Telephone conferenc eon V&V Process Synchronization
openETCS TelCo

Marc Behrens

Version 01, 2013-03-26

Document Control

'OETCS_VV_Process_Synchronization_TelCo_Minutes_130326.tex'			
Version	**Date**	**Author**	**Changes/Comment**
01	2013-03-27	Marc Behrens	All sections
02	2013-03-28	Hardi Hungar	Slight revision

Organizational Data

Type of meeting	WebConf	
Start	2013-03-26	11:00
End	2013-03-26	12:45

Participant	**Organisation**
Baseliyos Jacob	DB
Hardi Hungar	DLR
Jan Welte	TU-BS
João Santos	Institut Telecom
Klaus-Rüdiger Hase	DB
Marc Behrens	DLR
Marielle Petit-Doche	Systerel
Merlin Pokam	AEbt

Agenda

Results

1 V&V Process Synchronization

1.1 Synchronization on Agenda

Description	T	Resp.
Decision on safety functions: The ones who start the model are responsible to identify the safety functions. **Comment** by M.Petit-Doche: Safety Analysis and preliminary Hazard analysis to be done. **Question** by B.Jacob: Who is in charge of the safety analysis? **Question** by B.Jacob: How big will the scope be of the safety issues? **Question** by K.-R.Hase: What is the scope of the SSRS? **Answer** by M.Petit-Doche: SSRS is the functional architecture view. **Question** by M.Petit-Doche: Onboard only scope of the project? **Answer** by K.-R.Hase: Trackside has to be respected. **Answer** by M.Behrens: Agree there should be a trackside model defined, see Subset-026-2.4. Trackside model should be used for data preparation of the use case scenarios and test cases. **Comment** by K.-R.Hase: Clear interfaces are very important. The interface has to be described in the formalisation. **Trackside Model** It was agreed on to separate the SSRS into trackside (smaller data-preparation model) and on-board side (bigger part)	F/D	Marc Behrens

1.2 V&V Process Synchronization

Description	T	Resp.

Description	T	Resp.
1. Each design artifact needs a reference artifact which it implements. e.g. code to detailed model, detailed model to SRS model. Each step has to be verified. Saying this artifact comes from this part of the model: Verification needs a reference of each artifact of what should be implemented. 2. The implementation relation shall be specified in detail, (e.g. for a state machine and a higher level state machine, a mapping of interfaces, states and transitions is required). This includes additional invariants, input assumptions and further restrictions. This information is the basis for verification activities. V&V needs detailed references on parts of the model which are implemented. Relation between these parts of the model is needed. e.g. states of the concrete model map in a specific state mapping. 3. The verifiability shall be incorporated within the model design. The same applies to the code. For the code, the standard (EN 50128) includes some explicit requirements for verifiability. Every designer has to keep verifiability in mind when performing some kind of implementation task. At the very least, she/he should be able to justify the correctness of the implementation step (otherwise, the verifyer will most probably not be able to do his/her job). In order for the verifier to stand a chance on verifying explicit requirements for e.g. code verification should be anticipated beginning modelling. 4. The findings from verification shall result in corrections. Results can be: a) things we cannot verify b) the verification is able to identify detailed defects. Issues are reported back to the designer and need to be discussed and/or corrected. This feedback process from V&V should be defined by WP4 and referenced in the QA-Plan. The design process should include its part of the feedback loop (clearing issues, correcting defects). **Comment** by M.Petit-Doche: Taking and checking the feedback from verification is a complex process. 5. Preliminary verification steps shall be performed and during model design and code development. Only stable code which passes basic functional tests, and only models which are reasonably consistent and complete and, if applicable, animated so that the main functions has been exercised should be the subject of a thorough verification. This is common practice as it is too costly to have a third party analyze an artifact which is most probably immature and buggy.	D	Marc Behrens, Hardi Hungar

Description	T	Resp.
Question by Agenda: What are the requirements from V&V influencing the other working streams and thus need to be predefined. **Answer** by Meeting: The process should be described by WP4 **Open questions** 1. Which parts of the process do we expect to be described within the requirements? 2. At what level does e.g. the V&V plan fill in?	D	Marc Behrens, Hardi Hungar

T for type of item:

A action item

D decision

F fact / finding

Notes

This format lacks references to ITEA 2 so far.

End of Document