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.

Contents

1 Safety and Process 2

1.1 Safety Activities (JW) 2

1.2 Current State SSRS (System Analysis—JW) 2

1.3 Safety Analysis Approach 2

1.4 The openETCS Process (Bernd Hekele) 2

2 Documents Assessed 3

2.1 QA Plan (IdlT) 3

3 Internal Assessment (FV) 4

3.1 Internal Assessment Summary (SJ, MB) 4

4 Round Table (FV) 8

4.1 Methods and Techniques (FV) 8

4.2 Interface Between WPs (HH) 8

4.3 Implementing a CENELEC Process with SCRUM (KRH) 9

4.4 Traceability down to Goal Structuring Notation (JW) 9

4.5 Safety of Code (JG) 9

4.6 Train Localisation per Satellite (HM) 9

5 External Feedback (LM) 9

6 Outlook Internal Assessment and Workshop Roundup of decisions (MB) 9

7 09:00 - 09:20 Round Table Introduction - Frdrique Valle, All4Tec - confirmed 10

7.1 09:10 - 09:55 Round Table Topic Methods and Techniques Tables of CENELEC & Quality Plan/ Safety Plan contents - Ralf Pinger, Izaskun de la Torre and Jan Welte 10

7.1.1 **TODO** First Steps 11

7.1.2 **TODO** Estimated goal to reach 11

7.1.3 **TODO** Participants 11

7.2 09:50 - 10:20 Round Table Topic Interface between the WPs - Hardi Hungar 12

7.2.1 **TODO** First Steps 12

7.2.2 **TODO** Estimated goal to reach 12
7.2.3 **TODO** Participants 12
7.3 10:20 - 10:50 Round Table Topic How to implement SCRUM like agile development 12
7.3.1 **TODO** First Steps 13
7.3.2 **TODO** Estimated goal to reach 13
7.3.3 **DONE** Participants 13
7.4 10:50 - 11:05 - Break 13
7.5 11:05 - 11:40 Round Table Topic Traceability down to Goal Structured Notation - Jan Welte 13
7.5.1 **TODO** First Steps 14
7.5.2 **TODO** Estimated goal to reach 14
7.5.3 **TODO** Participants 14
7.6 11:15 - 11:40 Round Table Topic Safety within the code - Jens Gerlach 14
7.6.1 **TODO** First Steps 15
7.6.2 **TODO** Estimated goal to reach 15
7.6.3 **TODO** Participants 15
7.7 11:40 - 12:05 Round Table Topic Train Localization by Satellite - Hans-Jrg Manz 16
7.7.1 **TODO** First Steps 16
7.7.2 **TODO** Estimated goal to reach 16
7.7.3 **TODO** Participants 16

8 12:05 - 13:30 - Lunch Break 16

1. Find a way to get the information for the process documents is necessary
    - A clear plan to state “Who does what?” is needed inside the QA-plan.
        - Detailed competence matrix is necessary.
            - For each part a person has to be assigned.
            - Within this project an assigned task-leader or company is given.
            - How to argument the role inside the project is sufficiently qualified.
                - A derivation of this aspect can be asked.
        - Clear definition of the development part of the project is needed.
        - Define the main target of the assessment?
    - Are we oblidged to write the QA- Plan for all the approches?
    - The need to have one development chain is identified in order not to multiply effort in V&V and Safety Analysis.

- The need to have one clear process is identified.

2. Answer Questions:
    - First analysis on the papyrus model
        - Define feared events
        - Identify impact of feared events

3. Input needed for further work:
    - Lifecycle - part of the QA-Plan
        - WPs should no more mentioned - it should me more concrete - document based
        - All decisions should be inside the QA-Plan.
            - e.g. validation of the qualification of the people
    - Tools
    - Perimeter of the SIL-4 system
        - What is the part of the OBU that has the aim to reach SIL-4 standards?
            - Which portion of the OBU is used to demonstrate the SIL-4 qualification.
                - Have a look at the OBU- Architecture and identify a part which has SIL-4 functionality inside in reality.
                - Small enough to complete the SIL-4 specific tasks and big enough for demonstration.
                - Open question: Do we keep handmade code inside the SIL-4 part?
                - The Bitwalker could be part of the SIL-4 part.
                - Fraunhofer Fokus: Fomally verify the bitwalker.
        - Goal for the Assessment:
            - Questions answered
                - Pros and cons of implementing the SIL-4 standard
                - Checklists can be provided by the Internal Assessment (S. Jagusch)
                - Who should be audited for the assessment?
            - The possibility that the SIL-4 Assessment may not be completes is identified.
                - Due to project restrictions.
            - Usually an audit is performed on Techniques and Measures
            - Possibility to do an assessment on documents only could be a possiblity to deal with distributed contributions.
            - S. Jagusch will provide the 5 step process definition on assessment.
            - The lifecycle should be clearly stated in the QA- plan.

- ∗ Inside all process related documents the WP or tasks as stakeholder should be broken down to lifecycle elements.
- ∗ VnV and Safety documents should reference each each phase of the lifecycle.
  - · specifically state the:
  - · input
  - · output
  - · what has to be done.
- ∗ Approach within the internal assessment: With a go/ no-go decision after each step
  - (a) Review process documentation (is the basis)
  - (b) Audit on process
  - (c) the next internal mielstone to decide on this basis is the 13th of May 2014

  3 possible results of audit

  - · If there are open points there is no assessment report
  - · Failures - an assessment report is written
  - · Obligations are put on to the assessed parties
  - · Hints - Information what to improve in the next project
  - · Reviewing phase specific measures and techniques documentation
  - · Do an audit on techniques and measures

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 of decisions (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, this date is decided on the internal milestone at the 13th of May 2014
- **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.

Contents

7 09:00 - 09:20 Round Table Introduction - Frdrique Valle, All4Tec - confirmed

7.1 09:10 - 09:55 Round Table Topic Methods and Techniques Tables of CENELEC & Quality Plan/ Safety Plan contents - Ralf Pinger, Izaskun de la Torre and Jan Welte

- R. Pinger:
  - □ Start with a list of Functions and Architechture
  - □ have a risk of functions
  - □ Bottom up approach:
    - What do we have as tools covering the Techniques and Measures (and other CENELEC Tables)
    - Make a tool-related view of the tables inside the QA- Plan
  - □ Top Down approach: What has to be covered from CENELEC
    -
  - □ Risk Analysis: Which functions should comply to which SIL- level
  - start with existing tools 50128 bottom up - covering
    - list of tools
    - time is critical - no assessment in full glance
    - focus on the tools we have
    - try to make a real argumentation on the tools

    - Process persepctive - new ways
        - some parts will be open it might be much easier for the verndo's perspective
        - assessment on the tools if possible
- Frdrique: Define the perimeter and the process to follow this project
- Safetyplan: Risk analysis methodology
- Quality management plan

7.1.1 TODO First Steps

- □ Estimated effort for first steps

7.1.2 TODO Estimated goal to reach

7.1.3 TODO Participants

- □ Ralf Pinger
- □ Izaskun de la Torre
    - Rearrange the QA- plan in order to fulfill the decisions
    - HRA- plan should be included to Table 11
- □ Jan Welte
    - will contribute the lifecycle description to the QA- Plan
    - Proposal to call the Safety Plan: Hazard and Risk Analysis Plan
    - List of documentation to be done with Izaskun and Jan
- □ Hardi Hungar
    - will update the VnV plan to conform to the development accompanying lifecycle
    - for every phase there is a VnV action foreseen
- □ Ask WP7 for a list on CENELEC related coverage of methods (see tables)
    - Input to the QA- plan
    - Impact on VnV plan
    - WP7: Toolchain –¿ ask Ccile
    - WP4: VnV -¿ Marc (D4.2.1 p20 could be a starting point) Safety -¿ Jan
    - WP3: Bernd
    - WP2: Bernd will contact SNCF

7.2 09:50 - 10:20 Round Table Topic Interface between the WPs - Hardi Hungar

- Interace between Modelling and Verification (WP3 & WP4)
- It works at close collaboration level (small cluster)
- Visitbility of activities and results?
- Rough format for a design artifact should be defined
- Find out who collaborates with whom and get partners not involved in the main development stream to include
- D4.2.2 and D4.2.1 (p20)
- Ask peoplpe to contribute:

7.2.1 TODO First Steps

- Estimated effort for first steps
- Split of activities - which party is involved in which activities?
- Split in topics -¿ Marc

7.2.2 TODO Estimated goal to reach

- □ How do we get the DAS2V
- □ Which types/ models will be created on the development branch
- □ Who is in charge of the design model? – person: Bernd just assigned
- □ Who is in charge of the design quality process: That the verification is triggered: Bernd

7.2.3 TODO Participants

- □ Bernd Hekele
- □ Hardi Hungar
- □ Marc Behrens

7.3 10:20 - 10:50 Round Table Topic How to implement SCRUM like agile development

scheme with meeting EN50128:2011 goals in an Eclipse setting - Klaus Rdiger Hase

7.3.1 TODO First Steps

- Estimated effort for first steps
- Start with a basic function
  - Do a priority setup of the functions
  - add a function
  - Go through all the function issues
  - □ ? May cause iteration in the Architecture
  - Create shippable items within one week
- □ SCRUM Backlog is needed
  - What you do and how you do it
- Klaus: Update the QA- plan in a way that the procedure how to set up our agile incremental methon in a way that it meets the goals of the CENELEC safety requirements in our project

7.3.2 TODO Estimated goal to reach

- □ Have a product backlog organied for each WP
- □ Have the product ower makng a priorization of the tasks to be finished next
- □ Team creates the sprint backlog

7.3.3 DONE Participants

`CLOSED:` *2014-02-19 Mi 11:18*

- ☒ Klaus Rdiger . product owner
- Izaskun - product owner of the QA- Plan

7.4 10:50 - 11:05 - Break

7.5 11:05 - 11:40 Round Table Topic Traceability down to Goal Structured Notation - Jan Welte

- Jan: Introduction to GSN - Goal Structure Notation
- On methods level (not describing the product)
- Picture for the Kenrel from Subset-091

7.5.1 TODO First Steps

- Estimated effort for first steps
- 1. Write down approach (Jan)
- 2. Implement Tool (WP7)
  - Connect AC-EDit (GSN- Tool from York) to EGIT
- 3. Set up a model (Jan with AEbt: , All4Tec, Systerel)
- Build the first argumentation chain
  - Why is our argumentation chain conform to SIL-4
  - Providing Requirements, Arguments and Evidence (documents)
  -

7.5.2 TODO Estimated goal to reach

-

7.5.3 TODO Participants

Safety Analyst:

- Jan Welte
- Marielle Petit-Doche (Colleague of)
- Stephan Jagusch
- Anthony Faucogney

7.6 11:15 - 11:40 Round Table Topic Safety within the code - Jens Gerlach

- Estimated effort for first steps
- Investigating the relationship between formal proof and testing in the surrounding
  - where can formal verification repace certain test activities
- What are the properties I want to verify
  - Functional correctness
  - Worst Case execution time
  - Freedom of unintended functions

    - Bound on stack size
    - ...

- Caviar? (Predessessor of FRAMA-C)
    - Was productively used within AIRBUS development
- Unit testing is still done within the industry (evenif not mandatory in every case by CENELEC)

7.6.1 TODO First Steps

- Which properties to verify
    - Functionality
    - Robustnes
- □ Formal Proof choosen (Table A5 fom EN-50128)
    - Statis Analysis and Software Error Effect Analysis not choosen then?
- Which testing activities can be replaced due to formal methods
- Formulate what according to the CENELEC can be covered in which apect by Formal Proof
- Where does the bitwalker fit intot the architecture
- Necessity of testing on the background of formal proof

7.6.2 TODO Estimated goal to reach

- Which testing activities will never go away
- Which testing activities can be replaced by formal proof
    - Unit tests?

7.6.3 TODO Participants

- □ Jens Gerlach, Fraunhofer
- AEbt, All4Tec, Siemens, Fraunhofer, CEA/LIST
- Hardi Hungar, DLR
- R. Pinger, S. Gerken, Siemens
- Virgile Prevosto, CEA List
- Stephan Jagusch
- Anthony Faucogney

7.7 11:40 - 12:05 Round Table Topic Train Localization by Satellite - Hans-Jrg Manz

- Implement Satellite Localization inside openETCS one day?
  - Replacing the Odometer.
- Frdrique: Galileo COTS not CENELEC compliant
  - Availability figures for Galileo are not yet known
    - Only studies are known
- Klaus: The goal of openETCS is not to develop the standard further
- PTC is one example using satellite based positioning
- See TSI-CCS - ODO FIS reserved and planned

7.7.1 TODO First Steps

- Estimated effort for first steps

7.7.2 TODO Estimated goal to reach

7.7.3 TODO Participants

Conclusion: The topic was considered to be out of scope for openETCS.

End of Document