Workshop on Safety Strategy
openETCS Meeting in Paris

Marc Behrens

Version 01, 2013-03-11

Document Control

OETCS_SafetyStrategy_Workshop_Minutes_Paris_130311.tex			
Version	**Date**	**Author**	**Changes/Comment**
01	2013-03-11	Behrens	All sections

Organizational Data

Type of meeting	Face2Face	
Start	2013-03-11	13:30
End	2013-03-11	19:00

Participant	**Organisation**
Baseliyos Jacob	DB
Cyril Corny	All4Tec
David Mentré	Mitsubishi Electric
Grégory Guillaume	Alstom
Jan Welte	TU-BS
Jens Gerlach	Fraunhofer FOCUS
Klaus-Rüdiger Hase	DB
Luis-Fernando Mejia	Alstom
Marc Behrens	DLR
Marielle Petit-Doche	Systerel
Merlin Pokam	AEbt
Patrick Deutsch	ERSA
Piero Petruccioli	UIC
Pierre-François Jauquet	Alstom
Renaud De Landtsheer	ALSTOM
Stan Pinte	ERTMS Solutions
Stephan Jagusch	AEbt
Sylvain Baro	SNCF

Agenda

Results

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

Description	T	Resp.
# 1 Review of the openETCS Requirements	F	Pierre-François Jauquet
## 1.1 API Requirements		
### 1.1.1 Presentation API		
The API is presented describing e.g.:		
BsW Basic Software of the ETCS unit.		
Tolerance of generally 100ms is anticipated inside the software call (not the timestamp)		
Test service Contains i.e. end of power-up system test → which service is available		
MMU Movement Management Unit Position / Coordinate: Low, nominal and upper uncertainty (LNU) applying e.g. to Speed (LNU), Acceleration (LNU), Motion State, Motion Direction. ⇒ due to time passed between processing and availability of data ... everything has to be saved with the time stamp in order to use time-correction-algorithms		
BTM Recording timestamped balise-center-location in order to recalculate the position based on the time passed between availability of balise signal and the time data is processed. Weiting BTM Antenna- Information to write error messages.		
RTM On-Board Master of radio communication. Information about e.g. radio holes have to be provided.		
MMI Man Machine Interface shows and writes data .		
STM Interface to STM: read, write and queue data		
TIU Managing connection, and maintain connections and keep alive. If TIU connection is not maintained, an error has to be thrown. ⇒ safety related!		
LLRU lowest level replaceable unit e.g. Board at the OBU (replaceable, repairable unit) info to reset, request (e.g. 50 LRU, eg. 20 high level LLRU)		
Packet_44 transferred through serial interface (Interchange between Balise → EVC → specific STM)		

Description	T	Resp.
LOOP Messages from Loop **KM** Key management is not in focus of openETCS. **EB** Emergency Break in focus. **Principle Fault reporting** BsW is responsible to take appropriate action in case of error i.e. [-] Write error [-] Trigger EB [-] Shutdown of system **Data Monitoring System** recording all system data. **Question** : Why is the system time stamped? **Answer** by P.-F.Jauquet: Importance to services to define accuracy of the time. Also having influence to what can be the maximum speed of the line. When you are specifying the interface, you are talking about safety.	F	Pierre-François Jauquet
1.1.2 Proposition on abstract API Presenting WP 5 Input for abstract API. **Demonstrator code** is written in C. **Data exchanged** on high level should be described in the high level requirement document. **Odometry** of WP 5 Input for abstract API relates to MMU of ALSTOM. **Radio Service primitives** should be included inside the model. **Question** by P.Deutsch: Does the basic software (BsW) decribe the primitives? **TIU** Subset-121 defining the TIU released by UNISIG (UNISIG activity) opinion: TIU should to be as general as possible **DMI** described in a separate subset.	F	Patrick Deutsch

Description	T	Resp.
1.1.3 Questions and/or Comments & Responses **Question** by S.Pinte: Which format are the messages sent to BTM/ RTM? **Answer** by G.Guillaume: Binary messages/ bit encoding of the application is inside of the application (Decoding tool not part of the application, can be excluded). **Question** by S.Baro: Do we want to stick to the product or to stay on a high level description? Cycle wise logic to be hard coded or to leave open the possibility to have a driven interface? Work should be done refining on interface to drive it on a higher level? **Answer** by P.-F.Jauquet: We can have a high level abstraction of the API. **Question** by D.Mentré: Does the abstract model describe the dynamics of the API? **Answer** by P.-F.Jauquet: It describes good use rules to be modelled! **Question** : How can we integrate the real time constraint on safety impact? **Answer** by P.-F.Jauquet: You need an idea of distance which could have been travelled. Time delay as low as possible to be accuracy has to be as high as possible. All main functions of ERTMS are related to the train location. Uncertainty of train position caused to e.g. slippery phenomena. **Question** by K.-R.Hase: Reliable Data on train position depend also on weather condition? **Answer** by P.-F.Jauquet: Physical position correction regarded as black box. **Question** by L.-F.Mejia: Does the BsW comply to SIL-4 SW? **Answer** by G.Guillaume: Yes, except that there is no 2 out of 3 on BsW level. **Question** : Is BsW an operational system? Will terms be described in the API document? **Answer** by P.-F.Jauquet: Also management of different peripheral interface ie. physical sensor. Ok Terms will be described! **Question** : Which Services are called by the Basic Software? **Answer** by P.-F.Jauquet: BsW as global scheduler and calls underlying SW modules. **Question** : Document format? **Answer** by P.-F.Jauquet: To be evaluated. **Question** : Timestamp **Answer** by P.-F.Jauquet: Time dependency managed. Correction about information reviewed. Correction of position should be done before providing the position to the application. **Question** : How will the patency of the SSRS to the design model be? (WP2 issue)	F	Pierre-François Jauquet

Description	T	Resp.
1.1.4 Conclusion • Review cycle of the documents will be done using the format used in WP2 (XML Excel file). • Formal review of the documents will be done. • The questions to the API document will be answered using 'yes' or 'no' and giving justification. • Review of document will be done after answering (Timeline proposed to be discussed on Friday - give commands in one week, answer within 2 weeks). • Aim is to have API to be completely free of problems in terms of interfaces and operating system.	F	Pierre-François Jauquet

Description	T	Resp.
1.2 Open Issues on Requirements	F	S.Baro
1.2.1 SubSystem Requirement Specification		
Presentation: Going from the SRS to the formal model via the SSRS Proposing SubSystem Requirements (SSRS) as functional architecture in order to ... ... help functional testing. ... have Sub- Boundaries. **SSRS** **consists of** Boxes, Arrows and named I/O Streams **unambiguously** naming objects and I/O **enables Requirements** to be kept in natural language **pro** modularity at function level clarify the architecture **con** introduces another level of natural language **Other solution** could be to model directly from SRS to ease traceability and provide meta/data in the model(e.g. vital/ non vital). **Question** by M.Behrens: Does the SSRS have an influence on the API? **Answer** by P.-F.Jauquet: No. **Comment** by L.-F.Mejia: The SSRS defines the functional architecture. The API should comply the Archiretural Design. **Answer** by P.-F.Jauquet: The SSRS should be part of the WP2, not WP3.SSRS is very useful but part of the specification. • Assumption: For WP3 SSRS should be part of the OBU specification on System Model • WP2 should define what is the scope of the modelling **Question** by P.-F.Jauquet: Where will the SSRS be done? What ware we expecting in SSRS and in Detailed design? **Answer** by S.Baro: Open, to be discussed between (→ WP2/ WP3) **Comment** by S.Jagusch: Drawing a picture of the Y-Cycle stating that V-Cycle can be merged at the bottom by certified tools. The standard puts the CENELEC V-Cycle as a suggestion. When the formal methods come to the assessment there will be many questions to be answered.		

Description	**T**	**Resp.**
Question : Why is formalisation changing the game? **Answer** by S.Jagusch: In the model you cannot clearly divide the Architecture and detailed design(see scade). Component design and architecture melts together. **Question** : Do we do SSRS? **Answer** by P.-F.Jauquet: Yes SSRS is needed but WP2 should define it!!	F	Sylvain Baro

Description	T	Resp.
1.2.2 Process/Methodology - What we want to do - How We do It (Design Process) - Choose Means to do it (Tools) **Question** by M.Petit-Doche: Clarify the aim of the Project. • To define the system is out of the scope of EN 50129 (it is EN50129) • define formates to exchange information between activities **Color coding** of presentation: blue $\hat{=}$ design green $\hat{=}$ safety yellow $\hat{=}$ validation red $\hat{=}$ verification **Specifications** relevant for openETCS • System Requirements Specification: Subset-026 • System Safety Requirement Specification: Subset-091 **Verification** is needed in each phase to have an assessment. **Means** How to Design? **Language and output** chosen has to be justified. **At each software phase** we should have a set of methods following the main objectives of the standards **EN 50128 §6.7.1** For each tool we have to justify why we use it for which purpose and when. **Justification** is needed for each part of the tool's chain ⇒ lots of documents **Qualifying tools** you need to make a verification on the output Hard to get e.g. Eclipse / LaTeX qualified for T3 **Question** by R.De Landtheer: Is B-Development based on Eclipse? **Answer** by M.Petit-Doche: No. **Question** : How to define the openETCS design process? **Question** by M.Petit-Doche: Do we need an openETCS process with phases as described in EN50128, EN50129, EN50126? **Answer** by S.Jagusch: Needs to be put down in quality plan, you do not necessarily need to follow the example described within the CENELEC but you need to use the Methods described.	F	Marielle Petit-Doche

Description	**T**	**Resp.**
Question by P.-F.Jauquet: Model Developed validated and tested. How can I be sure that the tool platform can be used to demonstrate the model is compliant with the behaviour to be expected? **Question** by P.-F.Jauquet: After being compliant it is necessary to have the safety analysis? **Question** by P.-F.Jauquet: Safety demonstration of the model or safety demonstration of the platform to be demonstrated? **Question** by P.-F.Jauquet: What is our safety strategy to be sure that these platform can be used within any system? **Question** by P.-F.Jauquet: What is the safety strategy for: - the guy for the modelling? - the tool platform? **Question** by M.Petit-Doche: Which Which phases have to been included in OpenETCS design process? **Question** by M.Petit-Doche: Which interaction between design and verification and validation? **Question** by M.Petit-Doche: Which means and languages to develop a OBU? **Question** by M.Petit-Doche: Which tools to support openETCS design process?	T	Marielle Petit-Doche

Description	T	Resp.
	F	Stan Pinte
1.2.4 Full Model or full Compliance		
User Story 1 Formalize Subset-026 OBU part customer: ERA		
User Story 2 Use OpenETCS model as a shadow EVC customer: Railway operators **Comment** by S.Pinte: Use openETCS model in V-Cycle right branch: They need a white box, full reasoning tree.		
Question by P.-F.Jauquet: Is a spying interface needed? **Answer** by S.Pinte: They need white box view.		
User Story 3 Use OpenETCS model in V-cycle right branch customer: OBU supplier **Comment** by S.Pinte: How to reuse the model: if it is complete it is of more value!		
User Story 4 Make sure money is well spent in OpenETCS project customer: Brussels region **Comment** by S.Pinte: Calculating to model 100% of Subset-26 within 2 man-years.		
Conclusion openETCS must deliver a complete model		

Description	**T**	**Resp.**
Presentation of project goals Presentation of DB user story **Comment** by M.Petit-Doche: If the aim of the project is a T3 qualified tool's chain the tool's chain does not need to be SIL-4. **Question** by P.Piero Petruccioli: Which product and which system are we talking about? UIC is fully interested in having the formal specification of the system. **Comment** by S.Jagusch: The V-Cycle is not mandatory, see EN 50128 §5.3.2.15. **Question** by P.-F.Jauquet: Why are they using the V-Cycle? **Answer** by S.Jagusch: V-Cycle is used by the manufacturer to give evidence to the ISA. **Comment** by S.Pinte: We need to have the complete model and to have the time to do it. **Question** : Do we have enough time to do all 3 goals of the and what are the priorities? Explanation from WP1 needed. **Question** : Do we model the complete subset-026? **Comment** by S.Pinte: We need a full model!	F	Klaus-Rüdiger Hase

Description	T	Resp.
1.2.5 Classification of Formal Methods & Tools Presenting the classification of formal methods and tools. **Question** : Is the mathematical model formal enough? **semi-formal model** has rigorous syntax but informal semantics **Comment** by D.Mentré: ERTMS Formal Spec can be formalized. **Model checking** of conc./ synch. languages **temporal logic** = next state or states in future compared to real time is i.e. the next state within e.g. 15ms **Static analysis** of software code (abstract interpretation) **use of formal methods** check a model/software verifies properties **Subset-26** is very rich regarding data description. **Model structure** should be used to break down and reuse parts in different software. **Properties** should be extracted by Subset-026 **Subset of performance** does need to be respected. **Incremental development** Refinement **Comment** : Matlab, Polyspace is more sxpensive then 5k€. **Comment** : Topcased will merge to Polaris. • Due to limit to formal verification is very hard to do mathematical verification on a complex model. • Power PC/Arm certified compiler free for non commercial use exist. • Test, review and animation used on high level from susbsystem validation **SCADE** : Formal tools for model and not formal verification!!!! (only model checking techniques are formal) Clear methodology how to use verification when there are model checker **Question** : Which are the steps of the process? → WP2 **Comment** by L.-F. Mejia: Model review is best thing. You can check the model partially by simulation. ⇒ Simulate the formal models: Proof will disclose the holes, possible not 100% because in the informal models there are assumptions that are hidden. You cannot prove that the model is complete. Examples: CBTC Asltom and Siemens France; RATP introduced formal models for the verification. **Question** by P.-F.Jauquet: You need to define the safety properties. How is it possible to verify in safety our safety properties?	F	David Mentré

Description	T	Resp.
Question : Which properties need to be considered? → WP2 **Question** : Which single language and tools in which step of the process are needed? → WP3 + WP7 **Comment** : (ISA) ≙ Independent Safety Assessor	F	David Mentré
1.2.6 Formal methods & Safety limitation and/or concerns Model: "Only one train on the bridge" Event-B single (single event) Limitation There is no explanation in case that e.g. a failure was never found. Goal Diagram - Free formalizes. Engineer the model for Verification will make the model hard for code generation Validate you model for vacuity and emptiness before any proof can be considered valid –¿ Simulation: You have to show that the model is not empty e.g. by simulation soundness: there are some some unsound tools Bounded verification is unsound/ unsound claim completeness: tool has to comply Safety Argument relying on formal proof as well as a watchdog **Comment** by L.-F.Mejia: Use B-Method avoid some kind of software errors. They do not claim that B-Model guarantees safety? They do claim that the software does not have systematic errors. **Comment** : Very few safety model exist, (they did not succeed yet). **Question** by S.Jagusch: Difference between Software and System Development (50128 50129 50126) regarded? **Answer** by M.Petit-Doche: Yes **Question** by S.Pinte: Who defines Safety Invariants? **Answer** by S.Baro: System development properties to be written down and model them on a complete specification. **Question** : Where do safety requirements come from? **Comment** by P.-F.Jauquet: Safety Strategy is needed. **Comment** by J.Gerlach: There is in the avionics e.g. DO 330 333 where tools are considered. **Question** : Methods in other domains are not yet covered in the state-of-the-art report. Will they be included? **Question** : What will be the full SIL-4 safety property and to be brought from higher to lower level?	F	Renaud De Landtsheer

Description	T	Resp.
	F	Jan Welte

1.2.3 Safety Activities

Comment by K.-R.Hase: The complete safety case was never in the scope !!! E.g. aviation shortens time from the time the change is introduced to the time of deployment because they have formalized a specification, they have provided a tool's chain with strong confidence that the tool's chain is correct. Through the project we want to have correct implementation but not a safety implementation.

Question by S.Baro: Why should the tool's chain be certifiable in EN 50128?
Answer by K.-R.Hase: The idea is to qualify the tool's chain for later reuse.

Question : If you safety certify the tools, what is the objective?
Answer : open

Question : Is safety certification according to ISO-26262 out of context?
Comment by J.Welte: There is no open licensed certified tool's chain.
Comment by P.-F.Jauquet: If we cannot build a safety strategy it is impossible to safety certify the tools.

CENELEC For each tool in class T3 it is required that the output and failures are detected.

Decision If you do not test your tool on a real case / part of a real case /SIL-4 Development you cannot say that the tool is fit for development.

Question : If we want to qualify the tool with the model we need a model safety certified for a tool's chain?

Question : Should functional safety properties or EN 50128 properties be met?
Comment by M.Petit-Doche: Usually we do not prove safety properties by a model.

Question by S.Baro: Which types of safety properties should be shown?

1. Defining the sample tasks → WP2

2. Answering the question who will perform the safety activities → WP1

Description	**T**	**Resp.**
1.2.7 Conclusion Main open point for tomorrow: Safety Strategy Work on it on what part of the strategy ⇒ depending on the process.	D	Sylvain Baro

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