Protocol openETCS Internal Assessment Workshop

Hardi Hungar

Version 01, 20140218

Abstract

Document Control

PR_TS_IntrnlAssssmnt_140218_01.tex			
Version	**Date**	**Changes**	**Comment**
01	140218	All sections	Initial

Meeting Data

Start	140218	13:00
End	140219	15:00

Participant	**Initials**	**Institution**	**Position**
Jan Welte	JW	TU-BS	
Hansjrg Manz	HM	TU-BS	
Hardi Hungar	HH	DLR	
Izaskun de la Torre	IT	SQS	
Marc Behrens	MB	DLR	
Norbert Schfer	NS	AEbt	
Stefan Jagusch	SJ	AEbt	
Jens Gerlach	JG	Fraunhofer	
Ralf Pinger	RP	Siemens	
Luca Macchi	LM	RINA	
Frédérique Vallée	FV	All4TEC	
Anthony Faucogney	AF	All4TEC	
Bernd Hekele	BH	DB	
Klaus-Rdiger Hase	KRH	DB	

Day 1 (18.02.2014)

1 Safety and Process

1.1 Safety Activities (JW)

- Safety is a system property—the SW itself cannot be declared "safe" unless put into relation with the HW.
- The hazard list plays an important role in all safety activities
- The safety activities are tied to the artefacts produced—the parts of the design, their verification and validation.
- The safety case shall be written in Goal Structure Notation (GSN), linking the evidence.
-

1.2 Current State SSRS (System Analysis—JW)

- Table of System Functions
- Evaluation of function description in Subset 026—is it sufficient to start modeling (usually not)
- Two functions selected: Within train location functionality
  - read balise message
  - ¿which?
- Detail by sketching a SysML (Papyrus) model

1.3 Safety Analysis Approach

- Demonstration on Siemens design part (Management of Radio Communication)
- Hazard Identification performed
- FMEA performed, 18 safety criteria defined (text table), established tracing to Subsert 026
- **Preliminary conlcusion**: This approach will take up more ressources than available if pursued.

1.4 The openETCS Process (Bernd Hekele)

- Important Links
  - Development Process (aligned with Eclipse

  - Quality plan
  - ...
  - ...

- Make use and unify several different skills and approaches in openETCS
- Whole process: A standard V development process, but:
  - It defines an ideal final outcome of the development activities (which cannot be achieved with the project resources)
  - it does not (and cannot, as it defines the final outcome) the way to get there. This can be roughly seen from the WP 3 backlog.
  - First, the process will be instantiated for some small part of the funcitonality, from SSRS down to the SCADE model and including V&V
  - Then, this willbe iterated for a larger functionality chunk
  - There will be by mid 2014 a detailed version of the modeling work plan (building on Alstom's legacy)
- Agile/SCRUM work organisation—this is not in line with the "usual" CENELEC development approaches. But it is faster in progress and permits retargeting during development (which by chance fits well the needs of the project which has not got the time to first stabilize requirements)
- **FV:** We have a problem in the project, because Subset 026 does not suffice as a specification and more or less everybody in the project is waiting on the SSRS. At the moment, the internal assessment cannot progress any further.
- **NS:** There are too many processes in openETCS, and they are not consistent. **BH:** Quality is maybe more of a concern, with a highly diverse project team. **SJ:** AeBt did not encounter any agile development in practice. **LM:** In the end, one has to demonstrate that the requirements are met. **AF:** There was already some successful agile development (DO178).

2 Documents Assessed

2.1 QA Plan (IdlT)

- In the current (2014-02-18) version of the QA plan, five issues raised in the internal assessment have been fixed. The other issues cannot be fixed at the current state of the project.
- The life cycle description needs some refinement lateron.
- Roles and independence too.
- As methods and tools are not yet selected, the choice can currently not be justified (what would need to be done in the QA plan)

- The same applies to many other issues

NS: There is just one standard to observe: CENELEC 50128:2011. This standard is rather general, According to the CENELEC, several plans need to be written. Each one should name the documents to produce, later the authors. These plans should be specific, clear in stating what has to be done and by whom, and very detailed.

3 Internal Assessment (FV)

- The main problem was that there was no project to assess
- Five documents were assessed. For each, the quality was assessed and recommendations wrt. achieve CENELEC conformance
- Doceument control process ok
- Revision and review process considered out of scope
- QA plan considered insufficient.
  - It does not include the lifecycle (the V lifecycle which is to be considered as the end result, just produced in an agile way).
  - The safety plan should be included/referenced by the QA plan, but there was none at that time.
  - The tools, even if no final decision has been taken, can be described.
  - The models built and verification attempts are interesting, but it is not clear how they will ever grow to something coherent
- The SCMP and the CPMP have been written by different organisations without the necessary coordination
  - The SCMP is generally acceptable, but needs to be reconciled with the CENELEC in some places, and it needs to be instantiated to the project.
- **JW:** How to proceed with the safety plan? **FV:** The documents should be defined in the QA plan. How to produce them is part of the safety plan.
- In the QA plan, the methods and techniques chosen for design and V&V activities are to be listed. The justification for the selection has to be elsewhere (eg, the safet. Currently, one could try to name the ones responsible for the selection.

3.1 Internal Assessment Summary (SJ, MB)

- **SJ:** The planning documents need input from the WPs, and the WPs need guidance from someone to plan the project.

- **HH:** Usually, there should be a small group of informed people taking the main decision and detail the plan to a degree that different approaches roughly fit in (bottom-up).
- **FV:** It is not possible to assess many different approaches.
- There is the Papyrus/SCADE toolchain, and there are other approaches (B, ETFMS, ERTMS spec model). How "official" is the Papyrus/SCADE one?
- The overall project management needs to find a solution to install a coherent approach. Eg.: A lot of participants working in the official approach, with a few exploring the alternatives. This would emphasize the development aspect of openETCS as opposed to the research aspect (without completely abandoning the latter).
- **JW:** There are named responsibilities in the project for some tasks, and these should be acted upon. Some are missing (according to JW, ¿which—not named?).
- There is a problem with managing openETCS, as it is difficult to get all involved contributors in line.
- **FV:** The QA plan should include the life cycle as presented by JW. Methods and techniques should go in there, the perimeter of the project (what will be considered as demonstrating the openETCS devlopment process, methods and tools).
- The goal for the assessment should be to classify in which respect the project approach achieved compliance.
- **RP:** As an example: The Bitwalker could be formally verified, and the assessor should say eg. that it would be ok if the tools were T2 qualified.
- **SJ:** Merlin has already put checklists on github detailing what needs to be checked during an assessment. Roughly, first the process documentation is looked at, then an audit of open questions . This would be very expensive to perform for openETCS. One could simplify this to an assessment of (explained) documentation.
- **HH:** It would help to have the process definition of an assessment, and a version to be applied in openETCS.
- **MB:** The material to be assessed should be organized in a process-oriented way.

An assessment (SJ) works like that:

1. Assessment of the process. If there are open points, the process is stopped
2. An aufit of the process is done.
3. The manufacturer sends in the full documentation. The phase-specific measures an techniques are assessed.

4. An audit of techniques and measures is performed.

Along the way, the checklists are filled. Observations can have the form of asking for an reiteration of everything (severe omissions/violations), some improvement obligations, guidelines of how to improve or proceed.

Day 2 (19.02.2014)

4 Round Table (FV)

4.1 Methods and Techniques (FV)

To be considered are the tables of the 50128 (in partivular A.13 and A.14), and we have to define what goes into the quality plan and the safety plan.

4.2 Interface Between WPs (HH)

Assign a contact person, visit the grooming meetings.

4.3 Implementing a CENELEC Process with SCRUM (KRH)

4.4 Traceability down to Goal Structuring Notation (JW)

4.5 Safety of Code (JG)

4.6 Train Localisation per Satellite (HM)

KRH: This is out of scope of the current project.

5 External Feedback (LM)

- WP4 should lead the project, the V&V has to guide the project for it not go into wrong directions.
- There are many different organisations working on the project.
- **KRH:** So far, the project has been mainly concerned with selecting methods and tools. There is now some decision (7.1) on these, based on open formats. In the followup project, the transition to fully open-source shall be made. We have to learn the agile procedure. There will be just one backlog for the project for everybody to work on.
- **LM:** The Subset 026 is not usable by non-experts. If the participants doing the modeling are not trained to expert level, then a requirements analysis (translating the SS 026 to a readable and usable form (**KRH:** Currently, it is swiss cheese with very big holes)) is necessary. This will be a very effort intensive acitivity.

- **KRH:** With the ERSA simulator, some form of reference is available, for good use in the project.
- **LM:** The tracing has to be done while constructing the model, this cannot be done after modeling.
- **LM:** Personal qualification and CENELEC compliance of the agile model have to be assured.

6 Outlook Internal Assessment and Workshop Roundup (MB)

- **MB:** Next workshop in one year. **KRH:** Too late. make a followup workshop in the same week as the ITEA review (June 12). By that time, the work shall have been organized and progressed to some extent. Friday, June 13,
- **SJ, FV:** All the process documents will have to be prepared, and technical documentations will have to be written based on these documents. **KRH:** This must have been done by then, otherwise the project cannot work.
- **KRH:** Is there a list of issues to be addressed or a plan?
- **MB:** There is a high-level list of problems and approaches, but many details have to be added. Eg., the QA plan shall list all documents and activities, but its author cannot define the process and methods and tools—these have to be provided by others. In some cases, we do not even know who can provide the answers.

End of Document