PROPOSALS ON ETCS COMPATIBILITY TESTING & RE-AUTHORIZATION

Michel Van Liefferinge
UNISIG

CCRCC 2017

Agenda

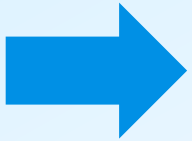
- **ETCS compatibility testing**
- Re-authorization after modifications
- Next steps

ETCS compatibility testing - background

- After certification of ETCS on-board and ETCS trackside constituents/subsystems, additional compatibility checks between real trackside and on-board systems are highly recommended :
  - ✓ Reference to CCS TSI – chap 6.2.5 Additional tests and chap 6.5 Compatibility tests
  - ✓ “Framework agreement on European Lab” signed by the UNISIG members in February 2014, including standardization of process and interfaces for remote testing (UNISIG Subsets 110, 111 & 112)
  - ✓ “Guideline for CCS authorization on rail freight corridor 1” from the NSA Corridor 1 working group

ETCS compatibility testing – current status

- Member States / Countries deploying ETCS already impose a compatibility process, but the detailed implementation is variable
- Examples: Switzerland, The Netherlands, Italy, Spain

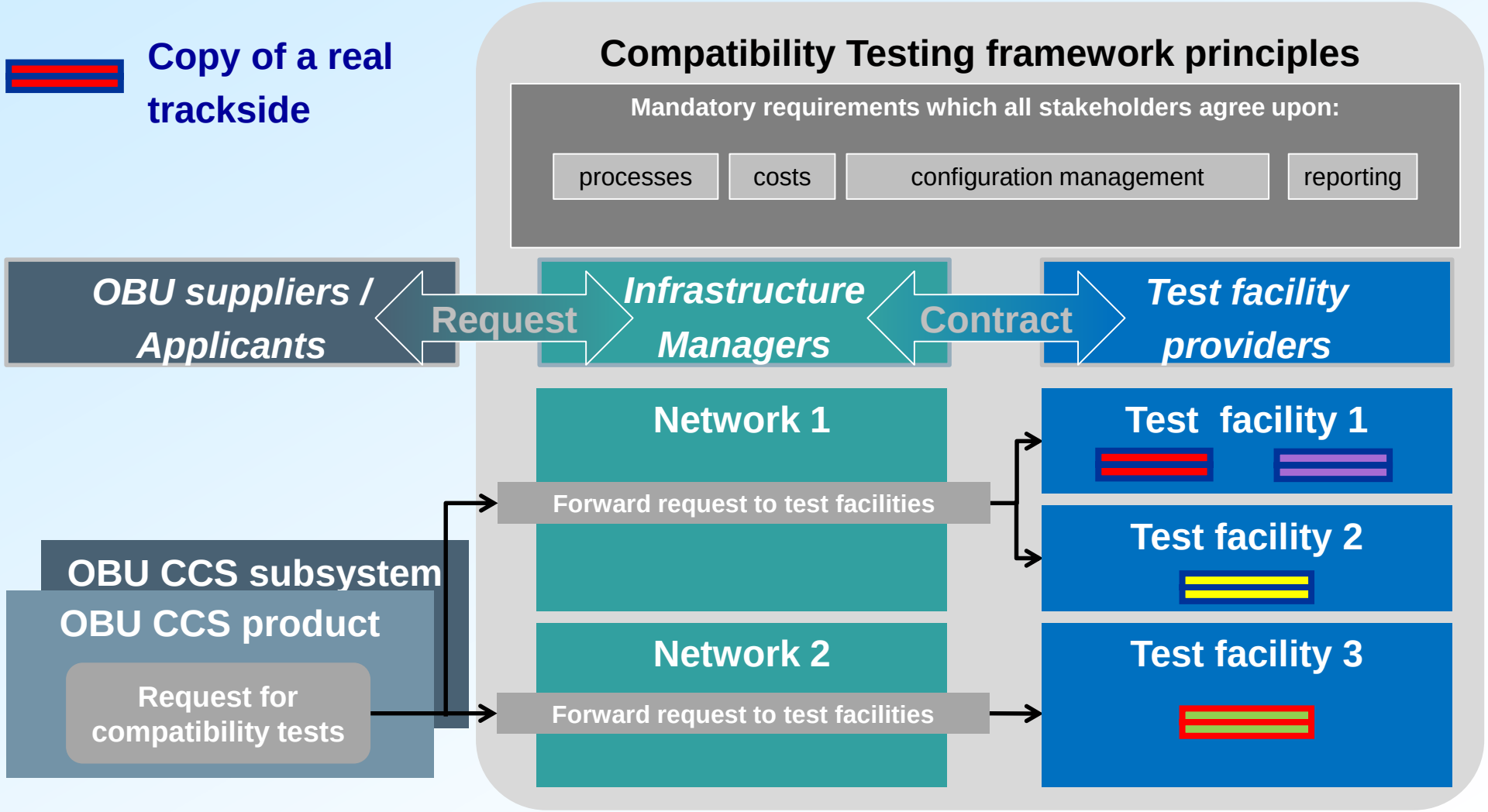


The ERTMS Platform Board decided to set-up a working group to propose an harmonised approach for compatibility testing to improve efficiency and predictability of ETCS approval

ETCS compatibility testing – preliminary results

- The T&V Sub-group of the ERTMS Platform analysed a number of real cases, considered the return of experience of the stakeholders, leading to some principles:
  - ✓ ETCS compatibility is based on the interaction among operational rules, engineering rules and product specific technical solutions of each ETCS on-board and each ETCS trackside supplier
  - ✓ The cooperation between OBU and trackside suppliers needs to be facilitated with the involvement of their customers
  - ✓ ERTMS stakeholders require the Infrastructure Managers to play a strong role in the ETCS compatibility approach

ETCS compatibility testing – process



Agenda

- ETCS compatibility testing
- **Re-authorization after modifications**
- Next steps

Re-authorization after modifications

Motivation:

- On-board CCS subsystems require re-authorization after almost every modification however small its significance or impact, involving NoBo/DeBo/ISA/AsBo and the NSAs.
- Time and costs of carrying out even a minor modification are substantial, and consequently activities to increase quality of the affected system slow down.

Re-authorization after modifications

Result:

- UNISIG members have elaborated conditions to classify a modification as **minor**.

- A **minor modification** will not require re-certification or re-authorization as it is defined as not having any impact on the basic design characteristics[1)] from the CCS point of view.

1) *Basic design characteristics are the basic parameters of the TSI CCS the interoperability constituent or subsystem is certified against*.

Re-authorization after modifications

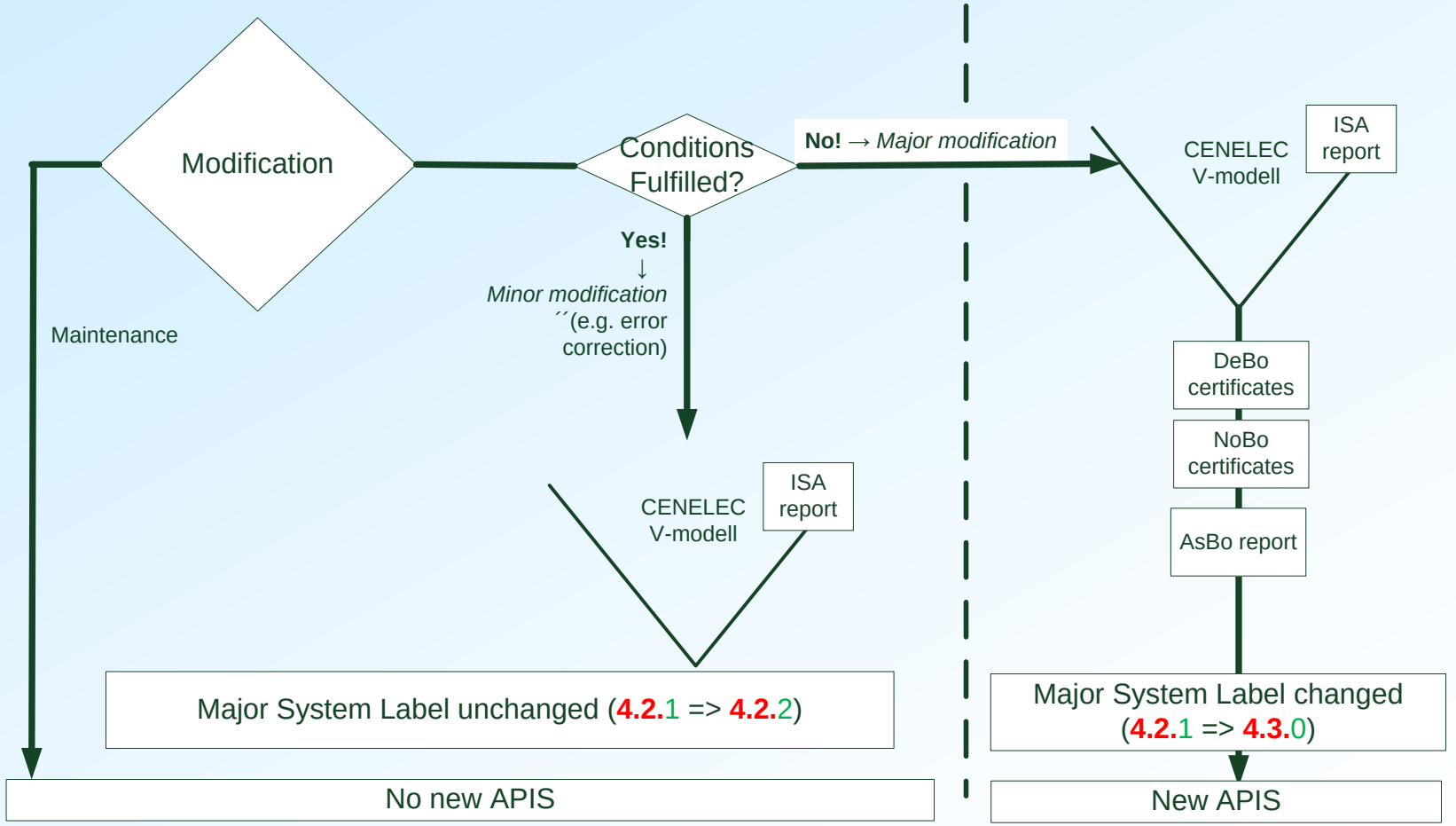
- The (sub-)system needs to be characterized with an identifier, distinguishing between a functional and a manufacturing part. Both parts are still distinguishable, after the system has been installed.
- Examples for conditions to declare a modification as **minor**:
  - *The target functionality (basic design characteristics) remains unchanged.*
  - *The functional part of the identifier has not been modified after the change.*

Example for a system identifier: **4.1,B**

Change does not require re-authorization

Change does require re-authorization

Re-authorization after modifications

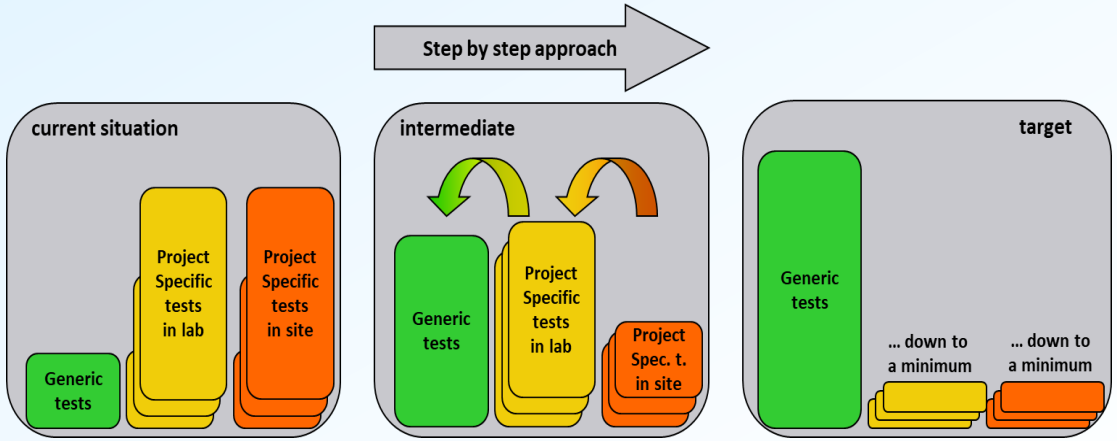


Agenda

- Re-authorization after modifications
- ETCS compatibility testing
- **Next steps**

Next steps

- Discussion of the proposals on-going with sector stakeholders
- Creation of detailed documents to substantiate the proposals
- Both proposals shall serve as a contribution for the TSI CCS amendment coming into force by April 2019
- … the target remains to minimize testing.



Thank you for your attention

www.unife.org

www.ertms.net

@UNIFE

@ERTMS