OpenETCS SSRS Task Force

Stanislas Pinte, ERTMS Solution
Baseliyos Jacob, Deutsche Bahn
Bernd Hekele, Deutsche Bahn

DoW

Task Force SSRS

Baseliyos Jacob, Deutsche Bahn
SSRS Task Leader

Bernd Hekele, Deutsche Bahn
SSRS Requirement for Tools & Process

Stanislas Pinte, ERTMS Solution
Task leader 3.5 & 3.6
Functional Analysis & Functional Allocation

1.1 Abstract

This taskforce will gather and sum up the necessary requirements, documents, variables and interfaces to develop a generic OBU kernel. In this case 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.
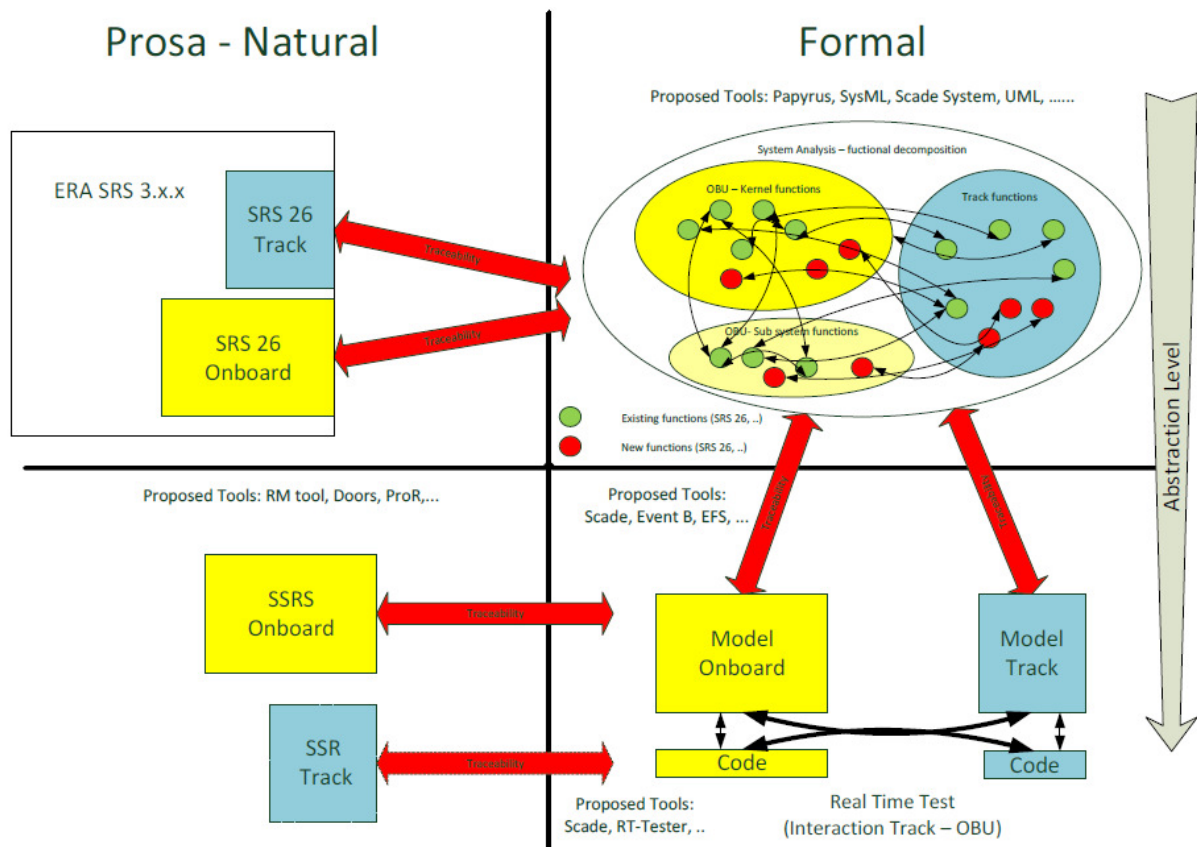
The first outcome of this Task force will an overview of all necessary documents from the operator, the industry and all the European Railway Authorities to manage this kind of a documents.

1.2 Objectives:

The SSRS will be composed of two parts: 1/ the functional decomposition and the API (architecture) and 2/ the requirements.

The functional decomposition & API (architecture) is a functional breakdown of the subsystem. It makes explicit the boundaries of the onboard subsystem itself, and also provides the internal functional allocations of this subsystem. This internal decomposition & API (architecture) is composed of functions and flows of data between these functions. From the API we will derive the limits of this System.

All the objects described will be unambiguously named (in particular I/O) in a data dictionnary.

This functional decomposition will be described using a semi-formal language.

This allocations 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 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.

2.1 Organisation of the work

The Task Force will be split in 4 Tasks:

Task 1: delivering of the Primary sources and the ERTMS knowledge from the industry and the operator.
Operators and Industry – running parallel

Responsible: SSRS Task Baseliyos Jacob, Bernd Hekele, Deutsche Bahn, Jan Welvaarts NS/Lloyds, Jan Welte TUBS

List of Primary sources:

- ERA documents (subset 26 necessary requirements 4.5.2 + other documents)
- Experience of the Operator
- Experience of the Industry
- Operation Rules of the Operator
- API /
- Hazard Analysis from the Operator

Task 2: Functional Analysis: (2.5 PY)
- Identification of the kernel functions between OBU and Track including inputs/outputs variables
- Identification of the relationships between the functions
- Creating of an consistent data dictionary
- Clarify the requirements (describe the functions in a clear way)

Responsible: Deutsche Bahn, NS/LLoyds
Participants: All4Tec, CEA, ERSA, Lloyds/NS, DB, (SQS), Systerel, ERTMS Solution
Reviewer: Alstom, DLR, Siemens, TUBS, SNCF, Deutsche Bahn, NS

Output:
Data Dictionary (Database)
Function (Database)
Link between Functions and Datas
Set of clarified requirements (Excel sheet)

Input:
Requirements on the tool:
Attributes
Data check
Traceability
Multiuser
Reliability for integration

Flexibility of the database
Reporting
Change Management

Task 3: Documentation of the openETCS System Boundary:
- Deriving all the interface specifications from the data dictionary
- Defining the scope of the SSRS
- Finalization of the SSRS

Responsible: DB
Participants: TUBS, DLR,
Review: Siemens, Lloyds/NS, All4Tec, Fraunhofer, TWT,

Input:
Data Dictionary

Outcome:
OpenETCS Interface specification
Functional architecture

Requirement on the tool:
Reliability for integration
Change Management

Task 4: linked with WP 4 V&V

Task 1								
Task 2	ERTMS Solution (ERTMS Experts)	Lloyds (ERTMS Experts)	ERSA (ERTMS Experts)	DB (Operator ERTMS Experts)				
Task 3								

Pic 1 - Task overview

SSRS

Task 4: V&V, Safety, Hazard Analysis and CR
Will be see of and check Task 1,2, 3 and the overall Process

Task 1: Primary Sources (Operator, Industry)

- Operation Rules
- Hazard Analysis
- Experience of the Operator
- Experience of the Industry
- API (Alstom)
- Data Dictonary (Alstom)
- (ERA Documents)

ERTMS Experts - Operator

Task 3: Documentatoin of openETCS System Boundaries - Identification of the overall function

- Deriving all the interface specifications from from the data dictionary
- Defining of the scope of the SSRS

Operator - ERTMS Experts

Task 2: Functional Analysis

- Identification of the functions including outputs/inputs
- Identifikation of the relationship between the function
- Creating of an consistent data dictionary
- Clarify the requirements

Modeling Experts - ERTMS Experts

Feedback

Feedback

Model

Formal Model 1

Formal Model 2

Formal Model 3

Formal Model 4

……

Semi Formal Model 1

Semi Formal Model 2

Semi Formal Model 3

Semi Formal Model 4

……
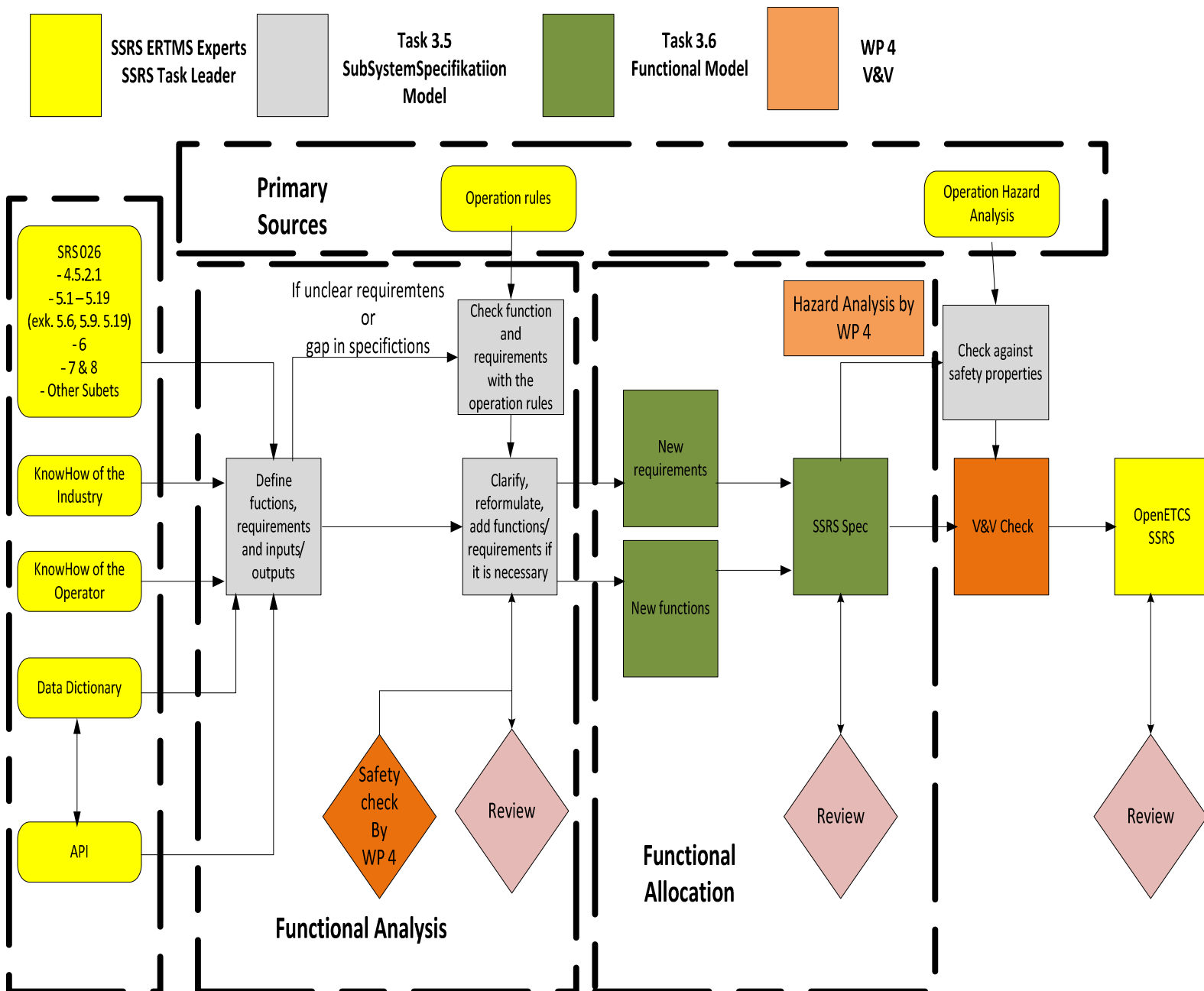
Note: the semi-formal and fully-formal modeling teams in tasks 3.5 and 3.6 should provide feedback to Tasks 1..4 during the whole project, and act as a reviewing team.
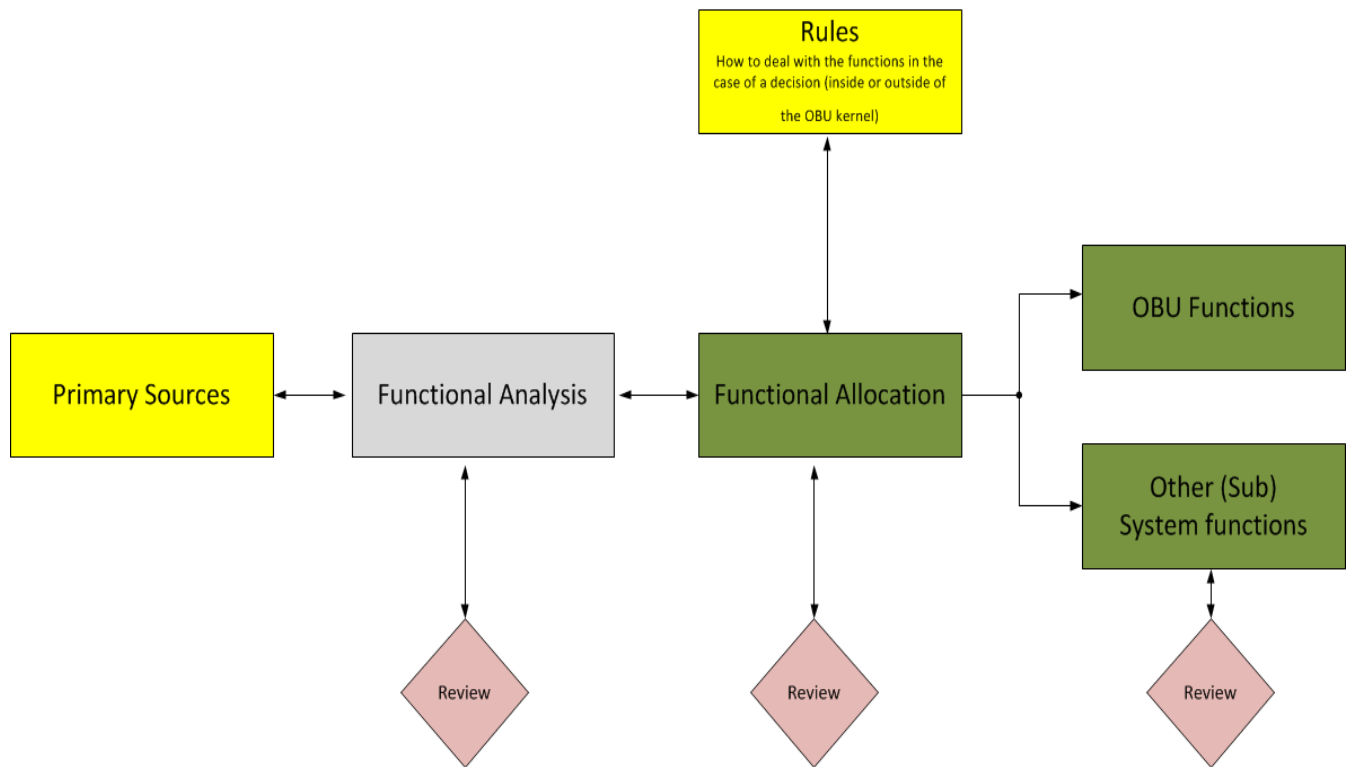
Actually, these teams are the customers of the SSRS team, as SSRS is the input for semi-formal model(s) and fully formal model(s).
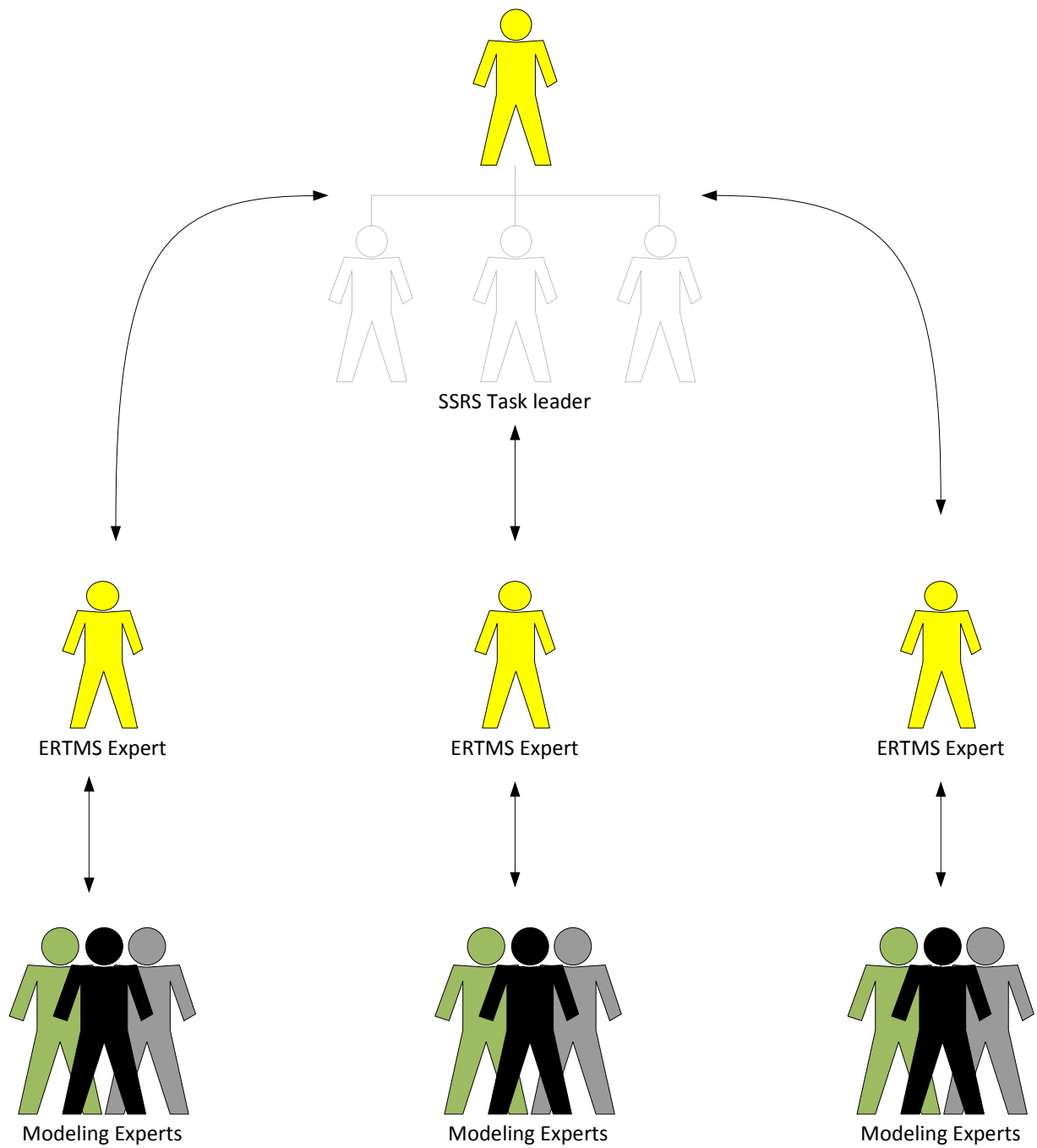
Pic 2 – Steps of Process

Pic 3 – Overall Process

Pic 4 – Working Couples

SSRS Task leader

ERTMS Expert   ERTMS Expert   ERTMS Expert

Modeling Experts   Modeling Experts   Modeling Experts

2.2 Sprint List:

Main Requirements Sources

4.5.2.1 Active FunctionsTable	
5.1 – 5.19 (exc. 5.6, 5.9, 5.19) Procedures	
6 Management of older systems	
7 ERTMS/ETCS Language	
8 Messages	
TSI Annex A	

Goal

Weekly Telco (30 min.)
Newsletter
Short communication sessions between operator – modeler – ERTMS Experts

08/7- 19/7. Sprint 1

Sprint 1 shall include the following work:

Baseliyos Jacob and Stan. Pinte:

- Put in operation a Temporary requirement tool
- Plan Next sprint tasks + schedule

Task 1 team:

- Gather operational and national rules documents
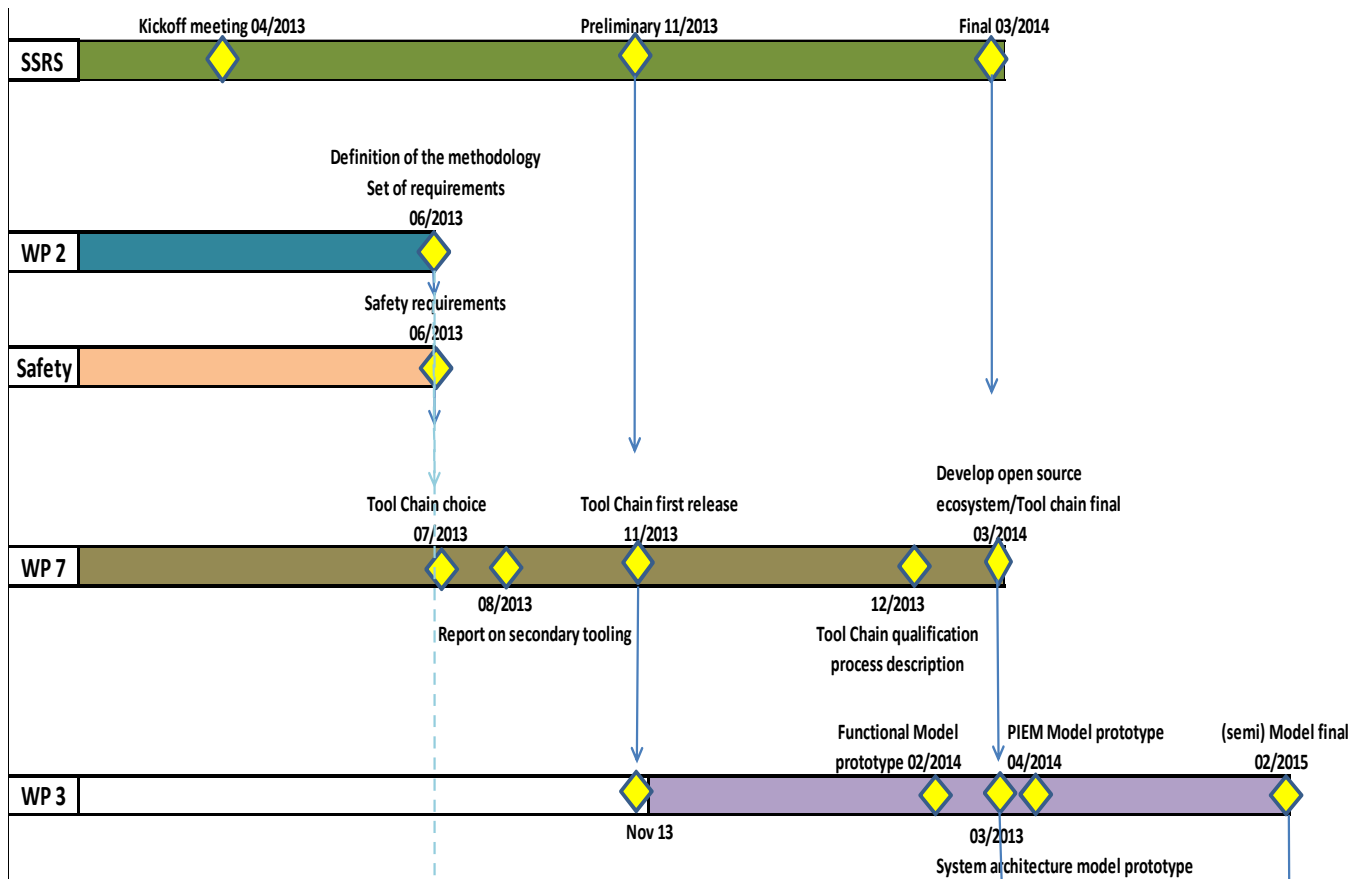- Gather hazard analysis documents

Task 2 team:

- Start graphical functional decomposition by modeling top-down the Subset-026, defining functions and data flows

Task 3 team:

- Integrate + Reviewing ERA documents and Spread the Requirements from the SRS026
- Integrate data dictionary from existing ERTMSFormalSpecs data dictionnary

3. Time Schedule

SSRS
- Kickoff meeting 04/2013
- Preliminary 11/2013
- Final 03/2014

WP 2
- Definition of the methodology
- Set of requirements
- 06/2013

Safety
- Safety requirements
- 06/2013

WP 7
- Tool Chain choice 07/2013
- 08/2013
- Report on secondary tooling
- Tool Chain first release 11/2013
- 12/2013
- Tool Chain qualification process description
- Develop open source ecosystem/Tool chain final 03/2014

WP 3
- Nov 13
- Functional Model prototype 02/2014
- PIEM Model prototype 04/2014
- 03/2013
- System architecture model prototype
- (semi) Model final 02/2015

13

4. Requirement for SSRS Tools:

4.1 Requirements for the SSRS Requirements Management tool.

- Need an documents based outcome (Excel)
- Must be compatible to a graphical decomposition and (semi) formal model tool
- Version management
- Multi user
- Data Dictionary Check

  <u>Attributes:</u>
- Requirement ID
- Document Source
- Related SRS §
- National Operation Rules xx country
- Variable Name – Input Variable/Output Variable
- Descritption
- ETCS language reference
- Version (Document)
- Source (source of required information)
- Range (possible values)
- Source assumed (if source is not clear)
- Comment
- Proposal
- Remark
- User – Unique/Multiple
- Discussion of the requirement in Subset 25 – xx ID
- Functions
- Functional Block
- Validated
- Informaton of requirement (need to/shall be)
- approval

4.2 Requirements for the SSRS Graphical Functional Analysis tool

- Must be compatible to the requirement management and (semi) formal tool
- Graphical Human interface
- Data Flow Check
- Data Dictionary Check

5. Requirement on the SSRS at all

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.

Architecture vs. functional decomposition

Definiton of architecture
What do we need?

What is safety means? Robustness?