Workshop on Safety Strategy
openETCS Meeting in Paris

Marc Behrens

Version 01, 2013-03-13

Document Control

OETCS_SafetyStrategy_Workshop_Minutes_Paris_130312.tex			
Version	**Date**	**Author**	**Changes/Comment**
01	2013-03-13	Behrens	All sections

Organizational Data

Type of meeting	Face2Face	
Start	2013-03-12	09:00
End	2013-03-12	17:30

Participant	**Organisation**
Armand Nachtef	CEA List
Baseliyos Jacob	DB
Cyril Cornu	All4tec
David Mentré	Mitsubishi Electric
Frédérique Valée	All4tec
Jan Welte	TU-BS
Jens Gerlach	Fraunhofer FOKUS
Klaus-Rüdiger Hase	DB
Luis-Fernando Mejih	ALSTOM BE
Marc Behrens	DLR
Marielle Petit-Doche	Systerel
Martin Schröder	ERA
Merlin Pokam	AEbt
Pierre-François Jauquet	ALSTOM BE
Ralf Pinger	Siemens
Renaud De Landtsheer	ALSTOM BE
Stan Pinte	ERTMS Solutions
Stephan Jagusch	AEbt
Sylvain Baro	SNCF

Agenda

Results

Description	T	Resp.
2.1 Workshop on Safety Strategy concerning Methods and Process K.-R. Hase: Project Goal Priority 1^{st} formal (or semiformal spec) specification of (step better than that what we have today) focus: formalize Subset-026 on-board unit part 2^{nd} tool's chain (to use formal spec and software generation) 3^{rd} running model 4^{th} tool's chain certifiable (what is the constraint on the tool's chain/ continuously) 5^{th} (inofficial) certifiable model Validation of the specification is planned by means of tests. K.-R. Hase: Project Goal in Steps 1. Formalize Prose (used to after generate code) 2a. formal system 2. Formal Language 3. SW Generator comment: 1.-3. are the main objectives of the project 4. Formalize the Test cases 5. closing the loop from 2 to 5 6. closing the loop from 2a to 6 7. insert code in EVC 8. Safety platform provided by industry **Comment** by F.Valé: For safety reasons operational rules are needed **2.1.1 Splitting up in 2 Groups : Methods and Process**	D & F	Klaus-Rüdieger Hase Marielle Petit-Doche Marc Behrens

Description	T	Resp.
2.2 Workgroup to define user stories on Safety Strategy on Methods	F	Renaud, Marielle, David, Pierre-François, Jens, Sylvain, Stan, Klaus-Rüdiger, Luis-Fernando, Stephan
2.2.1 Workgroup to define user stories on Safety Strategy on Process For a better understanding the process shoukd be classification into: • *Tools* development process concerning the tool chain • *Application* development process concerning the EVC application (application = model and executable model) Steps that should be defined while describing the process: 1. Choose use case 2. Pick tools 3. Get tools implemented 4. Collect all information available With the fully executable functional model ambiguities should be disposed. Different operational rules have to be respected to be applicable in different countries. Use cases should be taken from DB and SNCF possibilities could be: • Germany: VDE 8 - Verkehrsprojekte Deutsche Einheit • Netherlands: Betuwe line • France: who can provide a use case? Are BL3 Use cases available?	F	Frederique, Armand, Cyril, Jan, Merlin, Baseliyos, Marc, Ralf

Description	T	Resp.
2.2.2 Open debate & decision on Methods user story SRS → Semi-Formal-Model → Striclty-Formal-Model The model should be designed for verification. Result: Choose semi formal approach and strictly formal approach. To define clear rules for strictly formal models the following should be respected: • rules from strictly-formal model to the modernization • feedback from strictly-formal model to semi-formal model • (rules) to translate SRS to semi-formal model • coming from semi-formal to a formal model Info: Architectural decisions already taken at a semi-formal level Decision affirmed on way ahead to model and Jens will sum it up and put it on Github	D	Jens Gerlach
2.2.6 Presentation of workshop results on Process 3.x Use cases are not yet real in operation Results see presentation. **Question** by : Which operating Rules are we talking about? **Answer** by : Betuweroute & VDE 8 are proposed within the FPP **Question** by Session Participants: open Point: Do we need Aim 4 and if yes who will define the safety strategy If Safety considered you have to put it on top –¿ Is safety considered?	D	Merlin Pokam

Description	T	Resp.
2.2.7 Open debate & decision on Process user story Project has to deliver otherwise the project is failed We can not guarantee that we have a certifiable toolchain/ model But we can ... **Question** by M.Behrens: Who identifies the subset to make an assessment on it? Proposition: Mid of April (Workshop) - What is the requirement on which we will focus the safety demonstration of the tool's chain **Comment** by S.Baro & P.-F. Jauquet: Decision: Model as much as possible /all of the OBU and then try to do the whole safety activities on a small part of the subset. For which the tool chain a nd process are compliant. **Comment** by P.-F. Jauquet: WP3 takes a small part of the model out of the tool evaluation project to evaluate the safety model. Focus: Only the semi-final model should be safety certifiable. Decision:Safety proof will be done on semi- formal model Decision: Code Generation taking out of safety strategy No T3 Code generator in focus	F	Cyril Cornu
2.3 Follow-up user stories **2.3.1 Usage of openETCS-tools for development of ETCS on-board** Siemens would like to integrate to whatever comes out of openETCS. Formalization means lots of manual effort. The right hand of the V-cycle can be used for conformance testing. Tool qualification T1 or T2 should be needed for right hand V-cycle (CENELEC EN50128 CH6.7) Siemens would like to contribute to SIL-4 certifiable code. Risk & Hazard analysis, competence management needed in parallel for SIL-4 developement. For Siemens the best contribution would be to having the openETCS results at the left part of the V-cycle. Agreement on the Test-API Testing interfaces for testing (e.g. DMI) Chance to agree on a Test-API : Siemens could contribute there. ⇒ Left hand side of the V: executable SIL4 is very ambitous ⇒ Tool it makes sense to start a light tool.	F	Ralf Pinger

Description	T	Resp.
2.3.2 V&V Strategy and Scrum User Story of the Verificator is presented by M. Behrens Each user story has to fulfil the acceptance criteria and be testable.	F	Marc Behrens
2.3.3 Verification of code and API Results see presentation. It is important to investigate several properties to be formalized. Properties may come directly from the SRS or the API. e.g. integers are in a certain bounds, pointer always allocated, e.g. all integrer operation in the implementation never overflows, time constraints Different properties to be verified to what extend they can contribute to a high level of assurance. Pie diagrams in green and red within the model says: Real time property of the executable code can probably not mathematically verified.	F	Jens Gerlach
2.3.4 Project-, QA-Plan and Scrum Questions and answers see presentation. Presenting of project plan. Decision was voted to call a PCC meeting. Within the next PCC meeting Backlog is a tasklist and the product-owner of the backlog are the WP leader or Taskleader. For each task we have a backlog. The tool Jira with Greenhopper is currently in evaluation (for distributed Scrum teams).	F	Baseliyos Jacob

Description	T	Resp.
2.3.5 Conclusion The following decisions were agreed on: **4 goals** for the project have been defined: 1^{st} **priority:** semi-formal (or formal) specification (step better than that what we have today) with the focus on: formalizing subset-026 on-board unit aim: 100% 2^{nd} **priority** tool's chain (to use formal spec and software generation) aim: 100% 3^{rd} **priority:** running model aim: 100% 4^{th} **priority:** tool's chain certifiable (what is the constraint on the tool's chain/ continuity) aim: for validation of the safety strategy **Method** A development method integrating the following artifacts is foreseen: • SRS • Semi-Formal Model • Strictly-Formal Model • Running Software Model **Process** As a basis to evaluate the results for functional as well as safety reasons *Use Cases on Operational Basis* should be identified. It was agreed that within the project *safety does not touch code generation.* A small subset should be identified for the safety case. **Qualification of openETCS tools** is recommended to be started on the *Right Side of the V-Cycle* (T1, T2). After this qualification has proven in use the qualification for the *Left Side of the V-Cycle* is advised (depending on the 4th priority) (T3). **V&V SCRUM process** [based on user story] The user story, respecting the acceptance criteria, has to be testable within a defined timeslot **API Verification** [focus on the] different properties to be verified to what extend they can contribute to a high level of assurance **project plan** [Project Plan]proposed [PCC] meeting is voted on, the PCC will be planned around next month's in Munich [Releaseplan] is to be defined by the producttowner e.g. Task leader, WP-L [QA-Plan] is worked on currently [scrum] more scrum training for people is identified	D	Marc Behrens

Description	**T**	**Resp.**

T for type of item:

A action item

D decision

F fact / finding

Notes

There may be more elaorate formats for protocols. This format lacks references to ITEA 2 so far.

End of Document