Notes and MoM on the subject of the SSRS

Sylvain Baro – SNCF – 10/04/13

This document is the MoM of the discussions on the SSRS of the openETCS Charleroi workshop (28-29/03/13). For clarification, it also includes topics presented during the openETCS Paris workshop (11-13/03/13).

Participants (the 29/03/13)

- P.-F. Jauquet (Alstom, organizer of the workshop)
- Luis-Fernando Mejia (Alstom)
- Marielle Petit-Doche (Systerel)
- Jan Welte (TUBS)
- Merlin Pokam (AEBT)
- Baseliyos Jacob (DB)
- Stanislas Pinte (ERTMS Solutions)
- Stéphane Callet (SNCF)
- Sylvain Baro (SNCF)
- Ralf Pinger (Siemens)

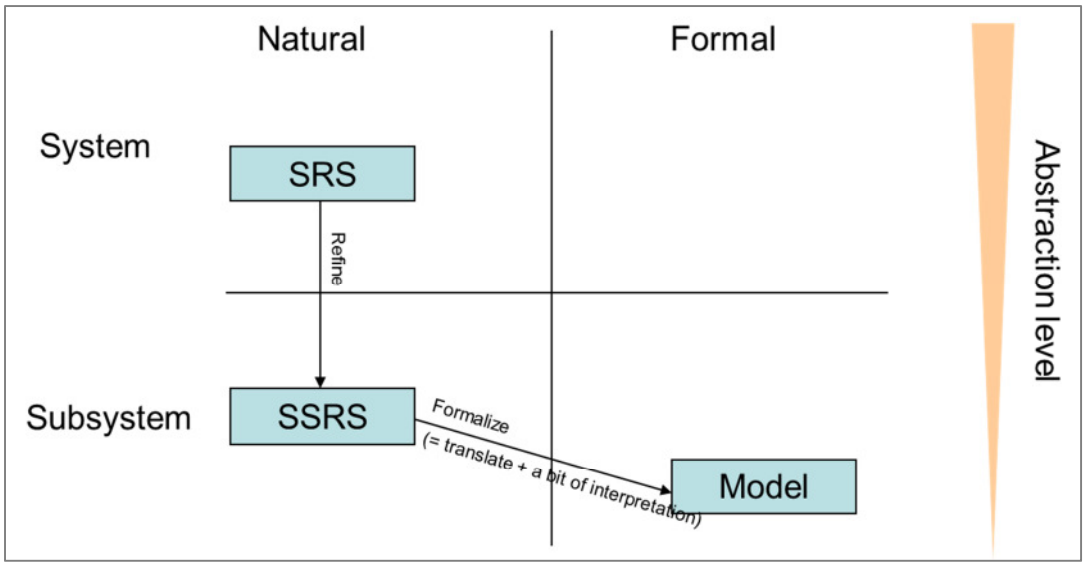
Why?

It is required to add a step of document between the SRS and the intended model of the OBU. The modeling of the SRS would require the following steps:

- to define the scope of the model (~ the OBU kernel);
- to provide an architecture for this model (functional and SW);
- to lift ambiguities;
- to detect errors and inconsistencies;
- to transform requirements into an executable content;
- to transform a natural language into a formal language.

Adding a step of documentation allows breaking these difficulties down. This step would be the Sub-System Requirement Specification. This step will allow the following:

- to define the scope of the model (more or less the OBU kernel);
- to provide an architecture for this model (functional and SW);
- to lift ambiguities;
- to detect errors and inconsistencies.



The remaining steps will be considered in the step between the SSRS and the model.

What?

The SSRS will be composed of two parts: the functional architecture and the requirements.

The functional architecture is a functional breakdown of the subsystem. It makes explicit the boundaries of the onboard subsystem itself, and also provides the internal functional architecture of this subsystem. This internal architecture is composed of functions and flows of data between these functions. All the objects described will be unambiguously named (in particular I/O). This architecture will be described using a semi-formal language.

This architecture is useful for the following reasons:

- it makes the system easier to maintain;
- it provides the boundaries of the system;
- it eases the safety analyses and the V&V (with the internal cut out, and the unambiguous flows of data);
- it also helps with modeling by providing some structure.

The second part of the SSRS is the requirements list. The requirements from the SRS are allocated toward the functions of the SSRS (the architecture), possibly split and rewritten in order to restrict their scope to these functions (of course, traceability is mandatory). They are also rewritten in order to match the objects named in the architecture (in particular internal and external I/O). The requirements are provided in natural language (even if the objects are unambiguously named). The formalization layer is coming below the SSRS, with the model.

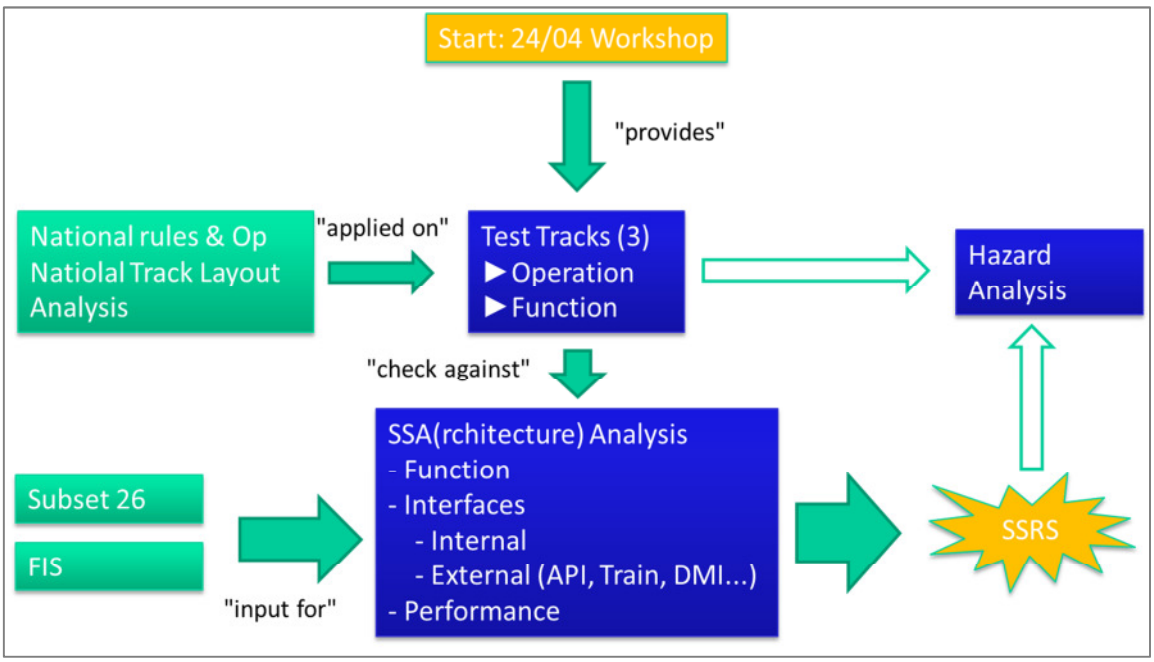
The architecture objects (functions, streams...) and the requirements are tagged Vital/Non Vital.

How?

The main input for the SSRS is the SRS (SUBSET-026) and other related subsets (SUBSET-040, SUBSET-091).The SSRS shall take into account the degraded mode (operational degraded modes as well as

functional degraded modes). It will also take into account safety. The SSRS has to comply to the SRS, so it has to be fully generic.

The SSRS will be "checked against" some sample tracks, but not "adapted to" these sample track. It has to be a generic document, but it should be proved against some specific samples. In the same way, the hazard analysis should be generic.



The SSRS work and discussion will start during a dedicated one-day workshop (SSRS Kick-Off). This workshop will aim for the organization of work as well as the preliminary data gathering (in particular for the definition of the scope of work for the first version of the SSRS).

After this workshop, the SSRS team will work aiming to produce a first version of the document. This first version will only cover the nominal operation for the reference track layouts (which should cover 2 lines from the DB and one from the SNCF).

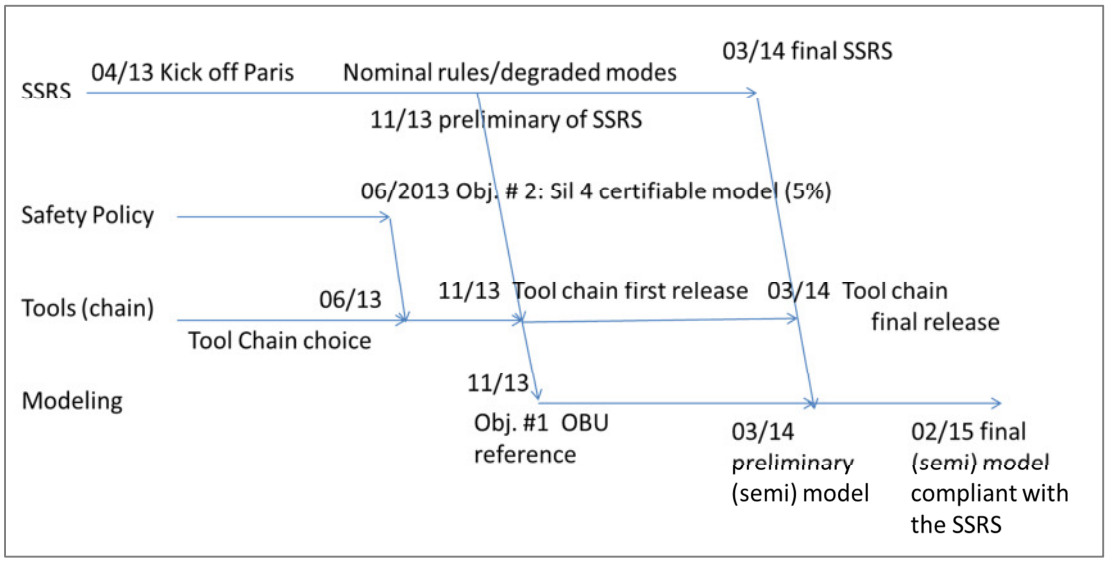
The second (final) version will be produced a few months later, and shall be fully compliant to the SUBSET-026.

Who?

The SSRS team will be composed of system engineers from both manufacturers and operators. Alstom made clear that they will only accept to work on the SSRS if the other manufacturers also contribute on it. It was asked that all the manufacturers that accept to work on the subject, and the SNCF and DB, send participants to the SSRS Kick-Off meeting.

Alstom proposed the SSRS task to be led by a UNISIG member.

When?



Appendix: requirements on the SSRS

The following is not part of the MoM, but is provided for the sake of completeness. This is an excerpt of the D2.6 – D2.9 document (current draft version).

R-WP2/D2.6-X-10 The SRS (SUBSET-026 for the reference baseline) shall be refined into a SSRS.

R-WP2/D2.6-X-10.1 The SSRS shall provide a functional architecture of the OBU.

R-WP2/D2.6-X-10.1.1 The SSRS shall split the KERNEL into independent functions.

R-WP2/D2.6-X-10.1.2 The description of the architecture shall be semi-formal.

R-WP2/D2.6-X-10.1.3 This architecture shall provide the functions and the data streams between them.

R-WP2/D2.6-X-10.1.4 The SSRS shall describe which part of this architecture will be modelled.

R-WP2/D2.6-X-10.1.5 The SSRS shall provide the interfaces between the considered subsystem and its environment.

R-WP2/D2.6-X-10.1.6 When the boundary of the formalized subsystem corresponds to a FIS or FFFIS, the SSRS shall try to comply to it even when it is not mandatory.

R-WP2/D2.6-X-10.2 The SSRS shall allocates the requirements of the SRS to the functions and their I/O.

R-WP2/D2.6-X-10.3 Full traceability between the SRS and SSRS shall be provided.

R-WP2/D2.6-X-10.3.1 Interpretations, additions and omissions shall be tracked and justified.

R-WP2/D2.6-X-10.3.2 The requirements allocated to other subsystemes (e.g. RBC) shall be tracked.

R-WP2/D2.6-X-10.3.3 Lower level requirements refined from higher level requirements shall be tracked.

R-WP2/D2.6-X-11 The SSRS shall identify the Vital and Non Vital functions, requirements, and data streams.