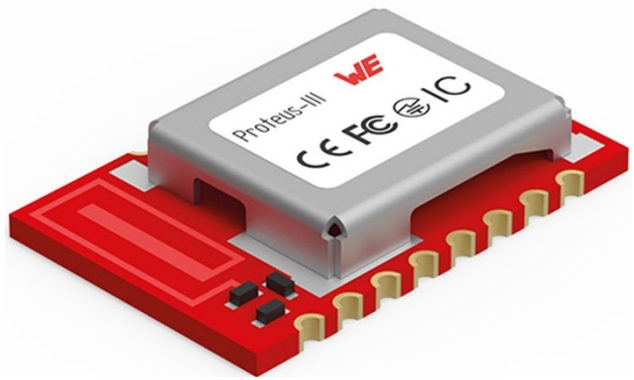
CE FC IC

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

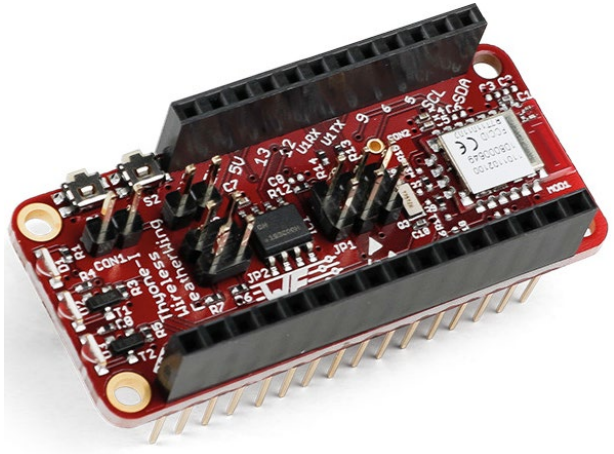


A good basis for secure end application !!!

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

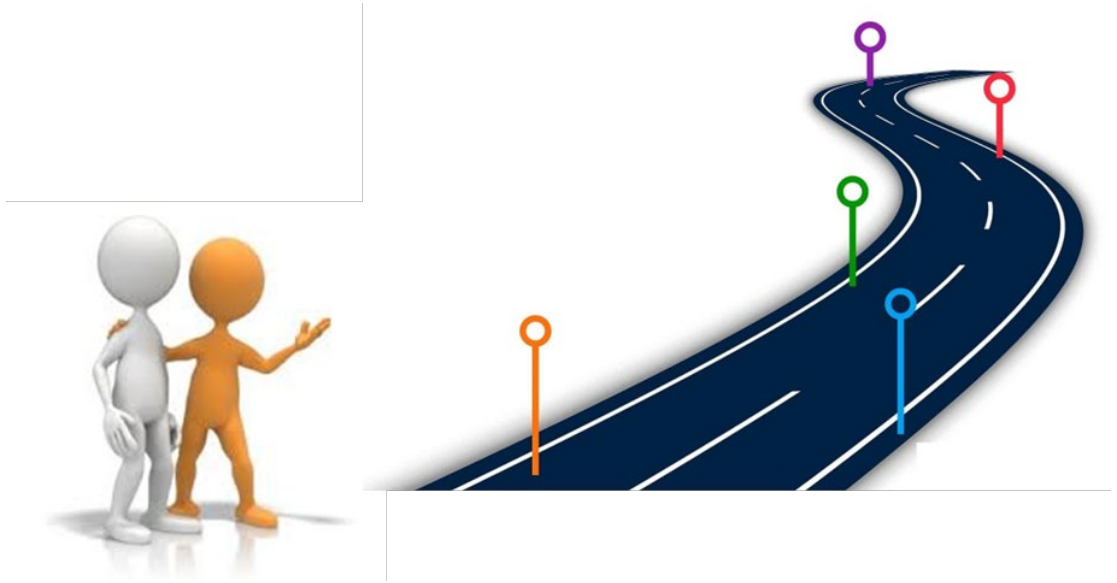
IIoT ready wireless
connectivity

A good basis for secure end application !!!

CYBERSECURITY COMPLIANCE WITH WE RADIO MODULES

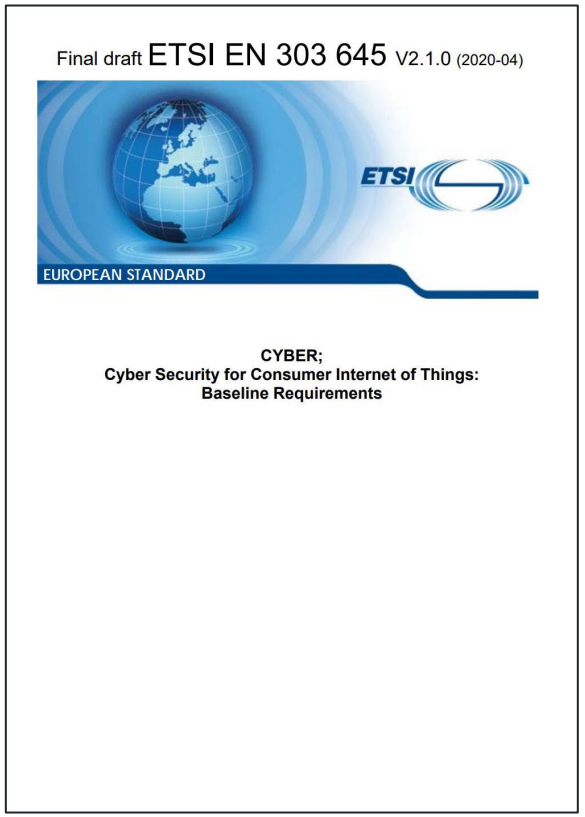
Our value addition

- 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



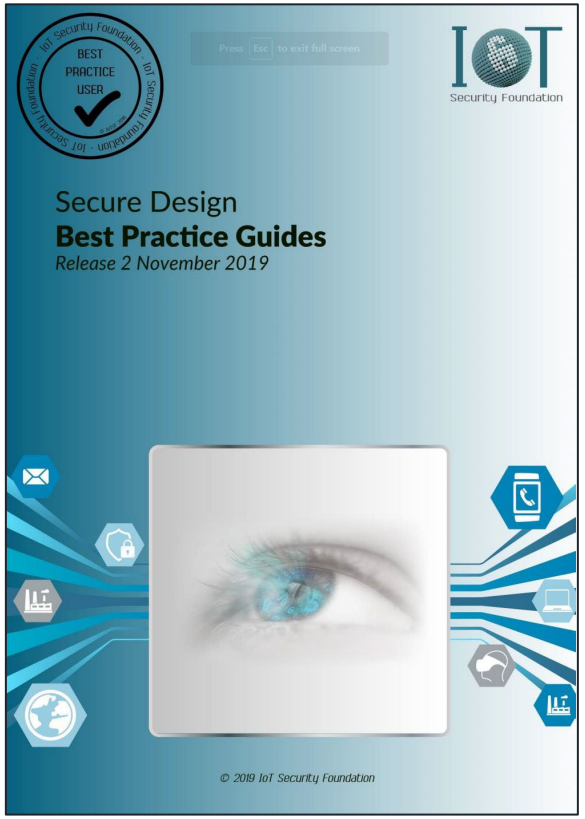
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

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:

CYBERSECURITY AT THE ELEVENTH HOUR

FROM RED TO CRA

INFORMATION AND DISCUSSION

1. **Introduction**
   Holger Bentje, Phoenix Testlab
   Background, origin, and relevance of RED-DA and CRA

2. **Conformity and Risk Assessment**
   Tobias Vogler, Phoenix Testlab
   What's required? Where are the uncertainties?

3. **Evaluability from a Market Surveillance Perspective**
   Jonas Bünnemann, Bundesnetzagentur
   Insights from the Federal Network Agency,
   handling legacy systems

4. **Practical Implementation**
   Adithya Madanahalli, Würth Elektronik
   How wireless modules can support compliance efficiently

5. **Open Q&A and Discussion** –
   Moderation: Michael Lang, Würth Elektronik
   Your questions, our answers – moderated and interactive

WÜRTH ELEKTRONIK
MORE THAN YOU EXPECT

PHOENIX TESTLAB

Bundesnetzagentur

WEBINAR:

CYBERSECURITY AT THE ELEVENTH HOUR

FROM RED TO CRA

INFORMATION AND DISCUSSION

FEEDBACK TO WEBINAR:

WÜRTH ELEKTRONIK
MORE THAN YOU EXPECT

PHOENIX TESTLAB

Bundesnetzagentur

WEBINAR:

CYBERSECURITY AT THE ELEVENTH HOUR

FROM RED TO CRA

INFORMATION AND DISCUSSION

RECORDING OF THIS EVENT IN A FEW DAYS ONLINE

WÜRTH ELEKTRONIK
MORE THAN YOU EXPECT

PHOENIX TESTLAB

Bundesnetzagentur

WEBINAR:

CYBERSECURITY AT THE ELEVENTH HOUR

THANK YOU FOR YOUR PARTICIPATION!

SEE YOU SOON!