

Panel 2

Cybersecurity and RED –
implementing measures

Speaker

Holger Bentje

Chairman REDCA

Radio Equipment Directive Compliance Association

- REDCA provides a forum for people concerned with the compliance of radio equipment with regulations and technical standards in the EEA.
- In particular formed under the requirements of the Radio Equipment Directive 2014/53/EU specifically for Article 26.11 and Article 38 for Notified Bodies (sectorial group of notified bodies).
- Members are: Notified Bodies, Testing Laboratories, Consulting Companies, Manufacturers, Member states and administrations, Authorities from MRA regions, etc.



<http://www.redca.eu/>



Notified Body Work Today

- More than 70 RED Notified Bodies are listed in the NANDO database
- They are located in the EU 27 countries, in the USA and Japan (MRAs with EU)
- Notified Bodies evaluate radio equipment where OJEU listed harmonised standards for Article 3.2 and Article 3.3 have not been followed, or not followed in full.
- The essential requirements to be assessed come from Article 3 of the Directive
 - Article 3.1a) Health and Safety
 - Article 3.1b) Electromagnetic Compatibility
 - Article 3.2 Effective and efficient use of radio spectrum
 - Article 3.3 Specific requirements

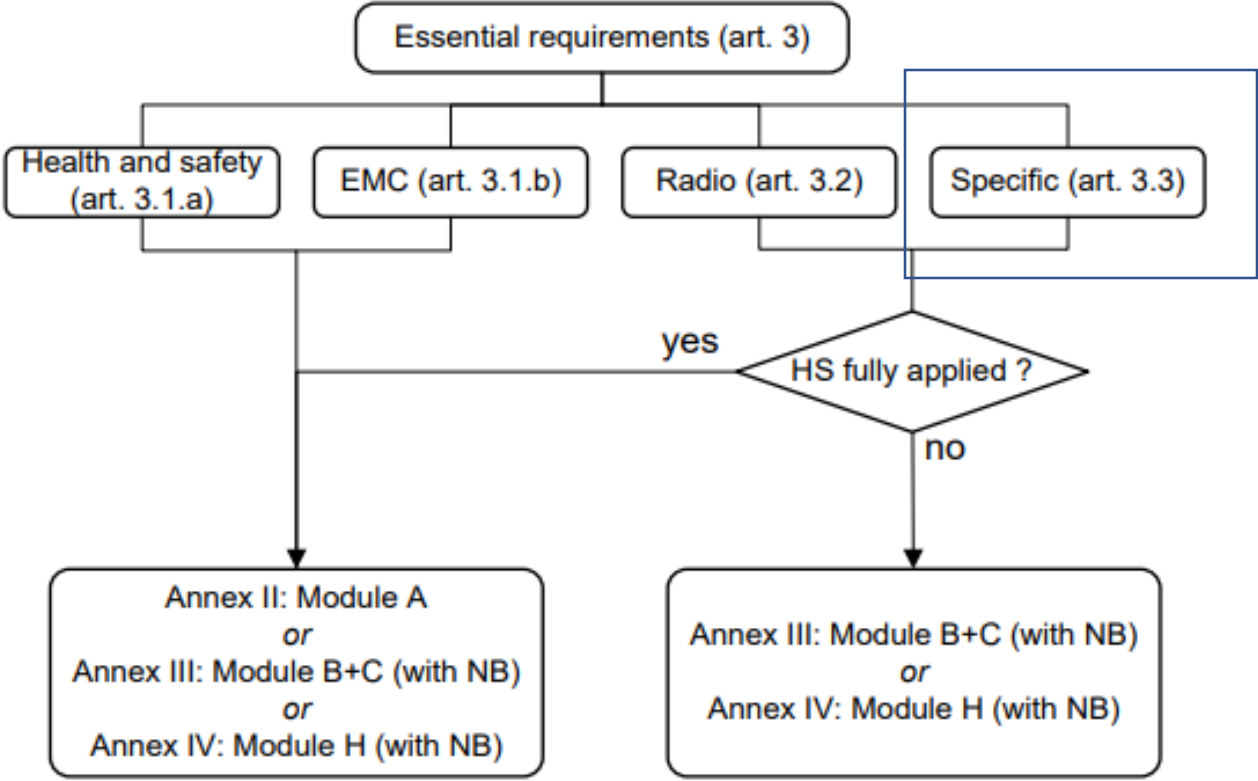


Notified Body Work – Article 3.3

- Currently, there are requirements according to Article 3.3 of the RED only towards emergency services
- These requirements have been taken over unchanged from the R&TTE Directive and continue to apply under the RED
- Discussions are currently underway to apply the following articles to include the topic of cybersecurity in the RED.
 - **Article 3(3) (d):** connected devices;
 - **Article 3(3) (e):** connected devices, toy devices and wearable devices, in so far as they are capable of processing any information or data covered by Regulation (EU) 2016/679 (GDPR) or Directive 2002/58/EC (ePrivacy).
 - **Article 3(3) (f):** connected devices, in so far as they enable the holder or user to transfer money, monetary value or virtual currency.



Conformity Assessment Procedures



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



Challenges for RED Notified Bodies

- Cybersecurity is a new, additional, area for RED Notified Bodies
- Expertise is generally not available at present and needs to be built up
 - RED Notified Bodies could extend their scope internally or
 - RED Notified Bodies could contract additional experts, often from within their company, but the RED Notified Body makes the final decision for certification
- In order to build up the expertise, it is necessary to have precisely defined the essential requirements in the RED beforehand.



Expectations on Standardization

- Manufacturers have to evaluate their products against the essential requirements of the RED.
- Manufacturers often give preference to the use of harmonized standards published in the Official Journal of the EU.
- These harmonized standards are also used by Notified Bodies in order to assess for equivalence of other supplied methods / evidence.
- In the absence of harmonized standards, it may be difficult to define a level of common approach by RED Notified Bodies.



Expectations on Standardization

- It is important that new Article 3.3 essential requirements are supported by standards, preferably harmonized, in the short term.
- These standards are also an important basis for ensuring a common understanding of the general requirements by the Notified Bodies in the cybersecurity environment.
- Notified Bodies often work where harmonized standards have not been followed, or not being followed in full.



Thank you for your attention