TC CYBER – State of play for security testing under the RED

Presented by: **Francois Ambrosini – umlaut, ETSI TC CYBER expert**

For: **ENISA Cybersecurity Standardization Conference, panel 2: Radio Equipment Directive – setting up the scene and future work**

02.02.2021

TC CYBER activities

Cybersecurity ecosystem

Protection of Personal data and communication

Cybersecurity for Critical Infrastructures

Direct support to EU legislation

Consumer IoT Security and Privacy

EN 303 645
TS 103 701

Network Security

Cybersecurity tools & guides

TR 103 787

Quantum-Safe Cryptography

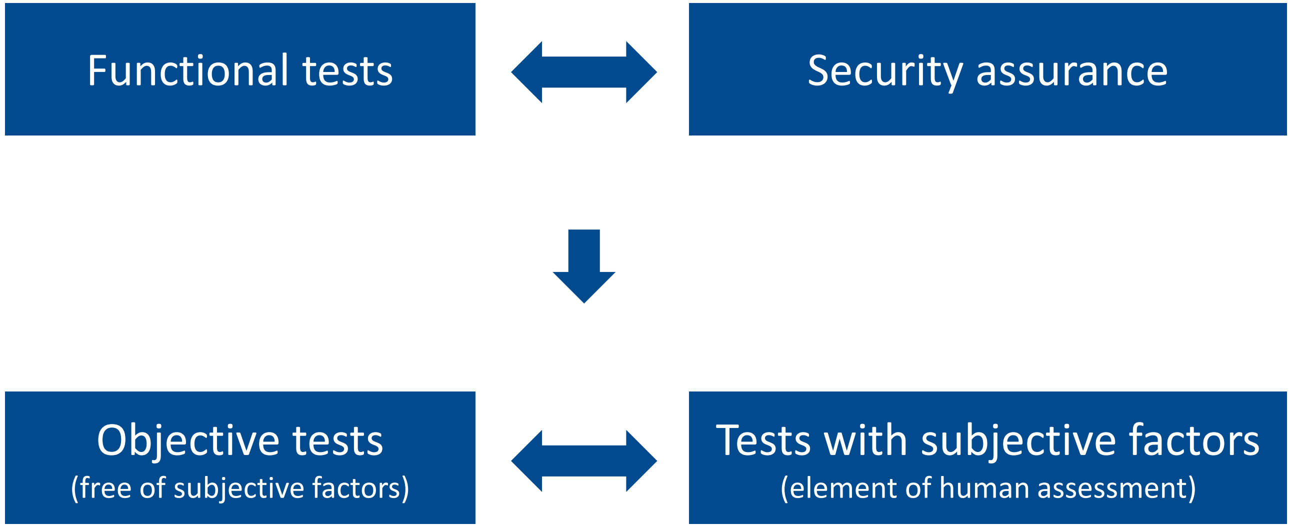
Background

- TC CYBER has taken a long-standing care towards the possible activation of Radio Equipment Directive articles 3(3)(d/e/f), which involve a security dimension
  - This presentation does not address interrelations with RED article 3(3)(i)
- European Standard Organisations will be asked to develop Harmonised Standards (HEN) to address these articles
- Security requirements specified in a HEN must be testable
- One challenge lies in the nature of security testing, which can be hardly mapped into legally certain requirements
- This presentation attempts to illustrate what can be done for security under the RED with a view of coordinating with other legal instruments, through the lens of security testing

Categorising security tests

- Security testing is a vast domain

- Analysis under the NLF leads to a new categorization



Functional tests

Security assurance

Objective tests
(free of subjective factors)

Tests with subjective factors
(element of human assessment)

- TC CYBER’s understanding is that only tests free of subjective factors are possible, that provide clear and unambiguous pass/fail results, to ensure legal certainty

Examples of test categories

Objective tests
Assessing properties on radio equipment documentation, packaging, casing
Assessing the existence of high-level to very low-level functions and features to achieve particular outcome
Assessing that a function with specific inputs yields the expected results
Observing behaviour with lab equipment

Subjective tests
Assessing adequacy of risk analysis
Assessing adequacy of mitigations to security objectives and context (appropriateness)
Assessing adequacy of mitigations to the level of risk
Assessing implementation against state-of-the-art
Assessing against open-ended questions
Penetration testing, fuzzing, etc.

These tests do not lead to pass/fail results without introducing an element of doubt

Conclusions

- Scope
  - scope of legislative instruments and standards should be carefully considered and overlaps avoided
  - duplication of testing efforts should be avoided

- Suitability is far from certain
  - only tests free of subjective factors are fit for the RED
  - this has consequences: only security requirements leading to functional tests can be defined under an HEN
  - thus the RED is limited in security scope and cannot provide any form of assurance, but needs to be complemented by a larger set of legislative instruments that address other aspects of cybersecurity, such as the Cybersecurity Act
  - This assumes that tests free of subjective factors can be found that are suitable – NOT GUARANTEED

A final note on documentation-based testing

- Testing based on documentation can be categorised as follows:
  - Testing of properties of the documentation itself (e.g., the user documentation contains a reference to a data protection policy)
  - Testing of properties of the radio equipment, which can be informed by documentation (e.g., a component provides secure memory, a library provides adequate cryptographic functions, the radio equipment hosts a secure element)
- The latter category relies on technical documentation (e.g. from a supplier) which equals to a manufacturer declaration and can be problematic under a concept of legal certainty
- Currently under discussion is the possibility of using security certificates to identify security properties of components of a radio equipment

Thank you!