Workshop on Safety Strategy
openETCS Meeting in Paris

Marc Behrens

Version 01, 2013-03-13

Document Control

'OETCS_SafetyStrategy_Workshop_Minutes_Paris_130313.tex'			
Version	**Date**	**Author**	**Changes/Comment**
01	2013-03-13	Marc Behrens	All sections
02	2013-03-27	Marc Behrens	Incorporating review from S.Baro to §2.3.2

Organizational Data

Type of meeting	Face2Face	
Start	2013-03-13	09:00
End	2013-03-13	12:00

Participant	**Organisation**
Armand Nachtef	CEA List
Baseliyos Jacob	DB
Cyril Cornu	All4tec
Frédérique Valée	All4tec
Jan Welte	TU-BS
Jens Gerlach	Fraunhofer
Klaus-Rüdiger Hase	DB
Marc Behrens	DLR
Martin Schröder	ERA
Merlin Pokam	AEbt
Pierre-François Jauquet	ALSTOM
Piero Petroccioli	UIC
Stephan Jagusch	AEbt
Sylvain Baro	SNCF

Agenda

Results

Description	T	Resp.
## 2.3 Global Safety Strategy ### 2.3.1 User story Internal-Assessor User Story of the Internal Assessor is presented by F. Valée **Question** by M.Schröder: Is the role separation mentioned in the TSI taken in account? **Answer** by J-F. Jauquet: There is also an Internal Assessor at ALSTOM. Everything needs to be analysied in detail. **Answer** by F. Valée: Issues need to be analysed as exhaustive as possible. **Question** by J. Welte: How do we want to handle the document, showing the status of the document being important for the safety case. **Conclusion** A report explaining all work being done containing global conclusion and displaying the conviction whould be done before intermediate report. Work needs to be done on safety requirements as input to further work.	F	Frédérique Valée

Description	T	Resp.
2.3.2 User Story SNCF User Story of SNCF is presented by S. Baro: a formal specification of Subset-026 b define (full) safety strategy complying to EN 50126, EN 50128, EN 50129 c provide tools chain on formal methods d apply safety strategy on a small part of the system (completely vertically on a small scale of the systrem) e provide executable sw spec, non vital **Question** by K.-R.Hase: Where are the resources for the additional goals coming from? **Answer** by S.Baro: For us, this is not a change of scope because we always understood that the scope of work included safety, considering in particular the number of times the word is used in the FPP. **Question** by J-F.Jauquet: What are the degraded mode on the test? – If the test does not support the degraded mode, the test model will never be taken. **Answer** by K.R.Hase: Not sure we can cover all of the degraded modes, e.g. failure modes result in degraded modes, in the project. **Comment** by P.Petruccioli: UIC: Fully in line point (b) but cannot understand why only limited to subset-026. In total there are more than 60 relevant documents for on-board inside the TSI with ANNEX A being the head document. further should be taken in account: • e.g. Subset-040 engineering rules, also a chapter for on-board • e.g. Subset-041 i.e. ch5 maximum response time, maximum delay of receiving a balise message and reporting the result on-board .... Final users are railway undertaking. The UIC is on the way to give official support to openETCS. **Comment** by P.-F.Jauquet: Performance of the basic functions is something very important e.g. performance of the odometry, you cannot decolourate the performance of the basic software and the performance of the functional software. **Question** by K.-R.Hase: Who will do the work on the safety issues? **Answer** by S.Baro: A sample of requirements will be chosen from Subset 91 by WP2. In my opinion, safety activities themselves were in the scope of WP4.	F	S.Baro

Description	T	Resp.
Question by K.-R.Hase: Who is doing the safety concept on system level? **Question** by P.-F.Jauquet: Who is defining the SSRS (WP2 or WP3?) **Answer** by S.Baro: Will be decided between WP2 and WP3. **Answer** by S.Baro: A proposed document on the safety already exists. **Answer** by J.Welte: Safety Issues should be defined very well in order to be taken by WP-4. **Answer** by S.Baro: SSRS is a huge task. SSRS is a semi formal architecture model. **Question** by M.Behrens: How is the SSRS coordinated between Semi-Formal Model and the architecture activities? **Answer** by S.Baro: TBD	F	Sylvain Baro
2.3.5 User Story ERA Do Impact Assessment on the Framework of ETCS Hans Bierlein - Dealing with certification • Interest to detect inconsistencies and errors inside the specification • Analyse Impact of the proposed solutions of change requests Baselines existing BL2, BL3 How would the system react integrating a change How is Backwards compatibility dealt with CH6 Subset-026 - we need support here: Idea compatibility matrix: What is the behaviour and what are the combinations and how to deal with it Hans Bierlein is dealing with testing Are we sure the formal model realy is in line with the test specification Support: Is our test specificaiton well, how can we improve it Support is needed Unfortunaly the ERA project formalizating the Subset-026 was dropped to be completed Feedback: Approach of SNCF going into the right direction	F	Martin Schröder

Description	T	Resp.
2.3.3 User story DB The DB user story is presented by K.-R. Hase. a) formal specification Comment Klaus: Does not mean the other subsets are out b) executing non-vital reference device c) tools chain supporting (a) and (b) including generation of code, test cases and documentation. d) Subset of the model is subject to safety assessment meeting EN 50128 requirements **Question** by P.Petroccioli: Will information be lost, will it be consistant? **Answer** by J.Welte: Tools will support, no push button approach expected. Fully formal specification used to proof properties. **Comment** by J.Gerlach: The pie diagram on the modelling method should be degree of verification. Evidence that the Strictly-Formal-Model complies to the Semi-Formal-Model is very different to do. The code is outside of the safety demonstration.	F	Klaus-Rüdiger Hase

Description	T	Resp.
2.3.4 User Story UIC The UIC user story is presented by P.Petruccioli. EIRENE Specification totally managed by UIC UIC would like to support openETCS as long as the conditions (see presentation) are fulfilled. **Question** by K.-R.Hase: Idea of reference for certification? **Answer** by P.Petruccioli: Idea of the golden on-board to be used at European level, a real train with such a device supported able to run at a certain line which has been pre-qualified at the labs by tests with such a 'golden on-baord vehicle' is similar with the reference to the original meter. Idea: The on-board should react in the worst timely manner. Expect: For the OBU to react in the worst possible way to be able to fully test the trackside. **Answer** by K.-R.Hase: This is an Error detection device, more than a golden devic **Comment** by P.Petruccioli: Designer Choices should be avoided thus to make a process for designer choices to have a common development.	F	Piero Petruccioli

Description	T	Resp.
2.3.6 Conclusion **User story Internal-Assessor** agreed on **Userstory SNCF** • *Work on safety requirements* is written within WP2 • *Work on SSRS* to be defined between WP2 and WP3 • *Definition of safety relevant SSRS* to be defined between WP2 and WP3 and WP4 • *Work on safety model* done within WP2/3 • *Work on safety verification* done within WP4 • *preliminary requirements* released planned by SNCF at end of March **Userstory ERA** • *Regular update of openETCS to Mr. Bierlein* planned • *Issues found on Subset-026* should be communicated via the representative sector organization CER, EIM and UNISIG (do not send the issues directly to ERA) • *Licence of ERA specification BL3 to reuse inside openETCS* Marc sends a question to Mr. Schröder and it will be provided to the legal services inside ERA • *Operational Scenarios* Baseliyos: Checks with Angelo Chiappini if member states already notified to ERA - on what installed on the trackside see additional at RINF (Register of Infrastucture) Database , UIC Database MERITS **Userstory DB** agreed on **Userstory UIC** agreed on	D	Marc Behrens

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