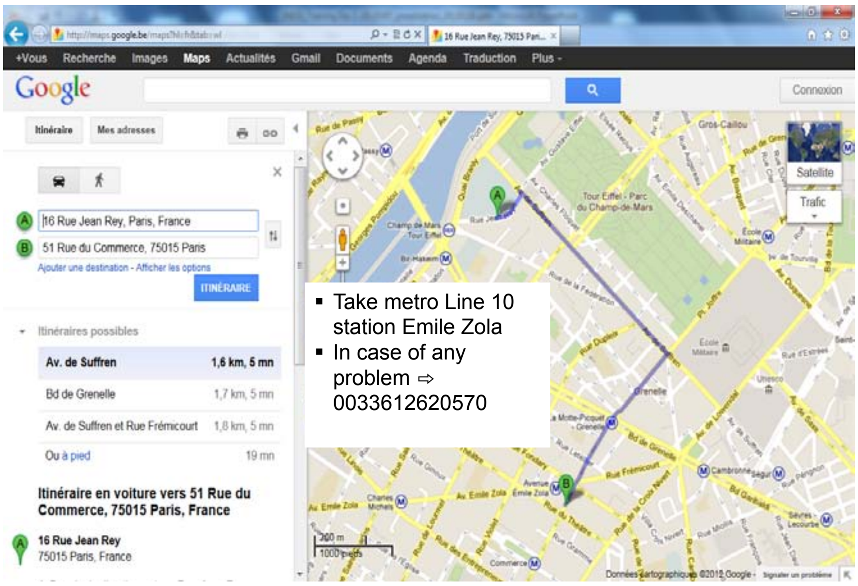
Welcome to the INESS training

7,8 & 9 March 2012

Welcome

- Thanks to UIC to hosting this event
- Please wear your badge at all times
    - Internet access info is on your badge!
- Please: No Food & Bevarage in meeting rooms
- Presentations available via:
    - Hardcopy of sheets available in lobby
    - Download via the www.INESS.eu webpage (Training)
    - The USB you got at registration
    - Evening Dinner 19h15 at **Le Café du Commerce,** 51 Rue du Commerce, 75015 Paris
- Questions?...ask the people with GRAY banner on badges

Le Café du Commerce, 51 Rue du Commerce, 75015 Paris



- Take metro Line 10 station Emile Zola
- In case of any problem ⇨ 0033612620570

INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

INESS Training (Day one)

Agenda Item	Speaker	Time
Arrival and registration	ALL	9:00
1. Welcome and Presentation of participants	Emmanuel Buseyne	09:15 – 09:30
2. Introduction to INESS - Program (Objectives, Context & Results)	Emmanuel Buseyne	09:30 – 10:00
Coffee break		10:00 – 11:30
3. INESS Requirements and Verification & Validation, Common Kernel • Introduction Common Kernel • Clarify link to other WS's	**WS D** Wendi Mennen	10:30 – 10:40
• Concept for setting-up the requirements • Structure chosen for requirements	Mirko Blazic	10:40 – 11:00
• Philosophy for Verification	Bas Luttik	11:00 – 11:20
• Challenges towards the Future	Wendi Mennen	11:20 – 11:30
General Discussion		11:30 – 12:00
LUNCH BREAK		12:00 – 13:00
Workshop on how to use the Common Kernel	WS D Mirko Blazic	13:00- 14:00

INESS Training (Day one), continued

Agenda Item	Speaker	Time
4. Functional Architecture & Interfaces • INESS architecture and interfaces • FFFIS Interlocking and RBC interfaces • Q&A • FFFIS Interlocking-CLC and interlocking-interlocking • Using the UML-based approach for specifying railway interfaces • Q&A	WS E Jorge Gamelas Thomas Lauscher	14:00 – 15:30
• **Coffee / Tea Break**		15:30 – 16:00
5. WS E presentation (Continued) • Fall-back possibilities & benefits • Q&A • Final recommendations for trackside migration and fall-back • Q&A	WS E Tobias Lindner Peter Winter	16:00 – 16:40
6. General Discussion and Closing day one	ALL	16:40 – 17:00
DINER, **Le Café du Commerce,** 51 Rue du Commerce, 75015 Paris		19:30 – 21:30

INESS Training (Day two)

Agenda Item	Speaker	Time
1. Unified European Railway Infrastructures data model (EUDRI); Status of activities • Explanation of work done in the WS • Overview of the Data Model requirements	WS C Tom Stein	09:00 – 09:45
• Q&A		09:45 – 10:00
• Challenges & Path forward • Identify challenges in the present data model • Needed actions to be able to implement the data model in your own organisation	Tom Stein + TBC	10:00 – 10:40
Coffee break		10:40 – 11:10
• Discussion about how to make the Data Model work in your organisation		11:10 – 11:45
LUNCH BREAK		12:00 – 13:00
2. Testing and Commissioning • Presentation cost efficient methods for testing and commissioning of interlockings + Handbook	WS F Neil Barnatt	13:00 – 14:00
• General Discussion about testing & commissioning		14:00 – 14:30
Coffee break		14:30 – 15:00
Conformity Testing / Data Reduction	Jorge Gason	15:00- 16:00
3. **General Discussion and Closing day two**		16:00 – 16:30

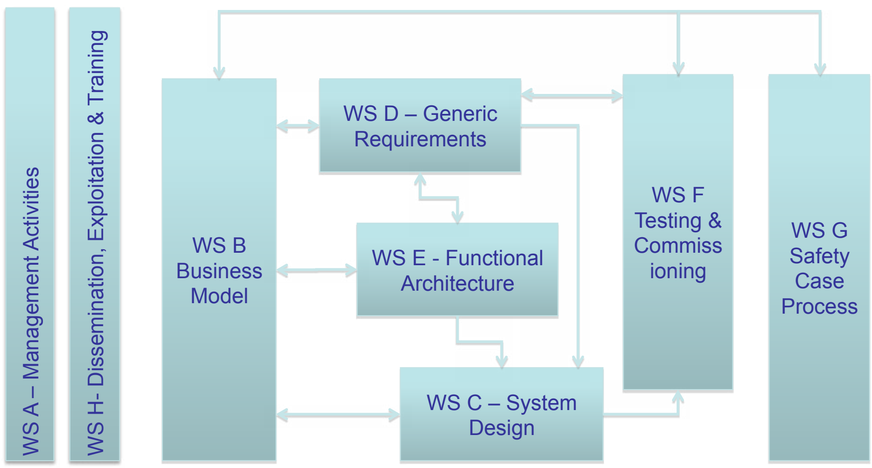
INESS Training (Day three)

Agenda Item	Speaker	Time
1. Safety Case Process • Improving the safety case development: Workflow improvement by Tool support	WS G Geltmar von Buxhoeveden	09:00 – 10:00
• General Discussion		10:00 – 10:30
Coffee break		10:30 – 11:00
Workshop on how to use the Tool	(parallel sesion) Geltmar von Buxhoeveden	11:00 – 12:00 Stephenson Room
2. INESS Business Case • Presentation of the INESS Life-cycle approach and the INESS Business model • Business model • INESS LC-model and cost saving potentials • System Dynamics methodology for developing the business model • Cooperation plan • Examples based on DB experiences • Questions to be answered	WS B Thomas Hirsch Karsten Kamps Hirsch/Kamps/Hoffart	11:00 – 12:30
LUNCH BREAK		12:30 – 13:00
• Workshop on how to Apply the Business model. • Exercise on the Business model to understand it • Exercise to adapt the model	Thomas Hirsch Christian Hoffart	13:00 – 14:30 Plenary room, Stephenson Room
3. **General Discussion and Wrap up of the whole programme**	Emmanuel Buseyne	14:30 – 15:00

INESS Training PM's presentation

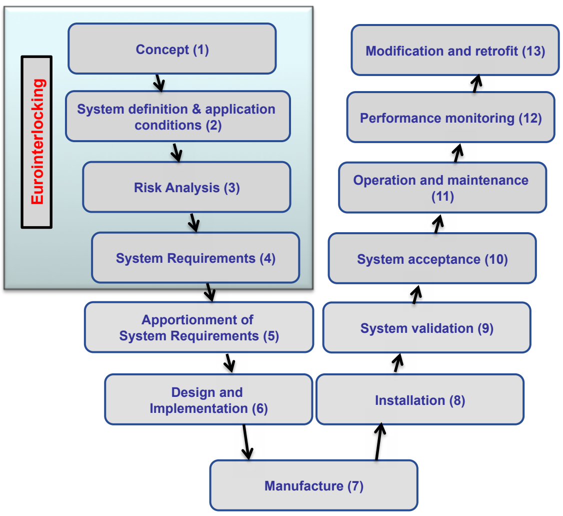
Introduction to INESS

Emanuel Buseyne



INESS context

Eurointerlocking - Harmonisation of IxL requirements



The Euro-Interlocking project was launched in 1999 by UIC with participation of 15 railways.

The aim was to harmonise requirements for a “European railway IxL system”.

The work was focused on the 4 first phases of the V cycle.

Results of the project are compiled on a CD ROM. The current Baseline is 8.2

The baseline were used as input for INESS requirements’ database

INESS - European Background

1

Around 20 different signaling sys… lea… inc… saf…

2

The EU stakeholders agreed … r to … IS

The EC promoted the idea of an Integrated (harmonised) signalling system in order to:

- **Harmonise** the Interlocking with its surrounding equipements
- Significantly **reduce the cost** of future signalling equipements
- **Accelerate the rollout of ERTMS**

4

Ar… im… economical nonsense

…ion …e to …tion of signalling systems

INESS – contract with the EC

COMMISSION OF THE EUROPEAN COMMUNITIES

SP1-Cooperation

Collaborative project

Large-scale integrating project

INESS

INtegrated European Signalling System

Grant Agreement Number 218575

SCP7-GA-2008-218575

- Planned duration: 42 Months (initially 36).
- Total planned cost: 16.6. M€ in which 10 M € financed by the EC
- 1200 Man Months
- 30 partners
- 8 Workstreams, 32 Workpackages, 97 Deliverables

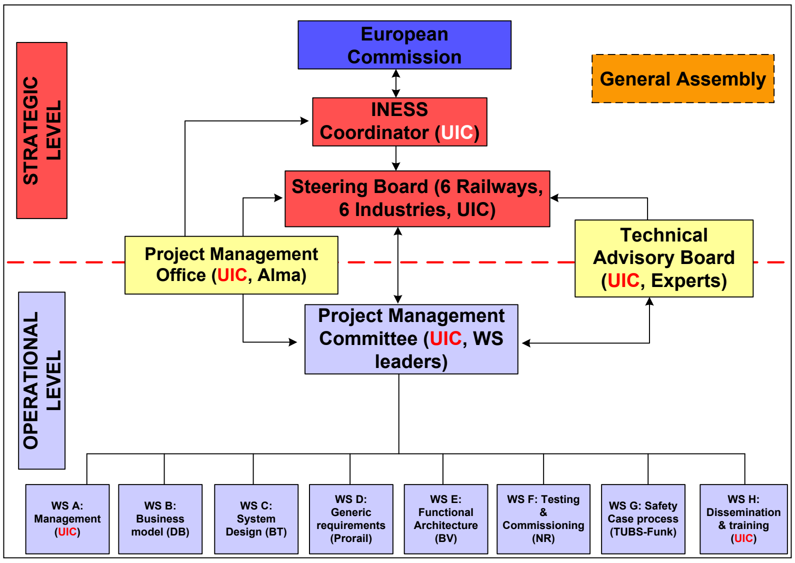
INESS - Partners

Railways	Industry	Universities & research institutions	Small and Medium Enterprises	Consulting
UIC adif BANVERKET DB NETZE Network Rail ProRail RFI Rete Ferroviaria Italiana Gruppo Ferrovie dello Stato	invensys Rail ALSTOM AZD Praha AnsaldoSTS BOMBARDIER NUCLEO mermec SCHEIDT&BACHMANN funkwerk information technologies unife SIEMENS THALES	DLR Deutsches Zentrum für Luft- und Raumfahrt RWTH AACHEN UNIVERSITY Carolo-Wilhelmina Braunschweig University of Southampton POLITÉCNICA TU/e Technische Universiteit Eindhoven University of Technology The University of York	BBR Verkehrstechnik Railsafe Consulting Ltd.	ALMA Consulting Group TIFSA

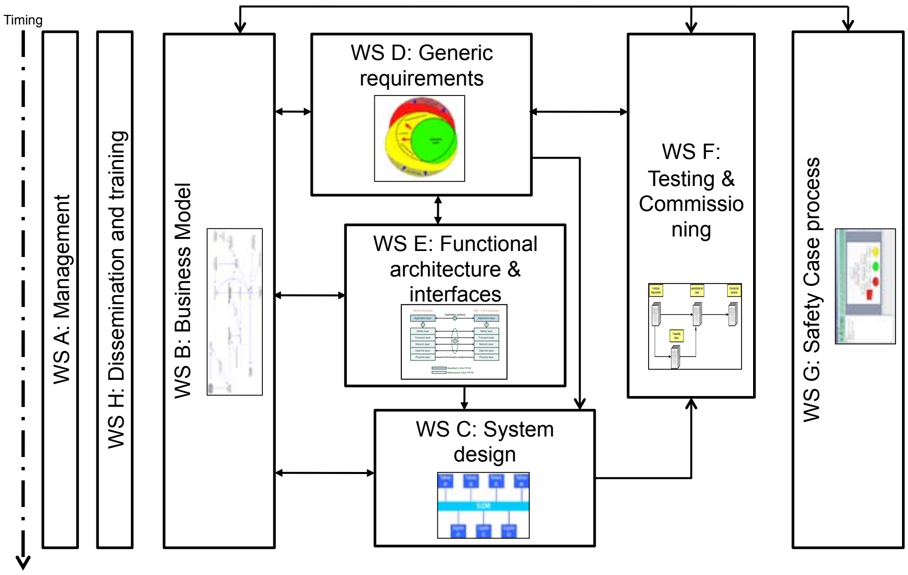
Including experts from BDK, JBV, ÖBB, PKP, RHK, SBB under the UIC umbrella.

INESS Scope

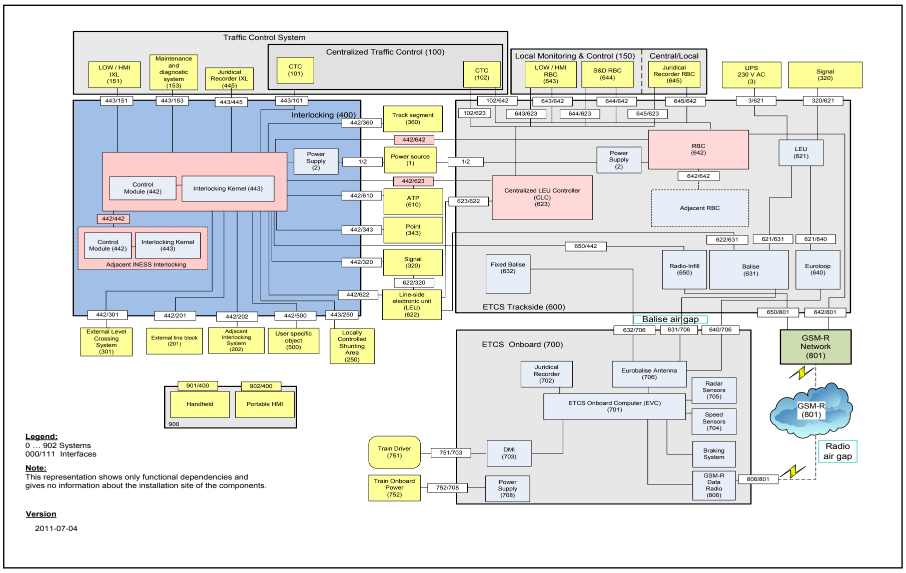
INESS - Organisation



INESS - Workflow



INESS - System Architecture



INESS Concept and results

INESS - main S/T Objectives

iness

Our Goals

- To develop a **common business model** to support **intelligent migration strategies** for ERTMS - (WS B)
- To describe a **Unified European Railway Infrastructures data model** (EUDRI) - (WS C)
- To develop a **common IxL Kernel** of validated standardised functionalities and methods and tools for **Validation and Verification** - (WS D)
- To propose **standardised system architecture(s) and the relevant interfaces** between the IxL and the ... subsystems - (WS E)
- To developp practical cost effici... **processes for Testing a...** outcomes – (WS F)
- To develop ... **and impleme...** ...**ion** ...**ss** according to t... ...G)

Ou... ...nges

- Variety of signalling systems
- Problems in ERTMS implementations
- Absence of normative framework
- Size of the consortium, various opinions and interests

Our Results

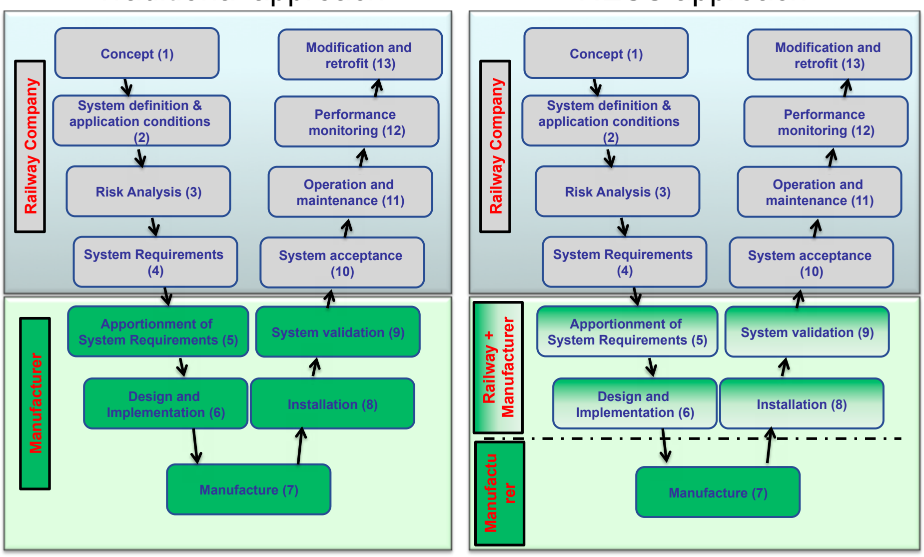
- **LCC and Business ...** ...o reduce the LCC of INESS ... ...l to support intellig... ...or ERTMS - (W...
- ...roposed ...DM (railML) ...C)
- ...**rnel of IxL standardised** ...**nalities** and executable Model ...oolchain and V&V proofs - (WS D)
- System architecture and **FFFIS of IxL-RBC, IxL-LEU and IxL-IxL** interfaces. Final recommendations on fallback and migration strategies - (WS E)
- **Test tools and techniques** enabling the testing and commissioning of signalling applications including INESS products – (WS F)
- **Methods & support tool** for an efficient implementation of the Safety Case Process. Trial in a real railway project and feedback of 4 NSA's - (WS G)

INESS has achieved a complete specification work and tool chain fully exploitable for the implementation of an INESS IxL

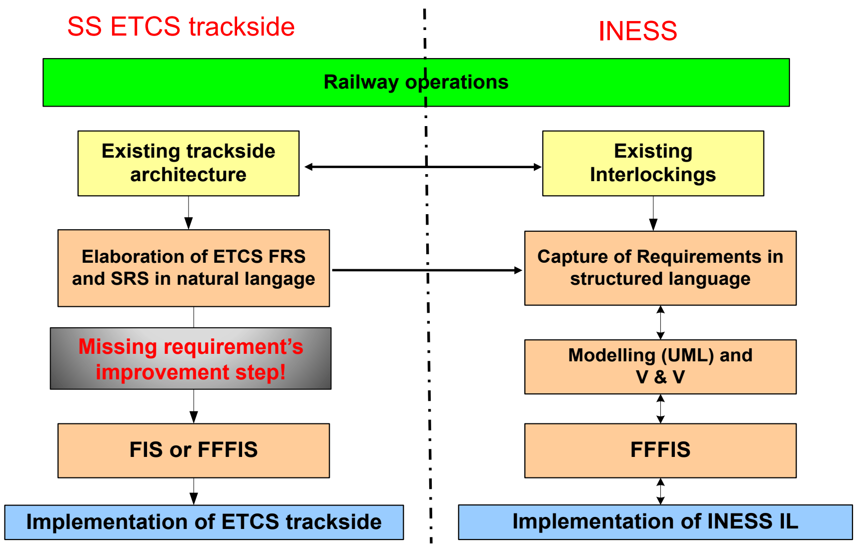
INESS – Innovative specification and design concept

iness

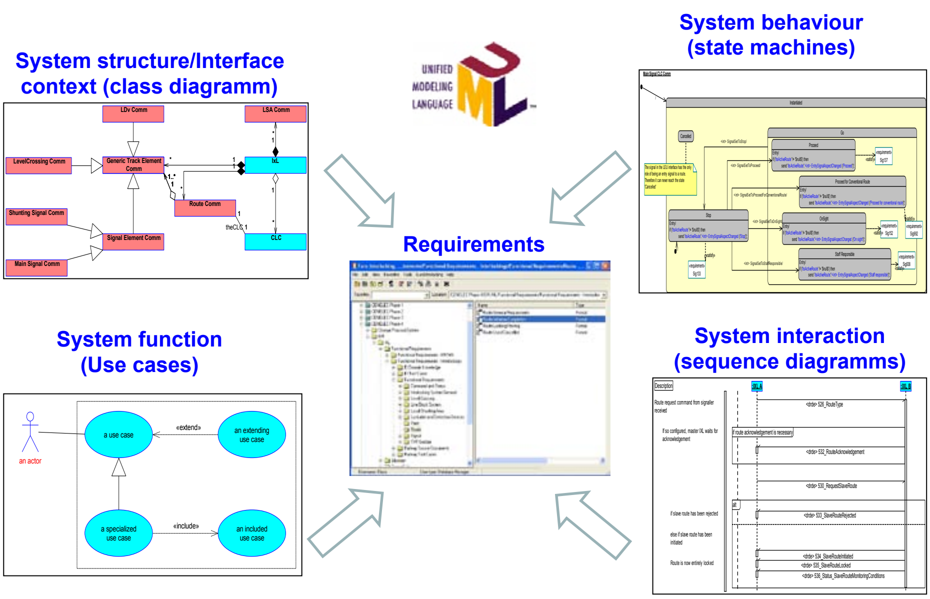
Traditional approach | INESS approach



INESS paradigm - the use of model based methods

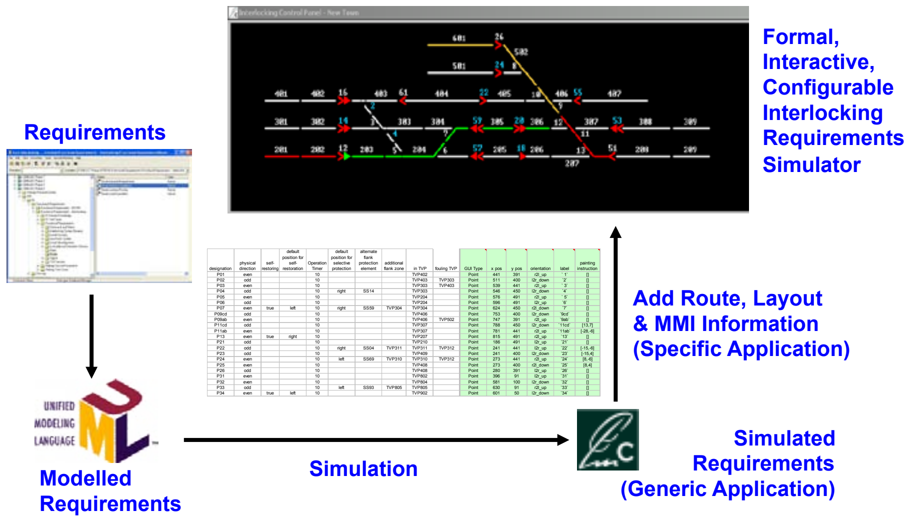


INESS – specification Methodology

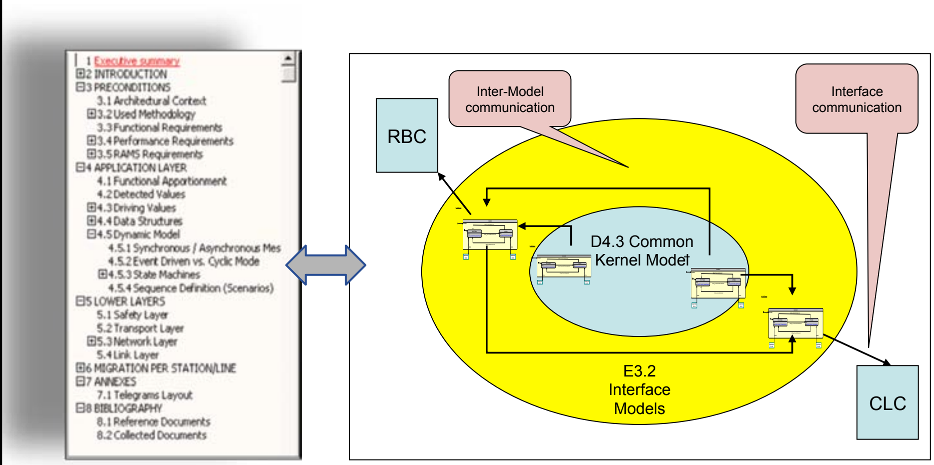


INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

INESS - functional requirements testing



INESS - FFFIS's standard format with linked Kernel + interfaces models



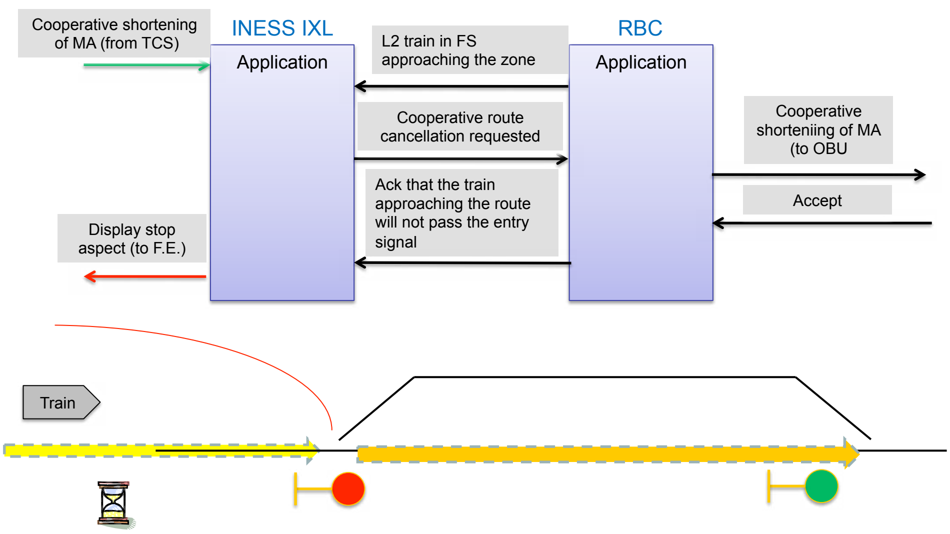
- FFFIS's structures are identical
- Models of Interlocking Kernel and INESS interfaces are kept in one place
- Kernel model communicates with interface models

INESS: Improved areas

INESS - improved areas

- Common understanding of both the technical and business needs for building an INESS IxL
- Enabling railway and industries to share "confidential" information
- Harmonisation of IxL's behaviour with ERTMS systems and reversely
- Applying model based methods and tools using the railway knowledge
- Framework setting for an efficient migration toward ERTMS

Interface Interlocking-RBC – Scenario Cooperative shortening of MA



INESS: Next steps

INESS - Expected impact

iness

Expected impact

1. Based on INESS FFFIS concept, remaining
Field obje
specified
2. Possibilit
cases for
in order t
conformit
3. Due to its
is a high
Kernel ac
more tha
4. ERTMS
allows op
functiona
5. Faster EI
- ...

Future use

1. Based on INESS FFFIS, remaining
uld be
BC's
ation
faces
S
al
ment to

- Accelerate testing and commissioning of ERTMS equipments (RBC's, OC's...)

INESS has developed the necessary background and tool chain to:

- **Improve the interoperability of various systems (RBC's, LEU's...) with IxL's**
- **Allow easy implementation of remaining interfaces**
- **Allow automatic testing of the interfaces specification in a lab environment**
- **Build an INESS compliant IxL functional prototype allowing RBC's optimization and delivering error free sytems**

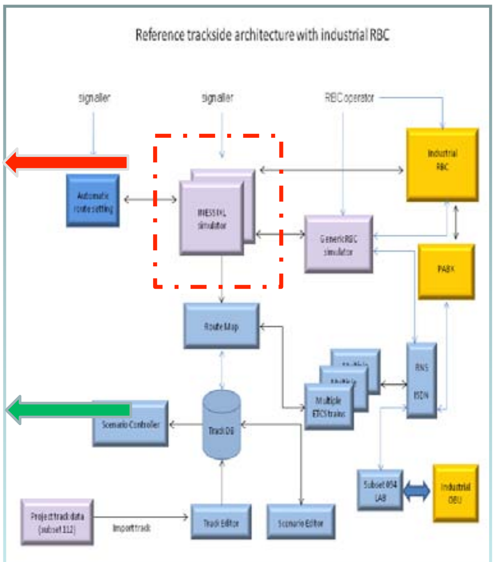
INESS – Maintenance of the results

iness

- Common Kernel DOORS on the UIC DOORS server. Maintenance licence bought for 5 year. UIC will maintain.
- Kernel and interfaces model on Artisan. Contract maintenance with ATEGO for 5 years. UIC will maintain.
- The INESS Datamodel will be further developped and maintained by a community composed of RailML and railway specialists. UIC will coordinate.
- WS G SaCaPro support tool: Open Source
- An INESS baseline compatibility matrix will be included in the Concluding Technical Report .
- Deliverables :
  - ALL ⇨ Myndsphere ⇨ 5 year access (UIC+ALMA)
  - Public ⇨ INESS site. Unlimited access

INESS – Technology Readiness Level

- **TRL9:** System qualified through successful operation
- **TRL8:** System qualified through test
- **TRL7:** Prototype in operational environment
- **TRL6:** Prototype in relevant environment
- **TRL5:** Component validation in relevant environment
- **TRL4:** Technology component validation in lab
- **TRL3:** Analytical/experimental proof of concept
- **TRL2:** Technology concept formulated
- **TRL1:** Basic principles observed



INESS - Benefits for railway and industries

INESS Dissemination

INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

INESS - Dissemination

[D H 1.1 http://www.iness.eu/](http://www.iness.eu/)
Web-site has been visited 15.677 times (19 January 2012)

D.H.1.2 INESS Brochure

D.H.1.5 Dissemination materials : INESS Poster

D.H.1.5 Dissemination materials : Presentation in related Conferences

D.H.1.6 INESS Publications

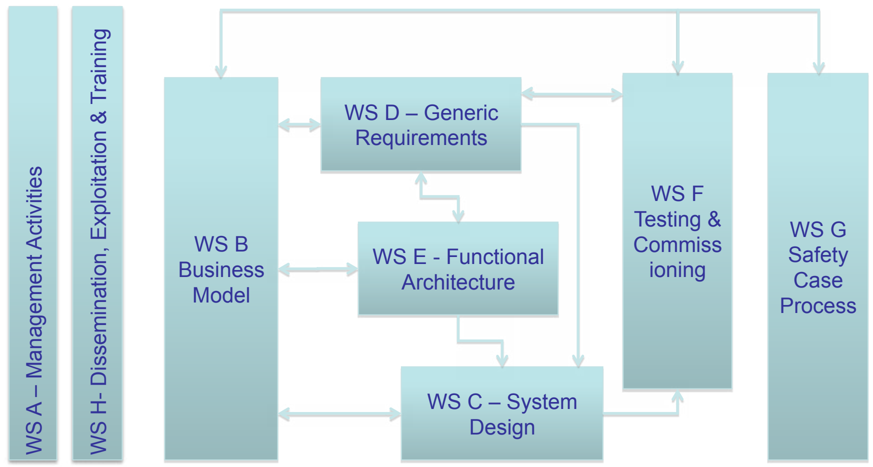
D.H.1.5 Dissemination materials : INESS Flyer

D.H.1.5 Dissemination materials : INESS Bulletin Board

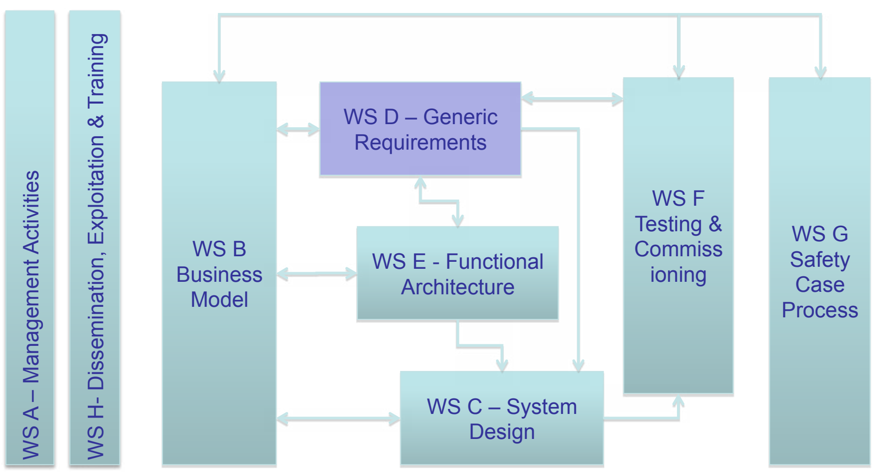
INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

INESS - Dissemination

Enjoy your training!



INESS Generic Requirements WS-D



Introduction

1. Presentation of:
   – The common core development process
   – Detailed presentation of the Common Kernel
   – Detailed presentation on Verification
2. Discussion
3. How to use the Kernel

Introduction

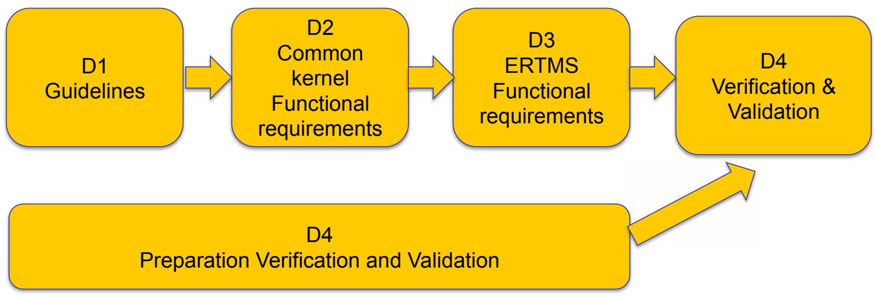
Differences in interlocking system functionality:

- historical developments, regional interlocking suppliers
- implementation constraints
- human behavior
- resulting operational rules

Where are our chances:

- common requirements focused on functions, not on implementation
- revised operational rules by the railways
- greenfield projects (HS lines, complete resignalling projects...)

WS D Generic Requirements: Objectives and roadmap



WS D Setting up

Main Objective: The requirements database in a harmonised format and structure

- Several guideline documents
- Database set up

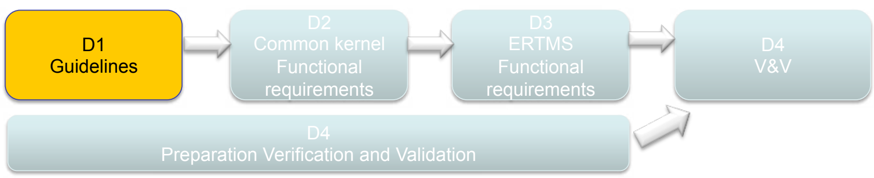
→

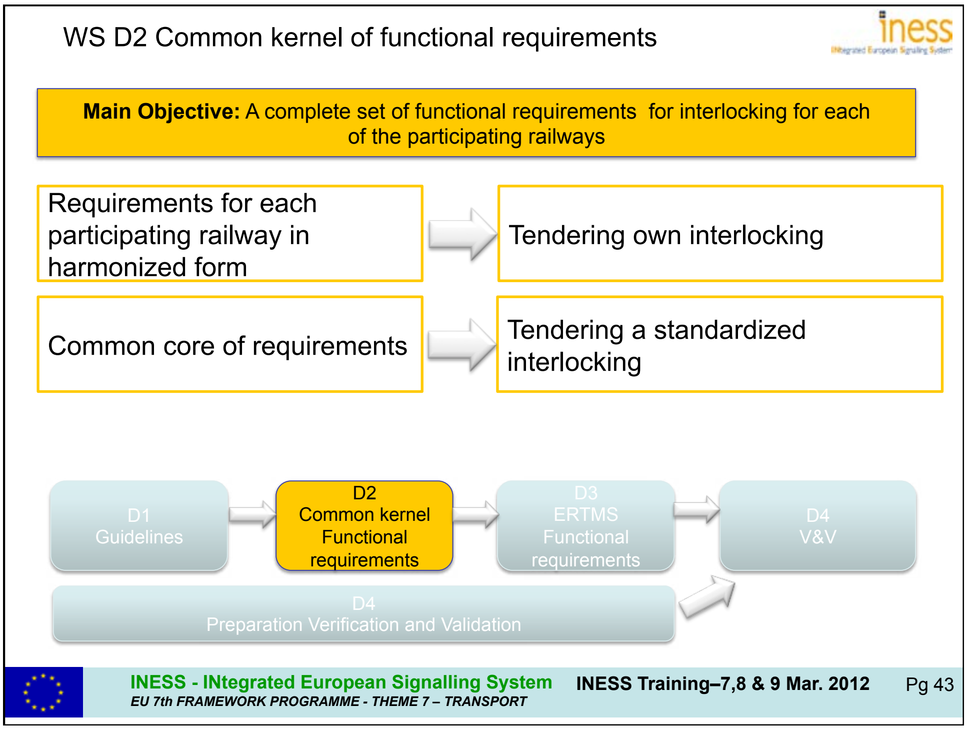
- Usable for setting up requirements databases
- Usable for modeling requirements

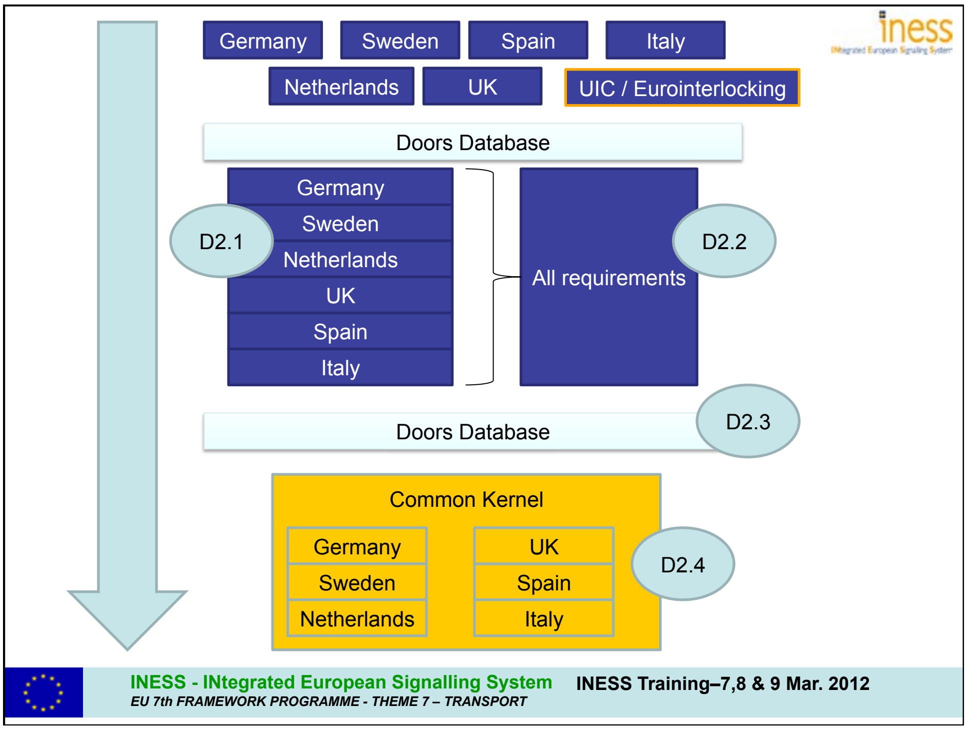
- Glossary of terms

→

- International communication tool




WS D2 Common kernel of functional requirements
iness
Main Objective: A complete set of functional requirements for interlocking for each of the participating railways
Requirements for each participating railway in harmonized form
Tendering own interlocking
Common core of requirements
Tendering a standardized interlocking
D1 Guidelines
D2 Common kernel Functional requirements
D3 ERTMS Functional requirements
D4 V&V
D4 Preparation Verification and Validation
INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012
Pg 43


Germany
Sweden
Spain
Italy
Netherlands
UK
UIC / Eurointerlocking
iness
Doors Database
Germany
Sweden
Netherlands
UK
Spain
Italy
D2.1
All requirements
D2.2
Doors Database
D2.3
Common Kernel
Germany
Sweden
Netherlands
UK
Spain
Italy
D2.4
INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

WS D3 Elaboration of ERTMS requirements

Main Objective: A common kernel of validated standardised requirements for future interlockings including functionalities required by ERTMS level 1 and 2

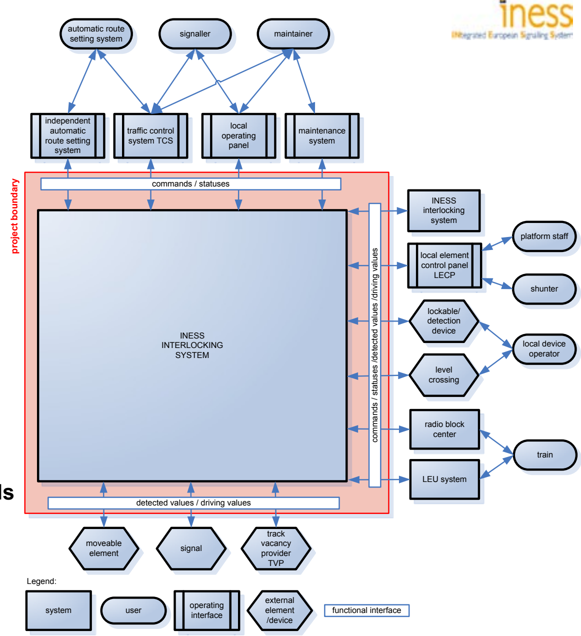
Common core of requirements including ERTMS → Tendering a standardized interlocking for ERTMS level 1 or level 2

D1 Guidelines → D2 Common kernel Functional requirements → **D3 ERTMS Functional requirements** → D4 V&V

D4 Preparation Verification and Validation

Scope

- **ERTMS baseline 2.3.0d**
- **Excluding: the RBC and LEU system**
- **Including:**
  - **Functional Interface between interlocking system and RBC/LEU**
  - **Transitions between levels**



How can it be checked in practice that the written requirements themselves are consistent, complete and correct?

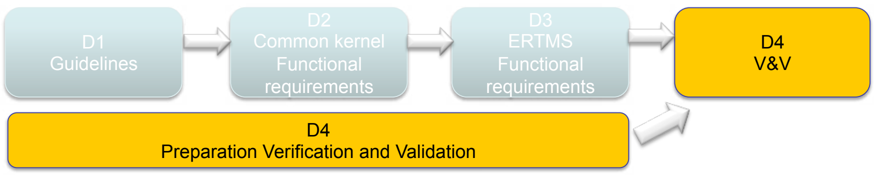
Verification and Validation of the requirements

WS D4 Verification and validation

Main Objective: Common method and tooling for verification and validation of the functional requirements

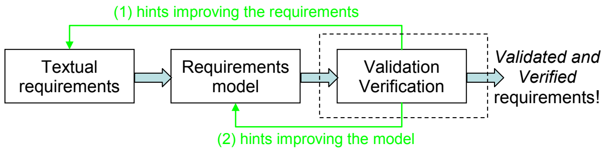
Method for validation → Improved INESS requirements
Method usable by railways
(although not easily)

Methods for verification → Improved INESS requirements
Method usable by specialists;
xUML modeling skills are needed



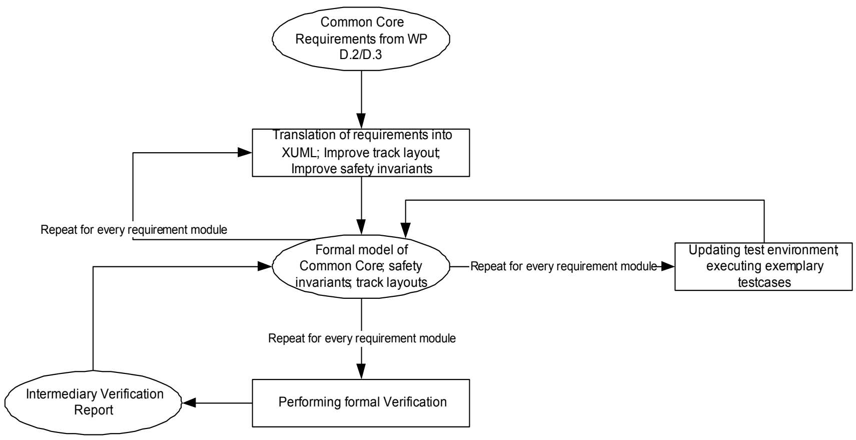
Methods used

- Requirements review
- Requirements verification and validation based on models



INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

Verification & Validation



INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

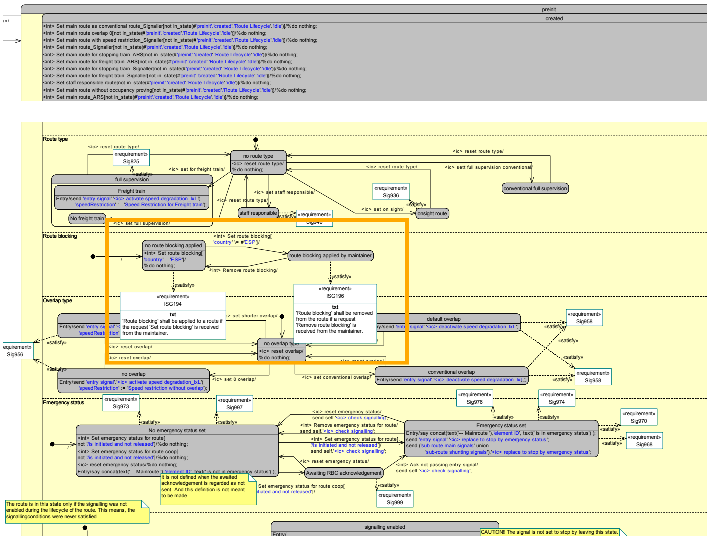
Validation

- *Validation* of a specification is that the textual functional requirements are actually those desired.
- Two problems:
  - This cannot be exhaustive due to the complexity of the task.
  - Having test-cases to help validate requirements and not to self-test against the requirements specified in the database.

Verification

- *Verification* of a specification is: the process of assessing that the specification meets a number of stated properties.
  - checking meta-properties of the specification, such as well-formedness, consistency, completeness and freedom of deadlock; and
  - checking identified high-level (emerging) properties that the specification is expected to satisfy

xUML model



INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

Insight in the Common Kernel
by Mirko Blazic

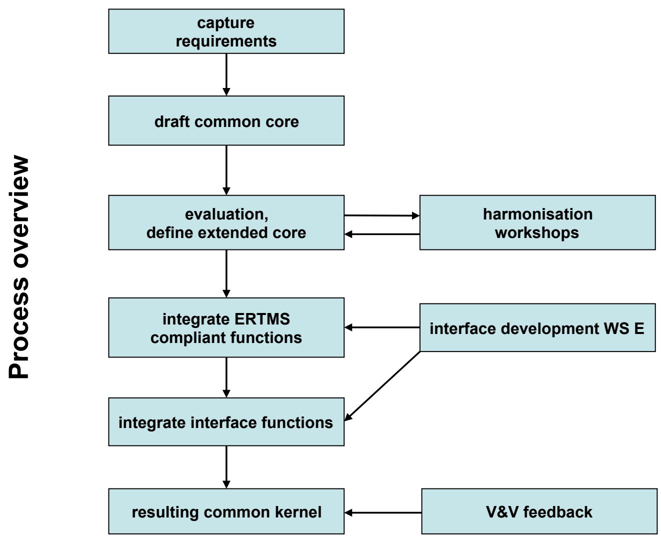
INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

Common Kernel development

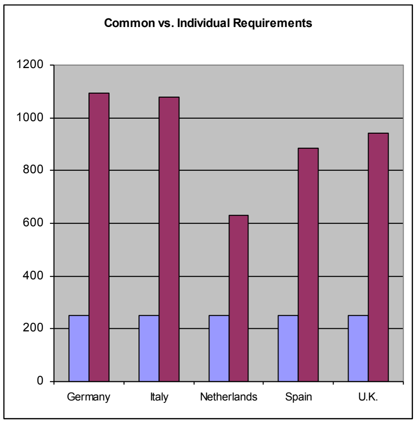
Starting steps:

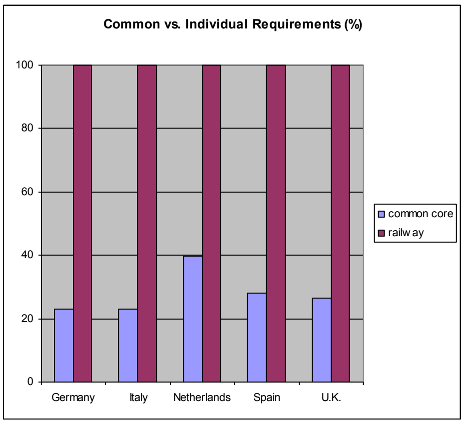
- setting up a requirements database in order to keep requirements of participating railways in comparable format
- establishing a glossary of terms to make sure we all refer to correct terms
- capture the requirements of individual railways (around 2500 requirements in the database, 6 INESS railways + Euro-Interlocking input)
- find common requirements (common core)

Common Kernel development



Starting status of the captured requirements

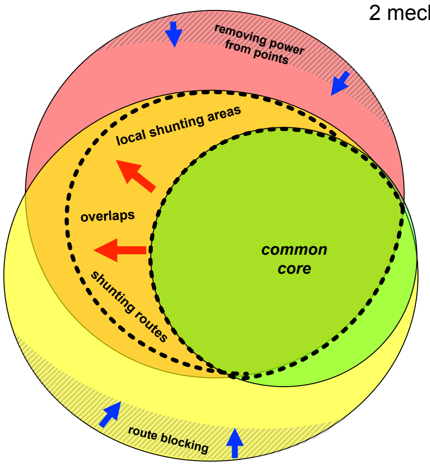




>number of requirements per railway: 630 Netherlands - 1092 Germany
>common core requirements 250
>common core covers 25 – 40 % of individual railways requirements

Common core methodology

2 mechanisms in developing the common core:



1. ***extending the core***
   >more functions would be included in the common core
   >certain functions would be redundant and not used for some railways

2. ***minimising the individual functions***
   >removing special individual functions
   >harmonising certain individual functions, thus moving them to the core

Common Kernel development

1. Extending the common core

Criteria for selecting a subset that would extend the common core:

- functions have to be used by multiple railways
- some functions may be used by a single railway, but only if no alternative exists or operation without such a function is not possible
  (approach delay of signals)
- traffic operation would become too complex without such functions
  (overlaps, shunting routes, local shunting areas)
- functions lead to increase in availability and performance
  (selective protection points, level crossing operation, route cancellation with approach zones)

Common Kernel development

2a. Minimising the individual functions by removing functions

Criteria for selecting a subset that would be removed:

- functions which compensate for the use of outdated or specialized equipment
  (line block functions, coupled points, key-locked points on the line, tunnel gates)
- functions which compensate for outdated regulations
  (self restoration of points, removing power from points)
- functions which are not safety relevant and can be moved to another system
  (composite routes, automatic route setting, alternative route setting)

Common Kernel development

2b. Minimising the individual functions by harmonising functions

Criteria for selecting a subset for harmonisation and moving to the core:

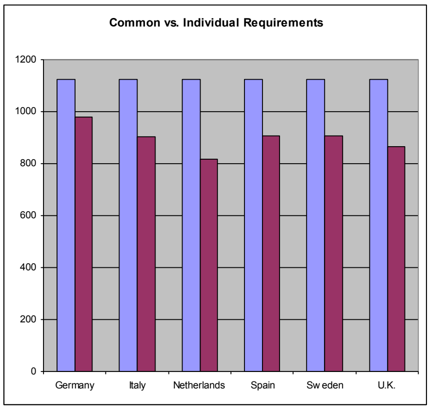
- functions used by a few railways, in a similar way
  (route blocking on tracks, points, signals..., route cancellation, train operated route release)
- functions that have existing alternatives which achieve the same result
  (point operation, fouling)

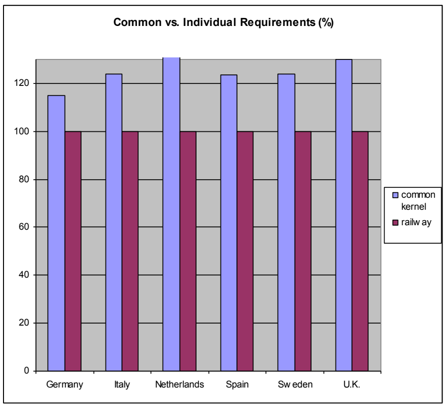
Harmonisation Highlights

Common Kernel for conventional applications:

- Fully functional interlocking containing all functions required to operate traffic
- Routes were harmonised into 3 types of main routes and 1 type of shunting route
- Route definition is a matter of configuration
- Route setting, rejection, locking and releasing have been harmonised
- Route setting on the line is proposed to replace the line block functions
- Key-locked elements were harmonised with lockable devices
- Level crossing functionality has been harmonised to be as generic as possible and aims to cover the majority of level crossing situations
- Signal aspects and indicators have not been considered for harmonisation

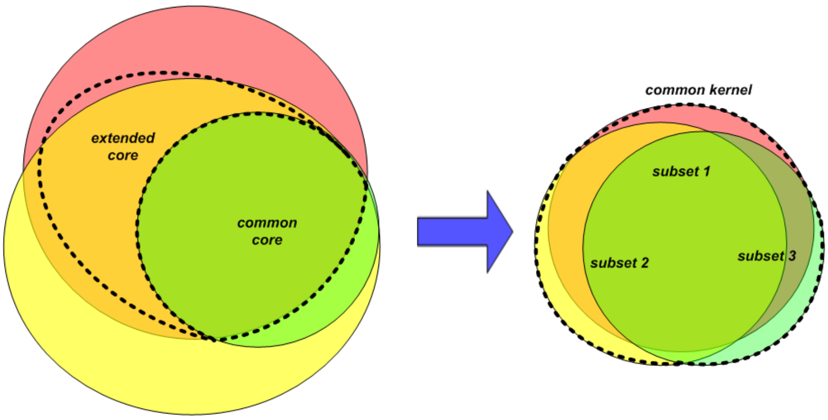
Common Kernel statistics





>number of requirements per railway: 818 Netherlands - 978 Germany
>extended common core requirements 1123 which form the **common kernel**
>extended common core covers 115 – 135 % of individual railways requirements
>successful harmonisation: reduction from 2500 overall requirements to 1100 requirements!

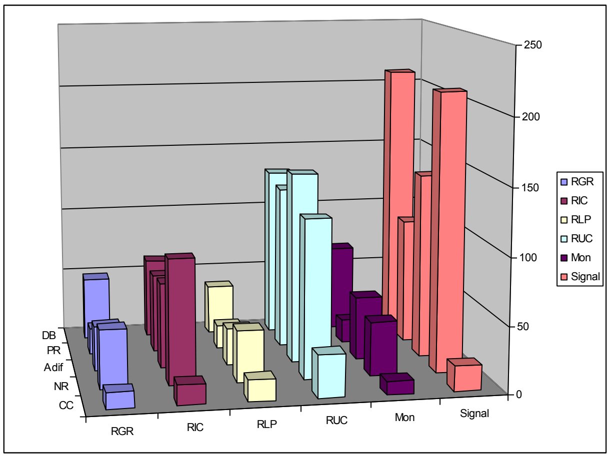
Resulting Common Kernel



The common kernel contains all requirements, which are in practice 6 subsets for 6 INESS railways.

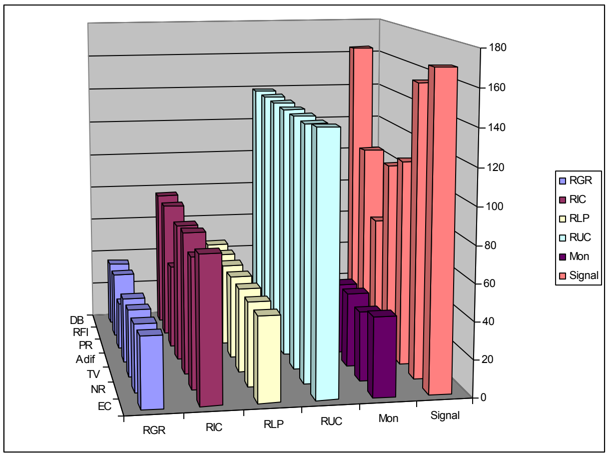
iness

Common Kernel statistics



iness

Common Kernel statistics



ERTMS compliant common kernel

Adding functionality to the common kernel for ERTMS compliance:

- ERTMS functions were compiled and examined based on experience
- relevance of each function was considered against the harmonisation criteria
- harmonised functional requirements were developed and integrated to the common kernel

Interfaces

Adding functionality for interface support:

- requirements resulting from the work in WS E on interface development were added
- functional requirements supporting INESS IXL-RBC, INESS IXL-CLC and INESS IXL-INESS IXL interfaces are integrated in the common kernel

Summary

- fully functional interlocking system is described
- supporting conventional, ERTMS L1 and L2 application, including transitions between levels
- featuring “standardised” interface support for CLC, LEU and IXL

Deliverables

- D.2.3 Methodology on the common kernel development
- D.2.4 Composed common core
- D.2.5 Guideline which clarifies the relationship between the deliverables of D.2
- D3.2 ERTMS compliant functional requirements

All further use of common kernel requirements should be based on the INESS functional requirements database in DOORS, ensuring that proper application requirements set of an official baselined version is used.

Workshop: **How to use the common kernel**

Formal verification of the INESS model

Dr. Bas Luttik

Eindhoven University of Technology

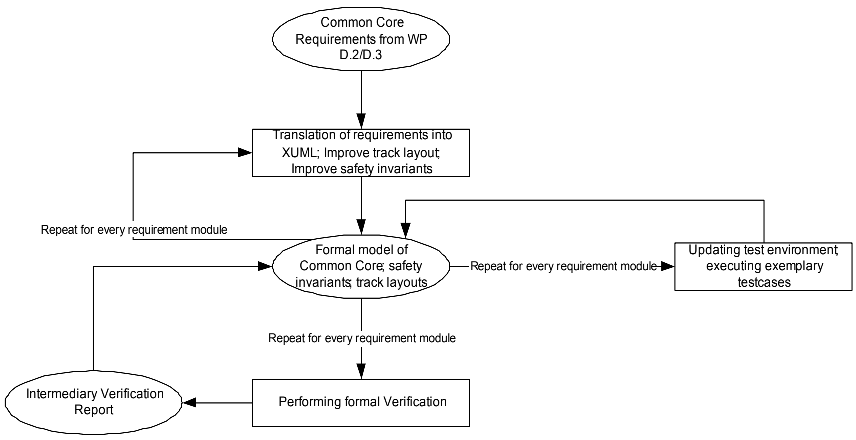
also on behalf of:

University of Southampton

University of Twente

University of York

Verification



Outline

1. Modeling and verification (general principles)
2. Developed tool chain
3. Application to INESS functional requirements
4. Conclusions
5. Small Demo (if time permits)

Goal

To analyze the INESS common core of functional requirements for

- Consistency

  Complex interplay of different requirements might bring system in error state

- Completeness

  The requirements are supposed to ensure certain high-level properties; are these properties indeed satisfied?

First step: make a **model** of the requirements

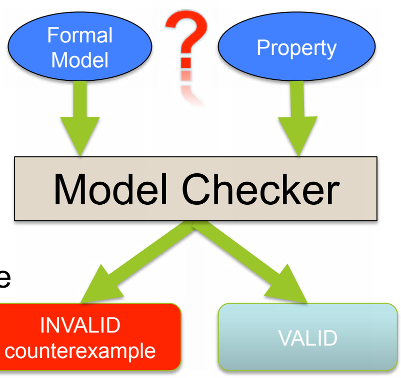
By a *model* we mean a precise description of the requirements in some *dedicated language*.

Some advantages of having a such a model:

- Less susceptible to different interpretations
- Makes consequences of implementation choices explicit already in an early stage
- Can be used to validate an implementation
- Facilitates automatic analysis

Formal verification by model checking

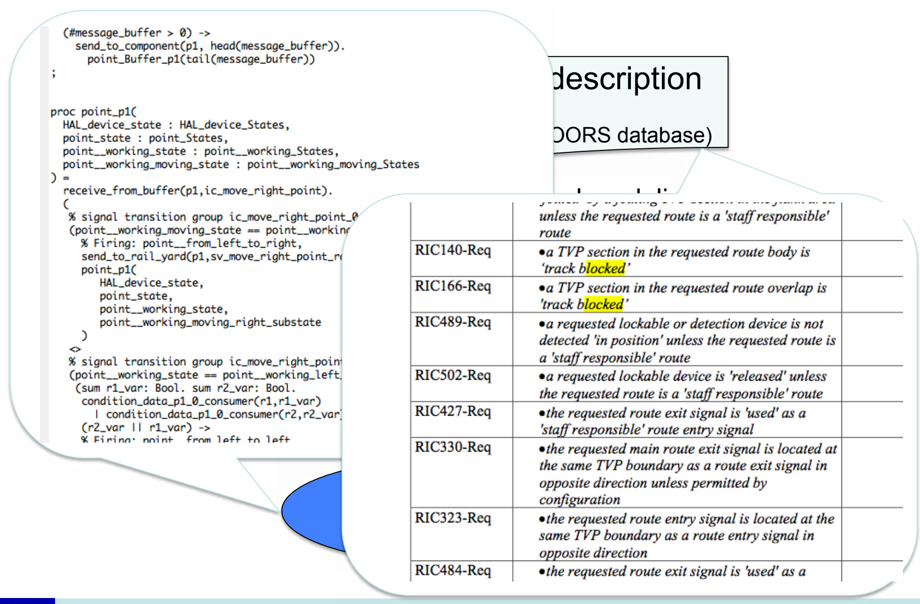
- A formal model describes the desired behavior
- Desired properties, e.g. safety invariants
- Verification Question: Does the model satisfy the properties?



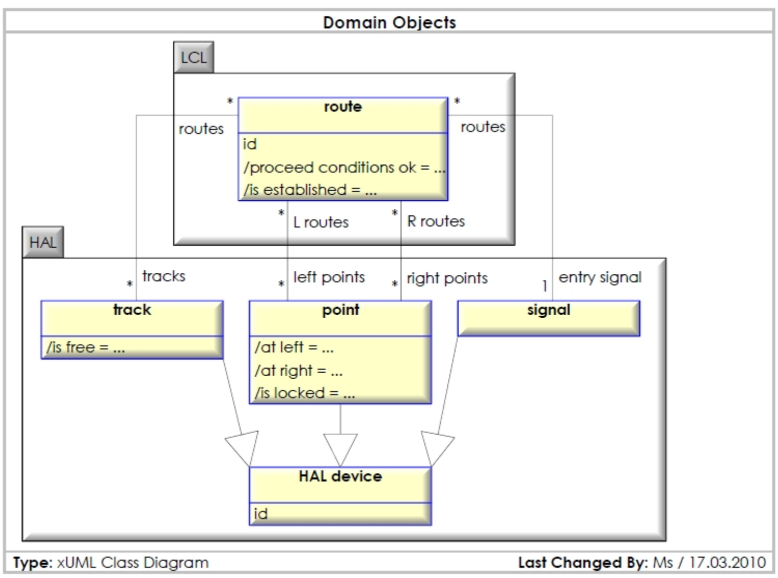
- Automatic verification:
  - Model checker
  - Based on exhaustive search
  - Provides yes/no answer
  - Generates a counterexample
    - trace through model

INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

How to obtain the formal model?

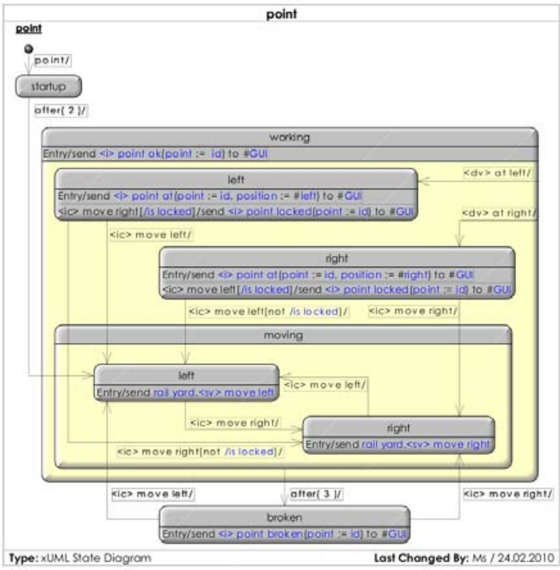


Micro 2010 Model: Class Diagram



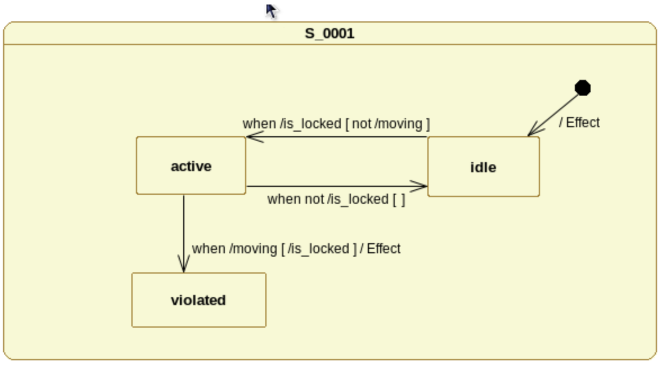
INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

Micro 2010 Model: State Machine

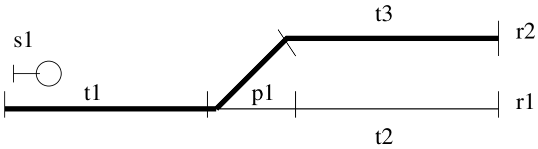


INESS - INtegrated European Signalling System INESS Training–7,8 & 9 Mar. 2012
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT

Micro 2010 Model: Property and Track Layout

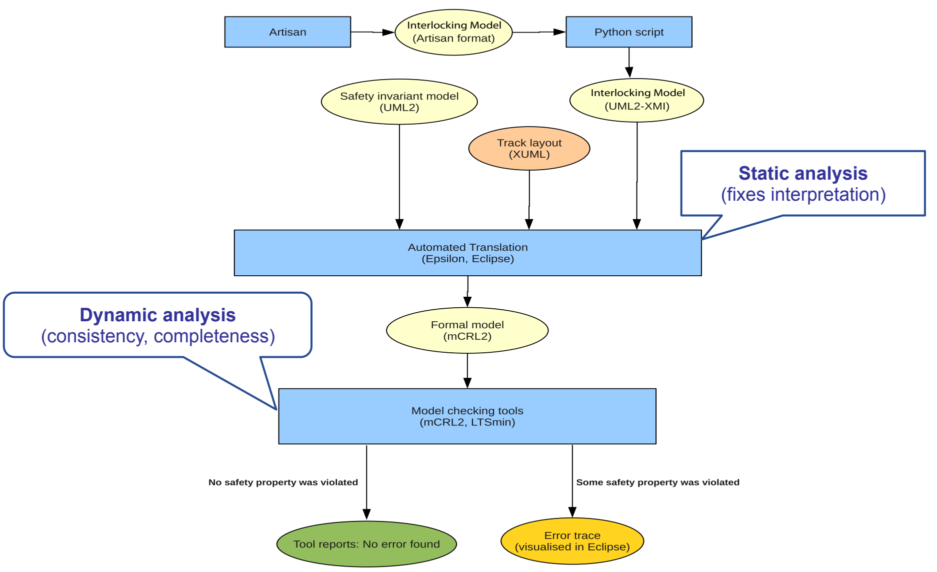


S 0001: "A locked point shall never move".



INESS - INtegrated European Signalling System INESS Training–7,8 & 9 Mar. 2012
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT

Tool chain architecture:



Running our tool on the common core model:

Our tool:

1. Performs **static analysis** on the xUML model
2. Translates it into an mCRL2 model
3. Runs **dynamic analysis**.

It turns out that the xUML model is so big and complex that we are still working together with the modeling engineers to get the entire model past stage 1.

Nevertheless, we got parts of the model past stage 1; did some dynamic analysis on those parts, and this resulted in some additional feedback on model and requirements.

INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

Some results of verification activities:

1. **Static analysis** produced a lot of feedback to the modeling engineers regarding
   - Modeling style (only use constructs with unambiguous semantics)
   - Technically correct expression of requirements (syntactic and type correctness)
2. **Dynamic analysis** revealed
   - deadlocks in early versions of the model
   - incompleteness of textual requirements
3. Proof (at least for an early version of the model) that the initialization phase resulted in a unique state

INESS - INtegrated European Signalling System INESS Training–7,8 & 9 Mar. 2012
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT

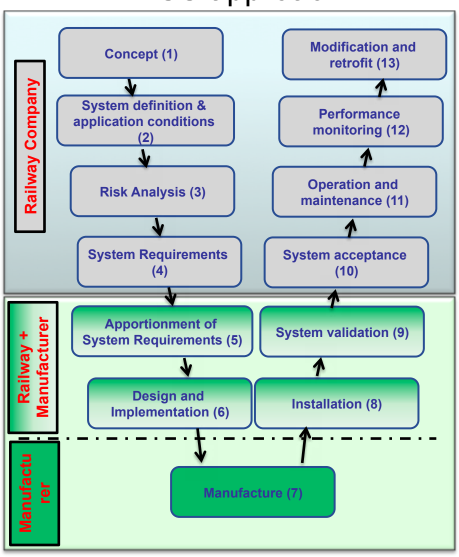
To conclude

It is impossible to overlook the consequences of the complex interplay between the functional requirements just by having specialists inspect them.

Making a model of the requirements facilitates analyses in the design phase, using verification tooling to support the modeling and the analysis.

A thoroughly analyzed model will be a very valuable asset in the requirements, design and implementation.

INESS approach



INESS - INtegrated European Signalling System INESS Training–7,8 & 9 Mar. 2012
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT

Conclusion & challenges

- Requirements of interlockings are defined and verified and validated by state of the art techniques.
- Verification and validation techniques have to be adapted to more ease of use.
- Requirements have to be maintained.
- Challenge is to go from requirements to more INESS compliant systems.

Further Reading

- All documentations of WS D are confidential
- All documents available for consortium members.

Discussion

How to use the Common Kernel
by Mirko Blazic

How to use the Kernel?

- Database Structure
- Requirements Structure
- Functional Requirements
- Further Reading

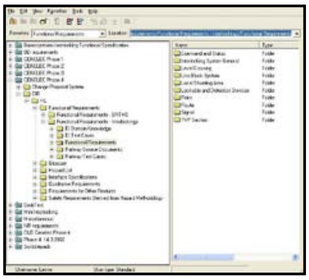
Common kernel functional requirements

Basic principles

- The goal was to capture the functional requirements of the participating railways, and develop the common kernel based on the captured requiremens
- DOORS requirements management tool is used to capture and manage the functional requirements
- Unified glossary of signalling terms to ensure all experts are understanding the meaning of requirements
- Requirements structure to keep the requirements as uniform and understandable as possible
- Requirements syntax to maintain the consistency of the requirements database

Requirements have to be described in a comparable manner!

Database structure



Identifier		Applicable To
RIC33-Com	2.1 Main Route Definition	
RIC34-Req	The main route shall consist only of the following route elements:	Denmark Finland Italy Netherlands Norway Poland Portugal Switzerland U.K.
RIC35-Req	• *the main route entry signal*	Denmark Finland Italy Netherlands Norway Poland Portugal Switzerland U.K.

Software used : DOORS (requirements management tool)

→ designed to capture, link, trace, analyze and manage a wide range of information

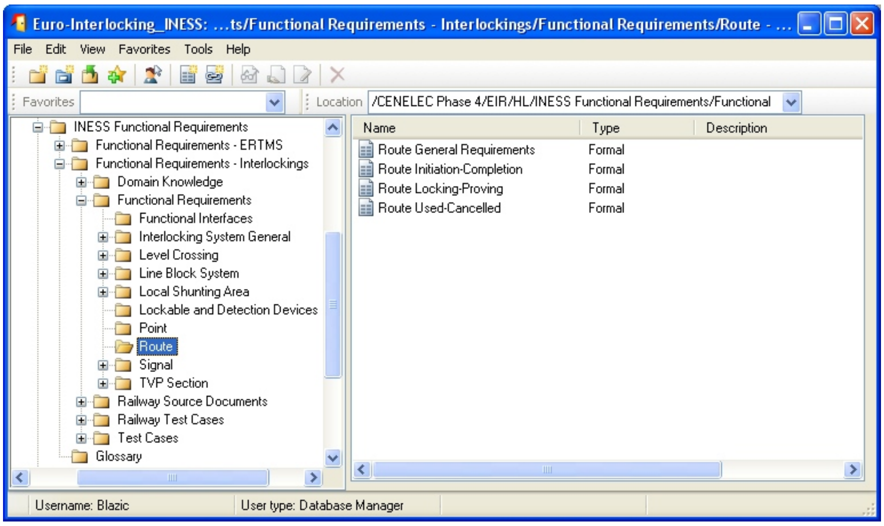
→ requirements and related information are stored in different modules in a central database

→ folders are used to organize the modules in the database in the same way as folders are used to organize computer files.

Database structure

- Modules are divided into objects
- An object is an individual requirement or a sub-requirement
- Each object has its own identifier, which does not change in the project lifetime
- Every change is automatically recorded in a historical log, includes the information about the user, the contents and the time of the change.
- Use of links provides good traceability and impact analysis across the database

Database structure



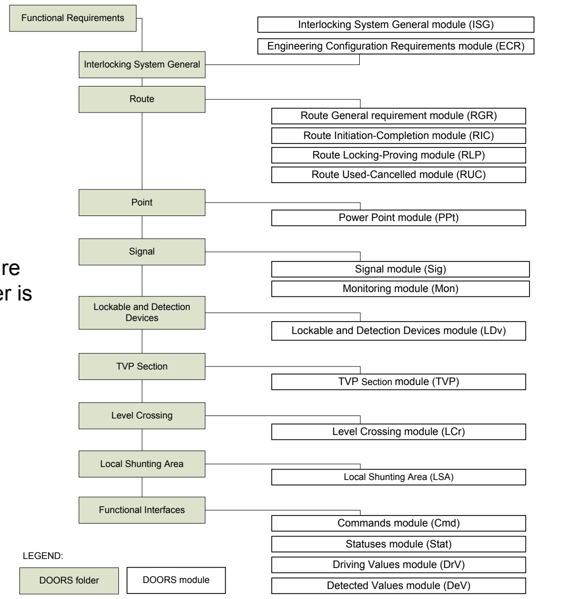
Database structure

The functional requirements are grouped in modules by logical interlocking concepts in the following manner:

Folder	***Description***
Interlocking System General	Interlocking System start-up procedures, adjacent systems, operation modes, configuration
Route	Requirements for setting, locking and using routes
Point	Requirements regulating powered points
Signal	Requirements regulating signals and monitoring
Lockable and Detection Devices	Miscellaneous lockable and detection devices such as key locked points, bridges, gates...
TVP Section	Requirements regulating TVP systems, including track circuit and axle counting types
Level Crossing	Functionality of level crossings from the perspective of the interlocking system
Local Shunting Area	Requirements describing the local shunting area
Functional Interfaces	Requirements for handling commands, statuses, detected values, driving values

Database structure

FUNCTIONAL REQUIREMENTS FOLDER STRUCTURE



A detailed overview of the structure of *Functional Requirements* folder is displayed on the diagram.

INESS - INtegrated European Signalling System **INESS Training–7,8 & 9 Mar. 2012**
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT

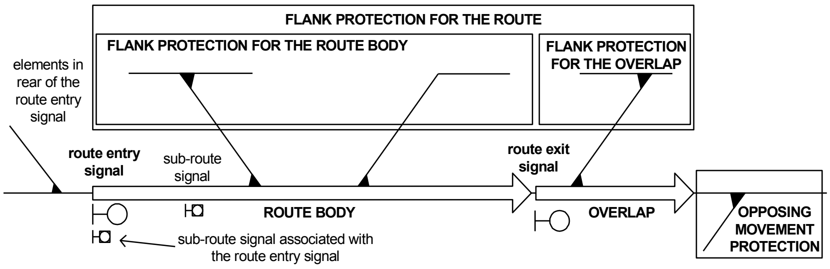
Unified Glossary of Signalling Terms

- Define the signalling terms used in the requirements
- Contains definition in English for all the signalling terms used in the functional requirements database
- Provides translations for these signalling terms in the different languages used by the railways involved in INESS
  (English, Italian, Swedish, Dutch, German and Spanish)
- Realized in close collaboration with signalling experts from the 6 railways involved in INESS
- Checked from a formal point of view by the UIC Terminology department

INESS - INtegrated European Signalling System **INESS Training–7,8 & 9 Mar. 2012**
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT

Functional requirements Domain Knowledge

- Created to support the functional requirements documents
- Explains some of the terms and concepts used for writing the functional requirements



INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

Requirements structure

1 requirement ⇔ 1 object in DOORS

Atomized requirements!

Basic templates as often as possible

<System> shall be able <action>
<System function> shall <action>
<System function> shall *<action>* if *<operational condition>*
<Element> shall become *<status>* if *<operational condition>*

PPt88-Req	The interlocking system shall be able to move points.
PPt614-Req	Reassignment of flank protection shall not disturb the monitoring conditions.
RUC162-Req	A route body element shall not become released ahead of a train.

RGR88-Req	A 'main' route shall be requested if a request 'Set main route' is received from the signaller.
RUC762-Req	An approach zone shall be assigned as 'occupied' if an occupancy that is considered as 'valid approach' is detected.

INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

Requirements structure

Use of indentation and logical connectors

Requirement R1:
- *condition C1*
  - *OR*
- *condition C2*
- *AND*
- *condition C3*

(C1 or C2) and C3

Requirement R1:
- *condition C1*
- *OR*
- *condition C2*
  - *AND*
- *condition C3*

C1 or (C2 and C3)

Sig393-Req	A main signal shall display a 'cancelled' aspect if all the following conditions are satisfied:
Sig431-Req	•*the signal is within an established local shunting area*
Sig852-Req	•*and*
Sig432-Req	•*the monitoring conditions of the established local shunting area are not disturbed*
Sig853-Req	•*or*
Sig854-Req	•*the signal is located in a route body*
Sig855-Req	•*and*
Sig856-Req	•*the 'signalling conditions' for the signal are satisfied*

Requirements structure

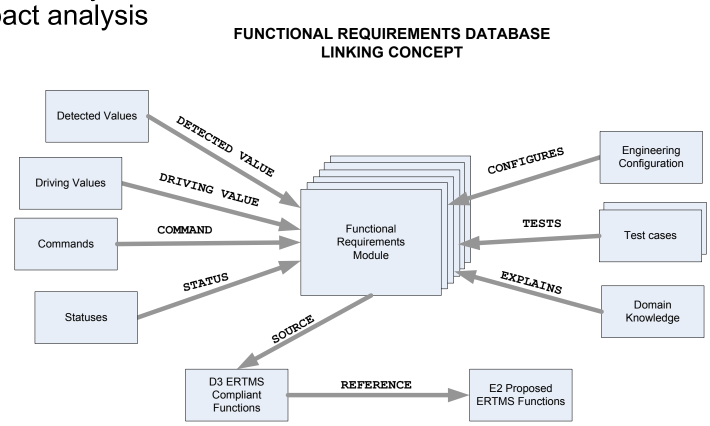
- Requirements syntax: To keep the database and all contents consistent, certain rules have been implemented for the syntax of requirements.

Syntax Rule	Example
All words in headings are capitalized.	2.1 Setting a Local Shunting Area
Bullet points are not capitalized and are in italics.	•*points* •*derailers*
Commands are described as requests and are listed in quotes.	A request 'Set local shunting area' has been received from the signaller.
Aspects are listed in quotes.	Setting a signal to the 'stop' aspect.
Functional statuses defined by these requirements are listed in quotes.	'trailed', 'occupied', 'blocked', 'failed', 'detected', 'released', 'locked', 'route blocked', 'fouled', 'initiated', 'established', 'used', 'released for maintenance', 'automatic operation', 'manual operation'
The lack of a state is described as *not 'state'*	*not 'occupied', not 'blocked'* *Unoccupied, unblocked* must not be used.
Heading of a section not used in the common kernel remains visible in the final deliverable to indicate the omission of functionality.	

The linking concept

The use of links in the functional requirements database

- traceability
- consistency
- impact analysis



INESS - INtegrated European Signalling System

EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT

INESS Training–7,8 & 9 Mar. 2012

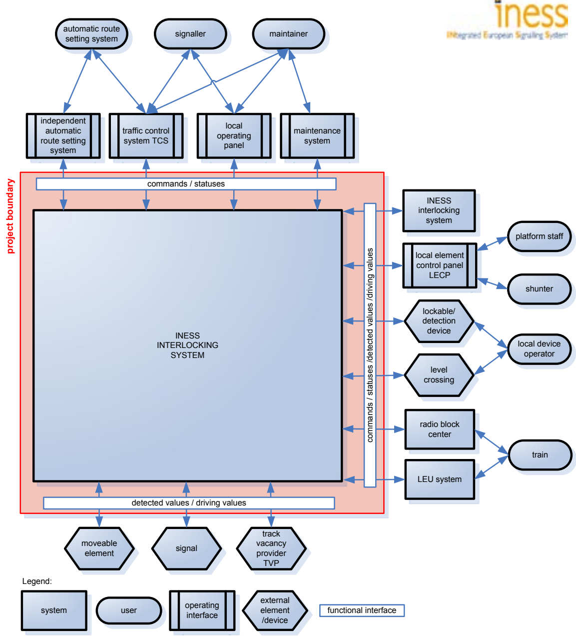
Common kernel functional architecture

> **presents the boundary of WS D work**

> **indicates users and operating interfaces referenced in the functional requirements**

> **indicates adjacent systems referenced in the functional requirements**

> **indicates the resulting functional interfaces**



INESS - INtegrated European Signalling System

EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT

INESS Training–7,8 & 9 Mar. 2012

Common kernel functional requirements

Presented information

Main attributes of each requirement (object) are:

- requirement identifier (unique identification of each requirement)
- requirement text
- comment
- linking/traceability information
- applicable to country (6 INESS participating railways)
- applicable application level (conventional, ERTMS L1, ERTMS L2)
- core rationale and core impact (rationale and impact of common kernel, if applicable)

Common kernel functional requirements

Displaying information

Based on attribute value, filtering can be applied into different views, which provides a subset of the common kernel requirements:

- views per each railway
- views per ERTMS application level

For example, the requirements defining a L2 application by Prorail can be obtained.

Common kernel harmonised contents

- the common kernel describes a complete functional interlocking system, where all necessary functions for traffic operation are included
- for the 6 railways of the INESS project, the kernel contains as subsets 6 fully functional interlocking systems;
- some functions that are in the common kernel will not be used by each railway – redundant functionality
- specific national functions, which are expected as not necessary for future use on new projects, have been omitted
- purely national interlocking requirements on national signalling aspects and national train protection were kept outside the scope of the harmonization process of INESS (harmonisation not possible, not rational)

Common kernel functionality

Route:

- full supervision route – normal operation route with full monitoring conditions, with complete overlap and flank protection
- on sight route – normal operation route used to send trains to an occupied track, no overlap, normal flank protection
- staff responsible route – degraded operation route, no overlap is set, all other available route elements are initiated and locked, SR aspect available if the path for the train is intact
- shunting route – normal operation shunting route
- other route features are set as full supervision route with a parameter (conventional routes, speed reduction, stopping train, freight train, no overlap)

Common kernel functionality

- route oversetting is supported
- dynamic overlap –overlap extending and overlap swinging
- route cancellation by use of approach zones and delay timers, and information from the RBC
- residual route cancellation
- cooperative cancellation by using the system function Cooperative Shortening of MA
- sectional route releasing by the train
- turnback route releasing
- destination track releasing
- overlap and destination releasing supported by train at standstill information from the RBC
- boundary routes (master and slave part) for IXL-IXL interfacing

Common kernel functionality

Local shunting area:

- local shunting area with flank protection
- dynamic setting of adjacent or overlapping areas

Moveable elements:

- automatic operation by route and local shunting ares
- manual operation for normal and occupied elements
- selective protection points – dynamic flank protection
- trailed status
- element blocking

Common kernel functionality

Level crossings:

- operation by route request
- operation by vehicle detection
- manual operation
- level crossing occupancy activation
- stopping train mode for stopping trains
- local mode

Signal/monitoring:

- route level aspects
- distant signals, repeaters
- various indicators
- signal supervision

Common kernel functionality

- blocking signals
- route emergency status
- route emergency status with Cooperative shortening of MA
- speed degradation as simple temporary speed restrictions

Monitoring conditions:

- monitoring conditions
- reclearing of route entry signals upon request

TVP section

- track blocking
- foul protection
- diamond crossing features
- axle counting reseting (sweeping sections)

Common kernel functionality

Lockable and detection devices:

- device releasing
- device blocking

General:

- IXL start up and shut down procedures
- interfacing to CLC, RBC and IXL
- L1 and L2 area entry and exit controls

Common kernel in practice

Use by INESS partner railways:

- common kernel is tagged for each of the railways and can be immediately used
- the high level impact analysis has been performed and is noted in the database
- as the national original requirements are already in the database, it is easy to analyze which requirements are not supported anymore or which have been replaced by other requirements
- operational rules have to be adjusted to match the changed functionality
- national signal aspects have to be aligned with the INESS route level aspects

Common kernel in practice

Use by non-INESS railways:

- the kernel is based on the main signalling “philosophies” from the INESS railways
- a review of the common kernel functional requirements is needed and an individual subset of the common kernel requirements has to be tagged
- an impact analysis has to be performed about the new or changed functional requirements, and especially about the existing national requirements not supported by the INESS interlocking
- operational rules have to be adjusted to match the changed functionality
- national signal aspects have to be aligned with the INESS route level aspects
- if the kernel is found to be not sufficient, adding national requirements has to be considered

Common kernel in practice

Considerations for adding national requirements:

- the kernel functionality has to remain unchanged (route life cycle...), otherwise the kernel becomes non-common, and thus not compatible with the standard INESS platform (interlockings and interfaces)
- functions necessary to resolve a layout issue should not be added, the layout of future applications has to designed to match the standard INESS interlocking
- functions which have an origin in a railway system issue (such as national signal or indicator, train control...) may be added, but as a separate function, not interfering with the core requirements
- maintenance of the common kernel requirements

  A managing body should manage and maintain the requirements through a change proposal system, otherwise the integrity of the INESS platform is lost!

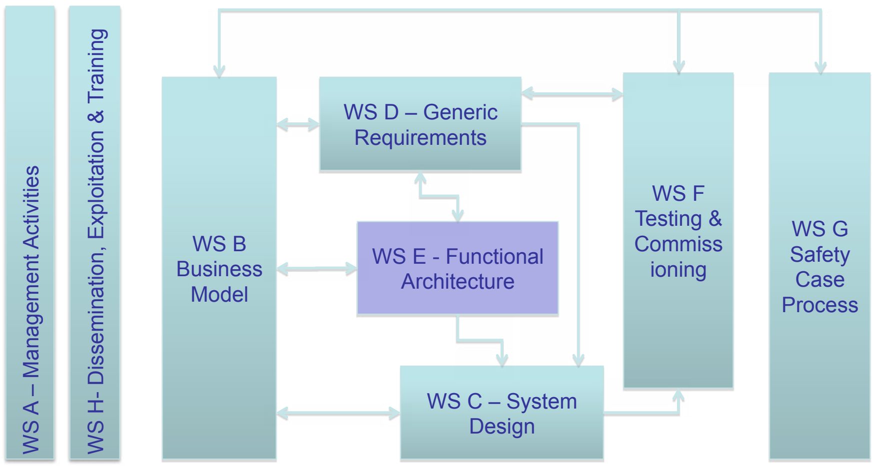
Further Reading

- D1.2 Requirements expression document
- D1.1 Unified Glossary of Terms
- D2.3 Methodology for developing the common kernel
- D3.2 Integration of ERTMS requirements (methodology)
- D3.2 Integration of ERTMS requirements ANNEX 1 (the common kernel requirements)
- D3.2 Integration of ERTMS requirements ANNEX 2 (domain knowledge)

Questions

INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

INESS Functional Architecture WS-E



WS E Functional architecture and interfaces

Training

By Jorge Gamelas, Emmanuel Buseyne, Tobias Lindner, Thomas Lauscher, Peter Winter

Collect information

- ❑ Collect information and assess the current architecture of signalling installations with regards to their functional configuration in the context of all their adjacent and neighbouring subsystems.
- ❑ Collect information and assess different current migration and fallback methods.

To be able to answer

How are functional interfaces made today?

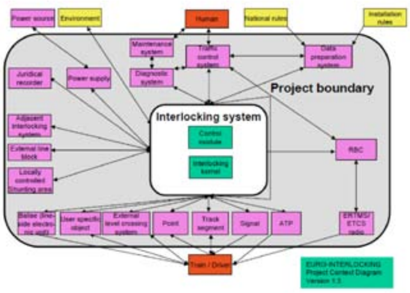
How is apportionment of functions and safety made today?

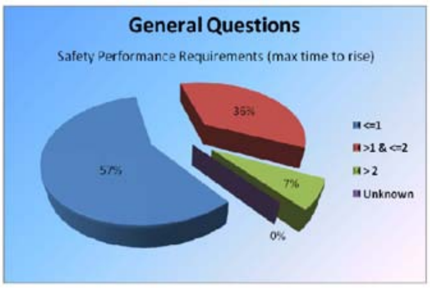
How much of the system is “standard”, supplier specific and railway requirements?

Are fallback systems used and if so, why?

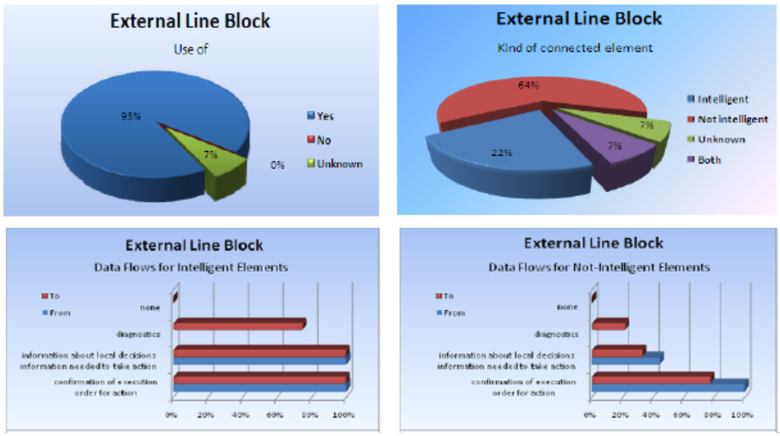
How is migration of trackside equipment made?

Collect information



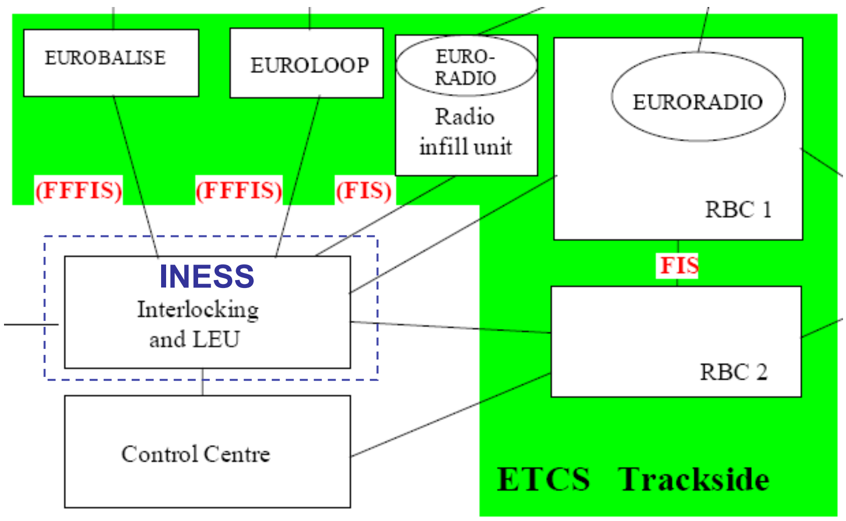


Collect information

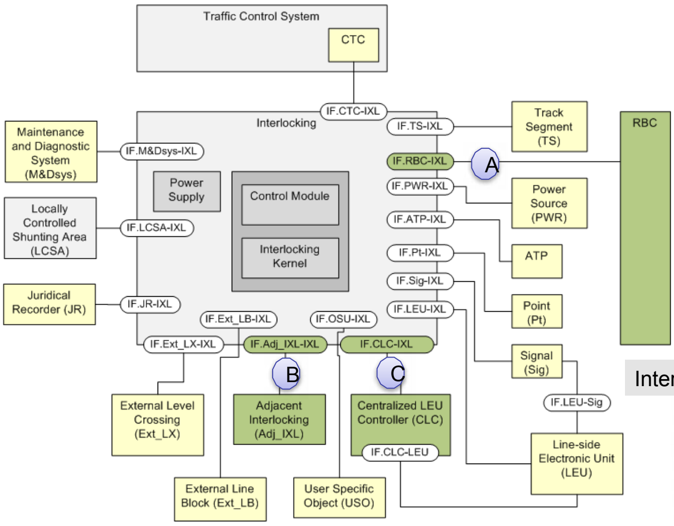


Picture 4 Graphs with Statistic of External Line Block

INESS and ERTMS



INESS reference architecture

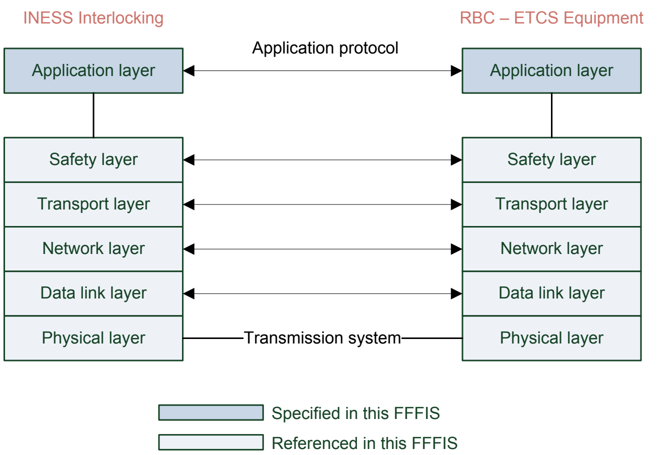


Interfaces to be harmonized

- A IXL – RBC
- B IXL – Adj. IXL
- C IXL – CLC (LEU)

Interface specifications

FFFIS Interlocking-RBC - Based on WS D functional specifications



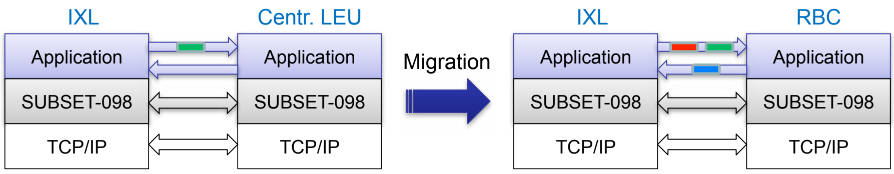
FFFIS document structure

- References to base documents (WS D common core, functional requirements)
- Interface requirements
  - System context
  - Application
  - Exchange of messages
  - Performance
  - RAMS
- Application Layer
  - Functional apportionment (e.g. message sequences)
  - Data structures (e.g. message structure)
- Lower Layers (safety, transport, network, data link and physical)
- FFFIS maintenanace

Function allocation - criteria

The following criteria were used to establish (in the group's view) an optimal function allocation:

Migration capability - To be able to roll out new components, products, systems or functions it is essential to consider the existing situation. At some point every new part has an interface to an already existing part. For example, a Centralized-LEU provides a subset of the RBC functionality.
Some railways might migrate ATP sections equipped with a Centralized-LEU (Level 1) to RBC (Level 2). To keep IXL communication consistent it is then advisable to keep the communication of these sub set functionalities the same for a centralized-LEU and a RBC.



Function allocation - criteria

The following criteria were used to establish (in the group's view) an optimal function allocation:

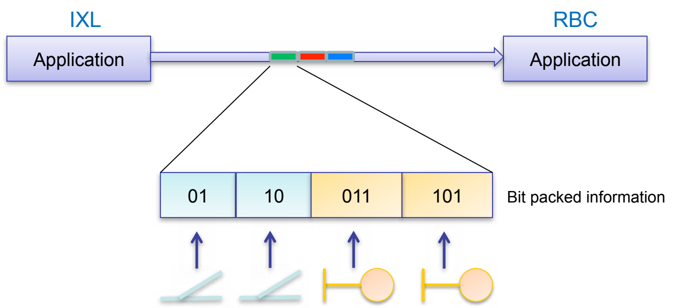
Avoid unnecessary time constraints or data mix-up - Do not split functions in such a way that dynamic behavior interacts with functionality. Time constraints, if possible, shall not be mixed with functionality.

E.g. Route cancellation performed by using closed loop.

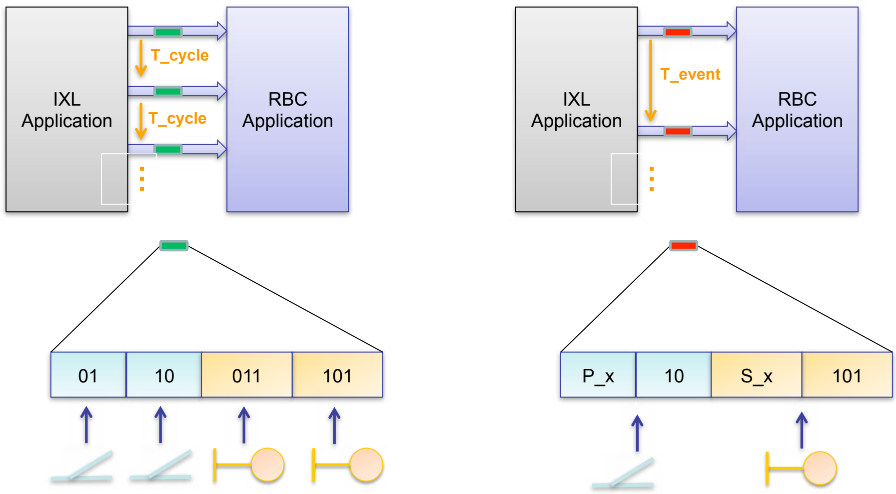
Function allocation - criteria

The following criteria were used to establish (in the group's view) an optimal function allocation:

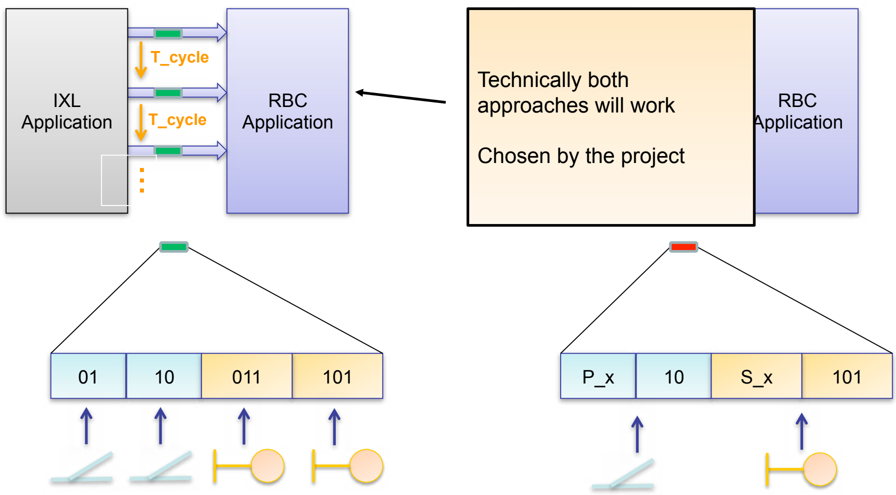
Keep Interfaces small - Minimize addressed partners and transmitted information, if possible. Small interfaces give clear responsibility, support migration and minimize functional interferences.



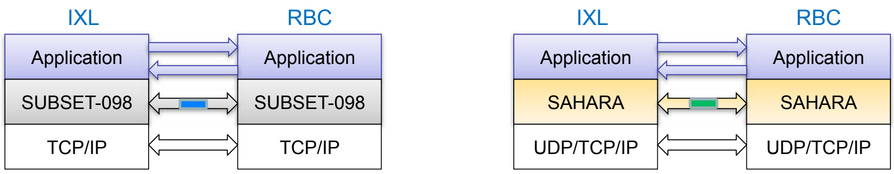
Cyclic versus event-driven



Cyclic versus event-driven



Safety & Communication layer: SUBSET-098 versus SAHARA

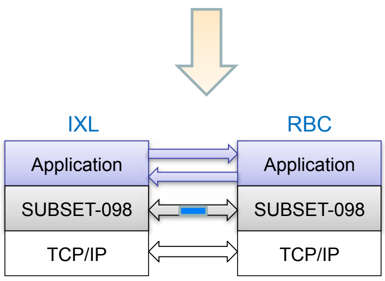


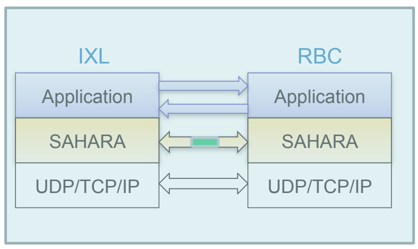
Technically both approaches will work

Both support cyclic and event-driven methods at the application level

Safety & Communication layer: SUBSET-098 versus SAHARA

Chosen by the project

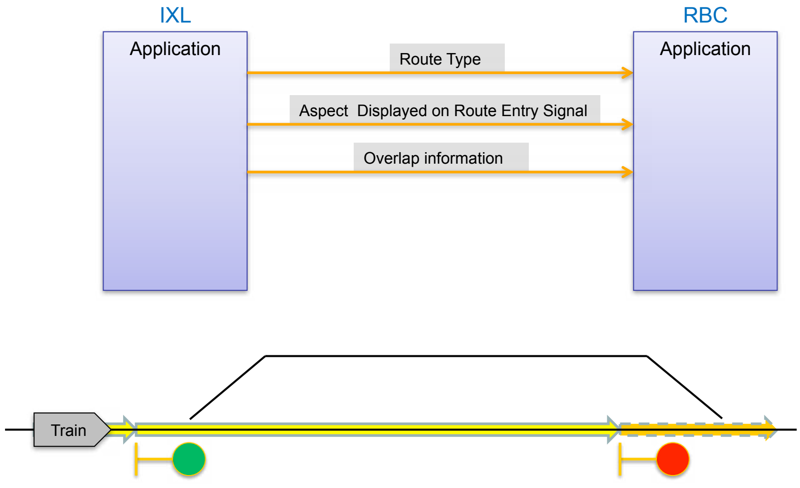




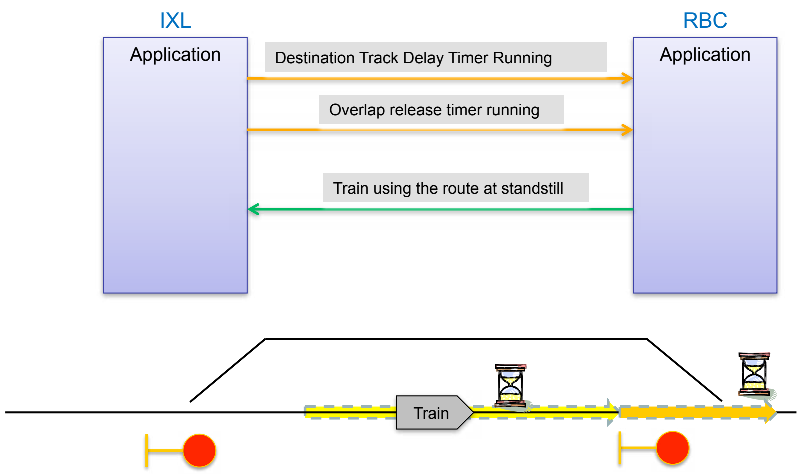
Interface Interlocking-RBC – Application layer

- Route information from the interlocking to the RBC (status, type, signal aspect, etc)
- Object status from the interlocking to the RBC (lockable devices, TVP sections)
- Level Crossing status from the interlocking to the RBC
- Supports cooperative route cancellation
- Destination track and overlap release based on standstill message from the train
- Shunting area establishment information from the interlocking to the RBC
- Supports entry/exit to/from ERTMS L2 area via interlocking/RBC cooperation

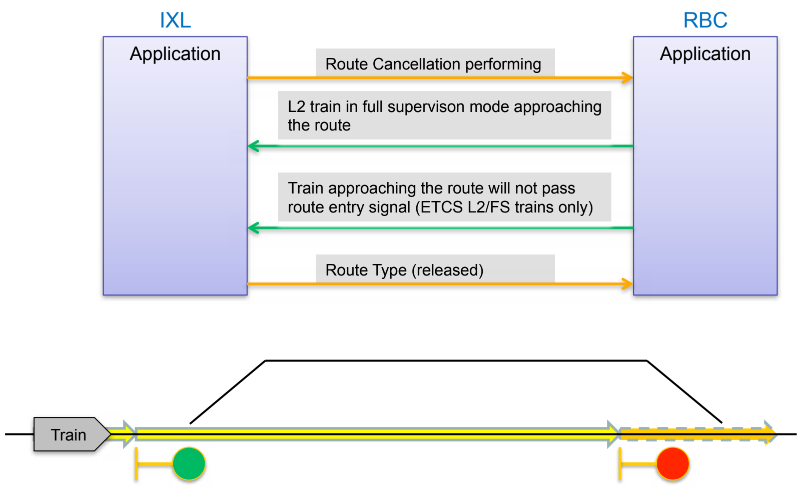
Interface Interlocking-RBC – Scenario Route Setting (simplified)



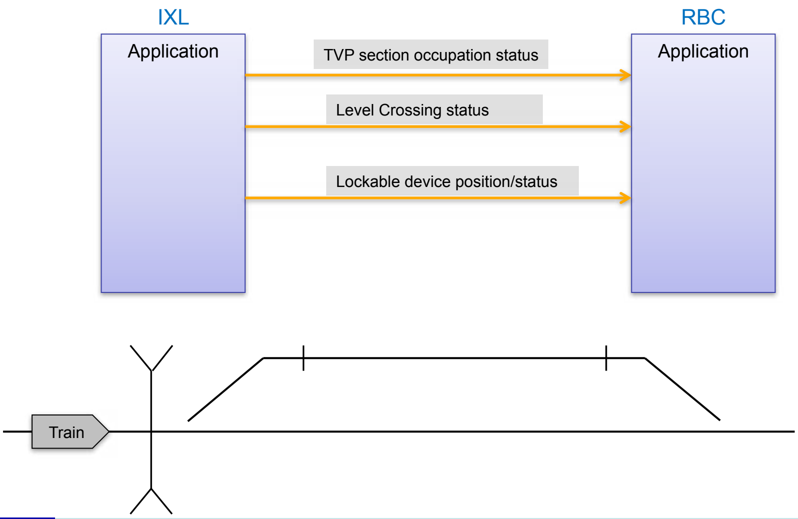
Interface Interlocking-RBC – Scenario DestTrack/Ovlp Release (simplified)



Interface Interlocking-RBC – Scenario Route Cancellation (simplified)

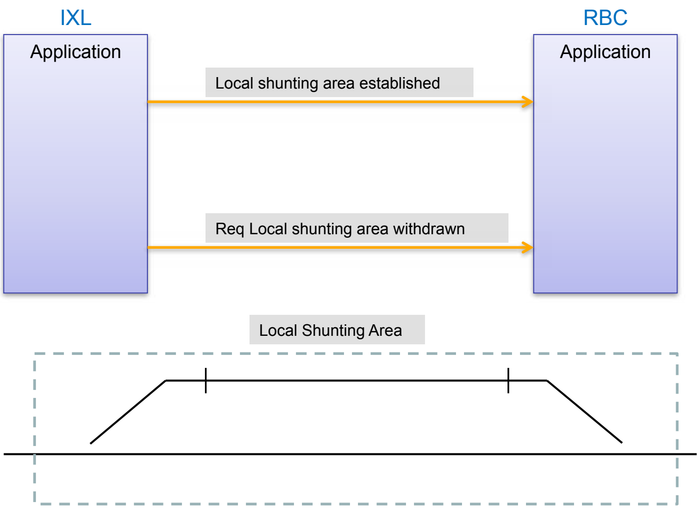


Interface Interlocking-RBC – Scenario Object Status (simplified)

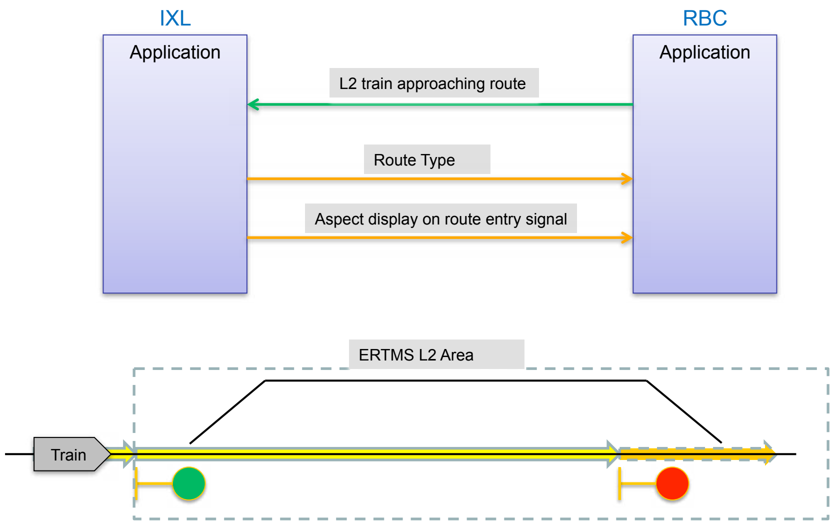


iness

Interface Interlocking-RBC – Scenario Local Shunting Area (simplified)



Interface Interlocking-RBC – Scenario Entry in L2 Area (simplified)



Discussion

WP E3.2

FFFIS Interface Specifications for Interlocking-CLC and Interlocking-Interlocking

Interface IXL-CLC

- Connecting an INESS interlocking to a **C**entralized **L**EU **C**ontroller.
- A pure one-way interface. CLC does not answer.
- IXL sends information about routes, route entry signals, overlaps, LDv, LSAs and LCr to the CLC.
- IXL reports its own availability to the CLC.
- IXL sends the version of its interface implementation to the CLC. CLC has to decide whether it can work with this IXL.

Interface IXL-IXL

- Connecting two interlockings, not necessarily INESS IXL.
- Main Purpose is to share route information. Necessary because INESS IXL do not support line blocks.
- Assumptions:
  - IXL boundary not at route entry / route exit but at TVP section boundary.
  - a master IXL is defined for every route. This IXL accepts the commands (route setting, cancellation).
  - the master IXL for a boundary route is the IXL containing the route entry.
  - handshaking has to take place between both IXLs, acknowledgements have to be used, and safe states defined if communication is lost
  - status of each route element of the shared routes has to be exchanged between both IXLs
  - route type, route ID and route entry signal aspect of the route in advance of the boundary has to be sent to properly generate signal aspects

Using a UML-based approach for specifying railway interfaces

Content

- Weaknesses of traditional specification approaches
- INESS WP E3.2 Specification Approach
- Benefits of WP E3.2 Specification Approach

Weaknesses of traditional specification approaches

Weaknesses of traditional specification approaches

- Quality problems in specifications
  - Misunderstandings due to inexact terminology
  - Ambiguities and underspecifications
  - Conflicting requirements possible

Weaknesses of traditional specification approaches

- Reduced Exploitability
  - No Simulation possible
  - No automatic test case generation
  - Difficult to maintain because of missing traceability
  - Communication between system engineers and developers is difficult

Weaknesses of traditional specification approaches

- Difficulties in Quality Assurance
  - no automatic checks possible
  - Non-standardized description syntax
  - Less traceability

Weaknesses of traditional specification approaches

Consequences of these weaknesses

- Additional effort and cost to connect systems of different manufacturers
- Multiple-supplier projects are made difficult
- Possible safety risks
- Use of railway products in different countries is hindered

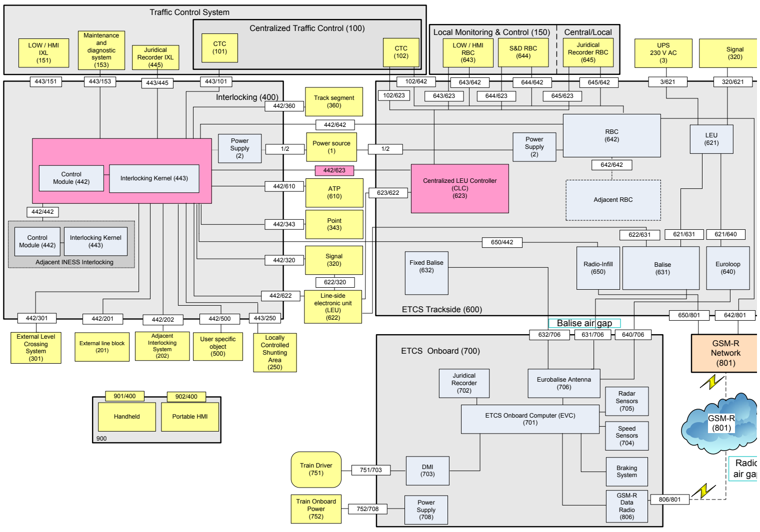
INESS WP E3.2 Specification Approach

INESS WP E3.2 Specification Approach

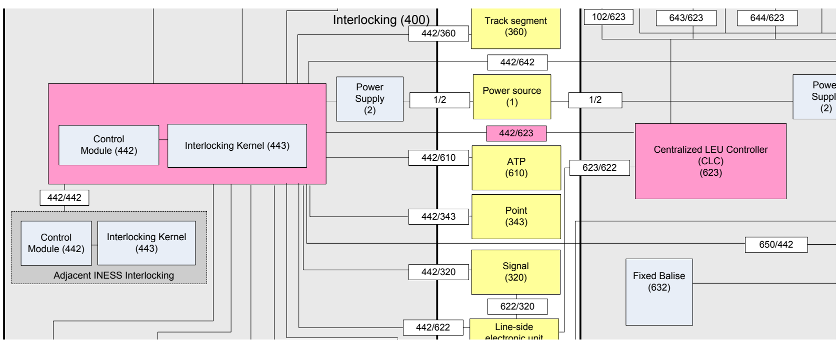
Important Elements of a FFFIS

- Architecture Diagram
- Interface Context
- Functional Apportionment
- State Machine Diagrams
- Sequence Diagrams
- Data Structures
- Message Structures

Architecture Diagram

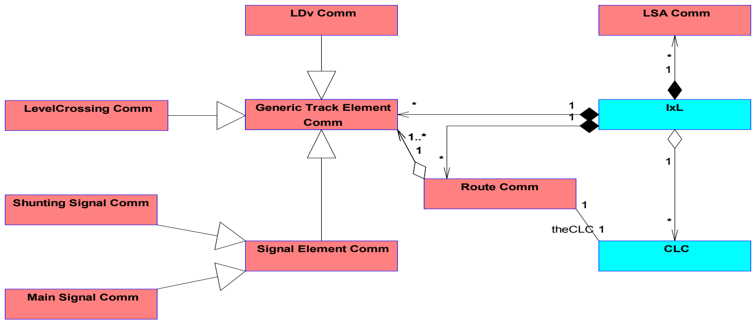


Architecture Diagram



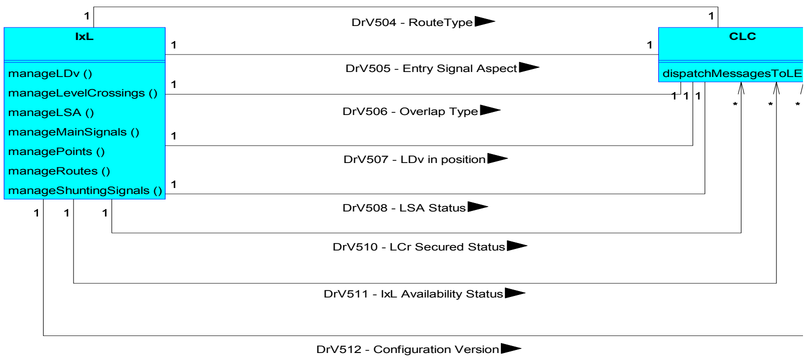
INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

Interface context IXL-CLC



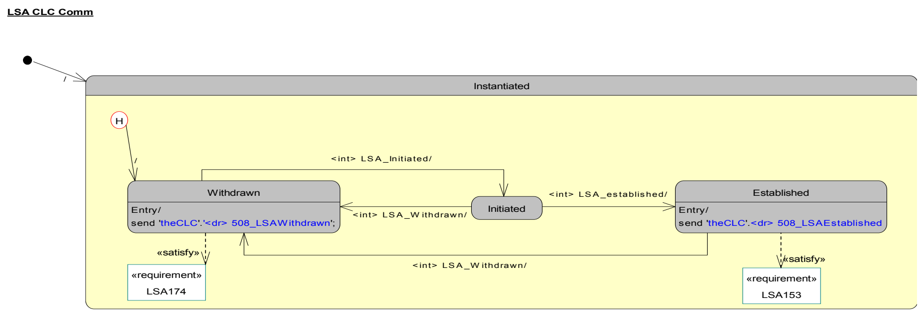
- Blue rectangles represent the system that are connected by the interface.
- Red rectangles represent parts of the interlocking that produce interface data.

Functional apportionment



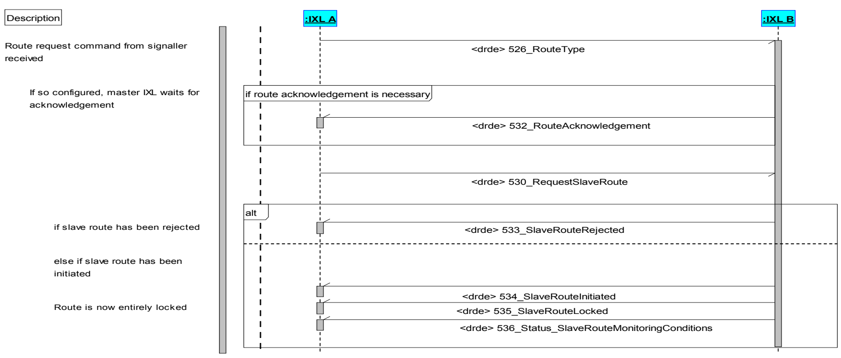
- The blue boxes show the major functions of a subsystem (in regard to the interface).
- Associations between the subsystem represent the messages on the interface.

State machine diagrams



- State Machines are complete by nature.
- White rectangles represent the Common Kernel Requirements and are here used for traceability.

Sequence diagrams



- Sequence diagrams are never complete. They are used to show some important scenarios.
- Sequence diagrams are not compulsory requirements, while state machines are.
- Sequence diagrams can be used to automatically execute test cases.

Data Structures

A.1.1.1.1 Data "ROUTE TYPE"

A.1.1.1.1.1 Purpose

The interlocking system shall provide the routes type according to ERTMS level and train location.

A.1.1.1.1.2 Message Type

Static information during lifetime of route.

A.1.1.1.1.3 Values specification

Length of variable	3 Bits
Value	**Status**
0	None
1	Full supervision
2	On Sight
3	Staff Responsible
4	Shunting
5-7	Spare

A.1.1.1.1.4 Instances definition

There shall be one data "Route Type" for each Train route.

A.1.1.1.1.5 Default value in case of communication failure

In the case of a communication failure the CLC shall assume all routes to be in the state '0=None'.

Message Structures

Prologue sub-frame

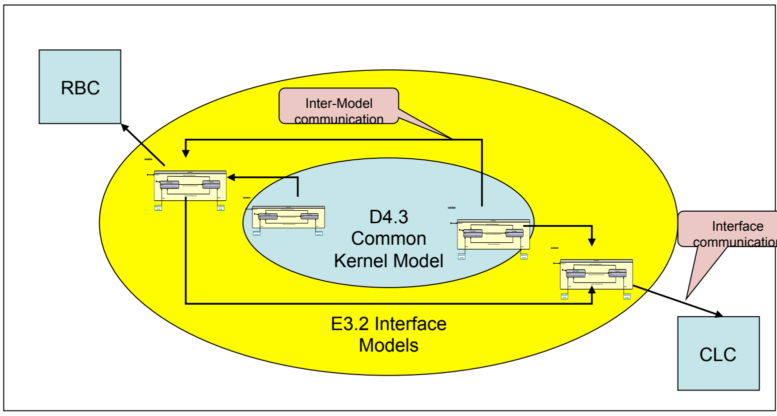
Field N°	Variable	Length (bits)
Pr.1	Application software version	8
Pr.2	Application data version	8
Pr.3	Number of boundary routes (N_{BR})	16
Pr.4	Number of lockable devices (N_{LD})	8
Pr.5	Number of local shunting areas (N_{LSA})	8
Pr.6	Number of level crossings (N_{LC})	8

Values sub-frame

Group Name	Variable	Length (bits)
V.BR	Boundary route 1 values	10
	Boundary route 2 values	10
	...	
	Boundary route N_{BR} values	10
V.LD	Lockable device 1 values	1
	Lockable device 2 values	1
	...	
	Lockable device N_{LD} values	1
…	…	…

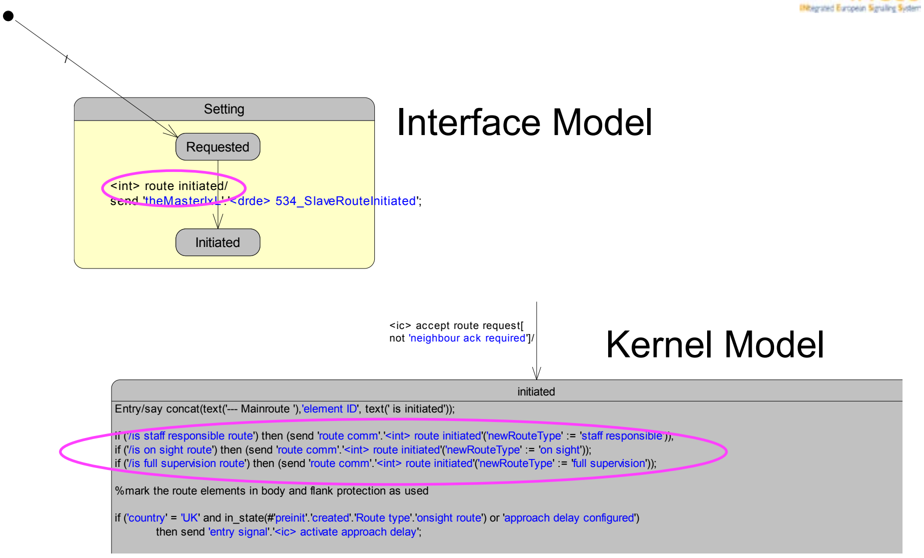
Correlation between Kernel Model and Interface Model

Connection between Common Kernel and Interfaces



- Models of Interlocking Kernel and INESS interfaces are kept in one place.
- Kernel model communicates with interface models.
- This ensures that kernel and interfaces are consistent.

Connection between Common Kernel and Interfaces



Driving and detected values

- ***Driving values*** are data the interlocking sends to a connected subsystem. Example: route types, signal aspects.
- ***Detected values*** are data the interlocking receives from a connected subsystem. Example: trains approaching a route.

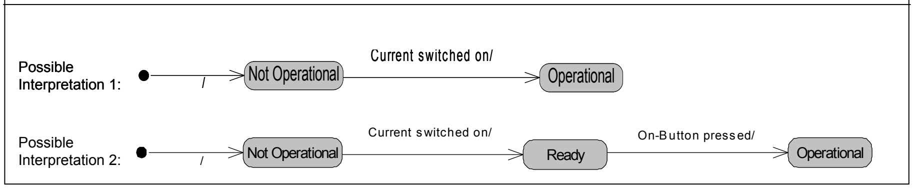
Benefits of UML-based approach

Benefits of the UML-based approach

Avoiding ambiguities

Textual requirement:

When the system is switched on it gets operational automatically.



INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

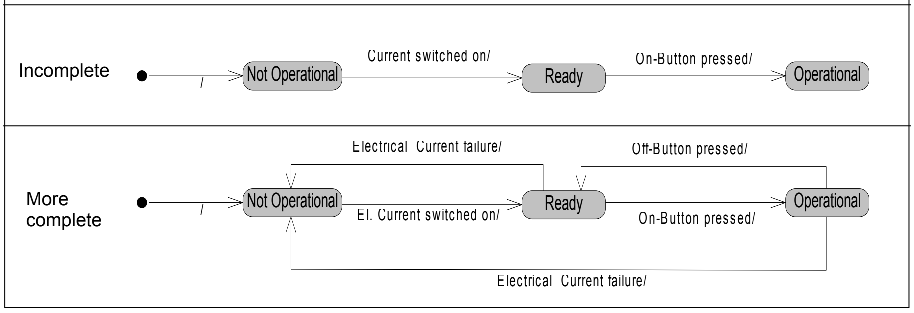
Benefits of the UML-based approach

Avoiding underspecification

Textual requirement:

When the system is switched on it gets operational automatically.

What happens when Off-button is pressed or electrical current switched off?



Benefits of the UML-based approach

Improving usefulness of specification

- **Simulation of State Machines**
- **Automatic test case generation**
- **Complete traceability from railway requirements to the interface specification**
- **Use of a common description language**

Benefits of the UML-based approach

Making quality assurance more effective

- Simulation of State Machines
- Automatic model checking
  - For UML conformity
  - For conformity to project modelling guideline

Thank you very much!

Discussion

Fallback possibilities and benefits

Description of work

„Recommendation for fallback: If there are benefits to use fallback systems, make one or more proposal of fallback techniques with description of benefit.“

Main steps of work

- **Task interpretation**
- **Criteria for evaluating fallback solutions**
- **Developing a method (formula) for evaluating different fallback solutions**
- **Examples for application**

Fallback possibilities and benefits

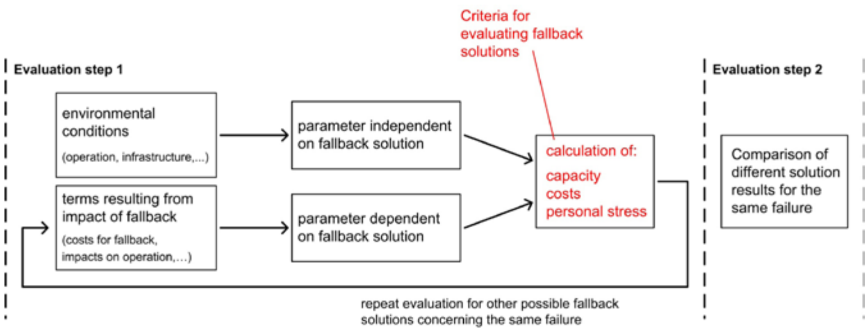
Definition of the term „fallback“

„Fallback means something – technology, rules –, that has to or can be used to maintain rail operation in a degraded mode when a particular entity of the system cannot be used and/or when the normal specified operation state is missed.”

Fallback possibilities and benefits

Aim of fallback evaluations

➢ **Comparision of different fallback solutions for one specific failure**



Fallback possibilities and benefits

<u>Criteria for evaluating fallback solutions</u>

The involved partners worked out three criteria that are necessary for evaluating fallback solutions:

- ***Fallback Operational Benefit (FOB)***
  Percentaged change of infrastructure capacity in case of fallback compared with normal operation

- ***Fallback Normal Costs (FNC)***
  Ratio of costs of fallback solution and normal operation

- ***Technical Solution Indicator (TechSI)***
  Mental stress of operator

Fallback possibilities and benefits

<u>Fallback Operational Benefit (FOB)</u>

Percentaged change of infrastructure capacity in case of fallback compared with normal operation

$$FOB = \frac{FR_{fallback}}{FR_{normal}} \times 100\ \% \times n$$

$$FR_{normal} = A \times E_{Traffic,normal}$$

$$FR_{fallback} = p \times E_{Traffic,fallback}$$

p	=	probability to get into a fallback situation
$E_{traffic,fallback}$	=	traffic energy in case of fallback
$E_{traffic,normal}$	=	traffic energy in normal operation
A	=	frequency of fallback problem
n	=	number of equipments

Fallback possibilities and benefits

Fallback Normal Costs (FNC)

Ratio of costs of fallback solution and normal operation

$$FNC = \frac{FC}{BC} \times 100$$

$$FC = LCC_{normal} + LCC_{fallback}$$

$$BC = LCC_{normal}$$

LCC_{normal} = life cycle costs for normal operation
$LCC_{fallback}$ = additional life cycle costs for fallback situation

$$FBQ = \frac{FOB}{FNC} \times 100$$

FBQ = Fallback Benefit Quotient

Fallback possibilities and benefits

Technical Solution Indicator (TechSI)

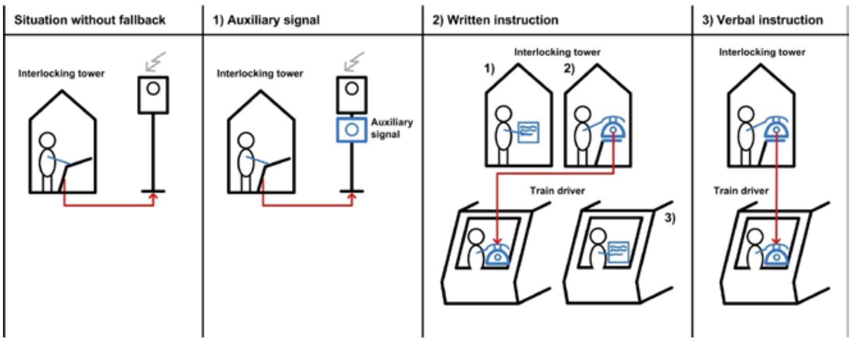
Mental stress of operator

$$TechSI = \frac{\rho \times s_{area} \times N^{0}_{system}}{N^{0}_{operator}}$$

ρ = numbers of trains controlled at the same time
s_{area} = size of controlled area
N^0_{system} = different types of operations
$N^0_{operator}$ = number of operators

Fallback possibilities and benefits

Examples for application (signal failure)



(The examples are described in detail in the report.)

Fallback possibilities and benefits

Examples for application (signal failure)

1) Auxiliary Signal // 2) Written instruction from the signaller // 3) Verbal instruction from the signaller

Results

Large operational benefit can compensate the high normal costs.

The difference in these values is based on the different entry parameters: In example 2, the train driver has to stop in front of the signal, for getting a passing permission. Example 3 allows a pass without stop
-> Different influence on capacity.

		example 1	example 2	example 3
criteria 1	FOB (%)	1,096 +	0,9133	0,5114
criteria 2	FNC (%)	123,46 -	102,00	101,66
	FBQ (-)	0,8877 +	0,8954	0,5030
criteria 3	TechSI (-)	30 +	45	45

The calculation of the TechSI depends on defining the written instruction as 1 or 2 operations.
(In case of 2 you would have a difference to the verbal instruction possibility, TechSI = 60)

(The calculation steps are described in the report.)

Fallback possibilities and benefits

Results

- **A positive value in one of the criteria must not lead to positive values in the other criteria**

→ Only one single value would not lead to significant results.
→ Only as a whole, the criteria values allow a significant evaluation.

Discussion

Main content of the Report on deliverable E-4.3
"Final recommendations for trackside migration and fallback"

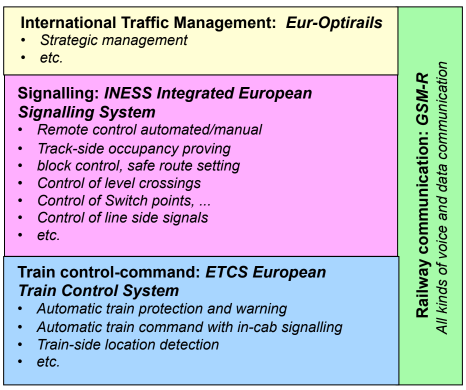
By Emmanuel Buseyne and Peter Winter

Introduction

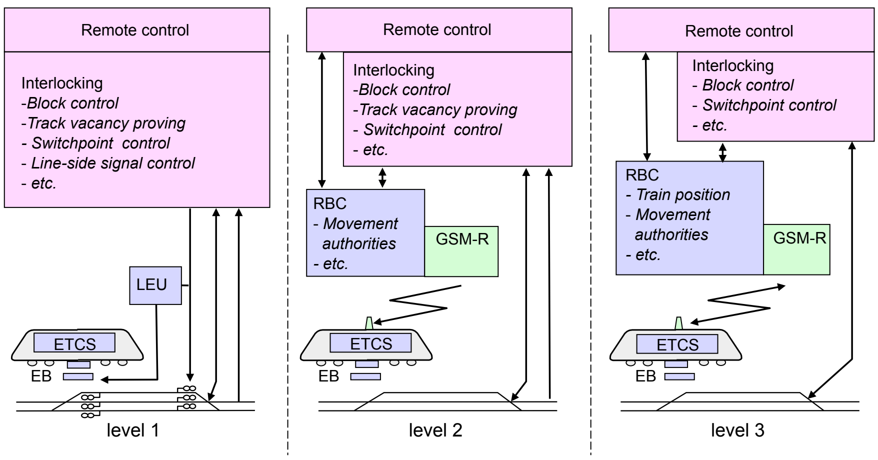
The final recommendations for migration and fallback are merged into one joint final document D.E.4.3. The ETCS part is focused on the current status of the specifications (version 2.3.0.d); for general considerations also the foreseeable extensions with baseline 3 and level 3 are taken into account. In Europe the market for new lines (green field) is relatively small, therefore high priority is given to INESS applications on existing lines and nodes with ETCS or national train control systems (brown field).

Functional structure of ERTMS and associated European projects

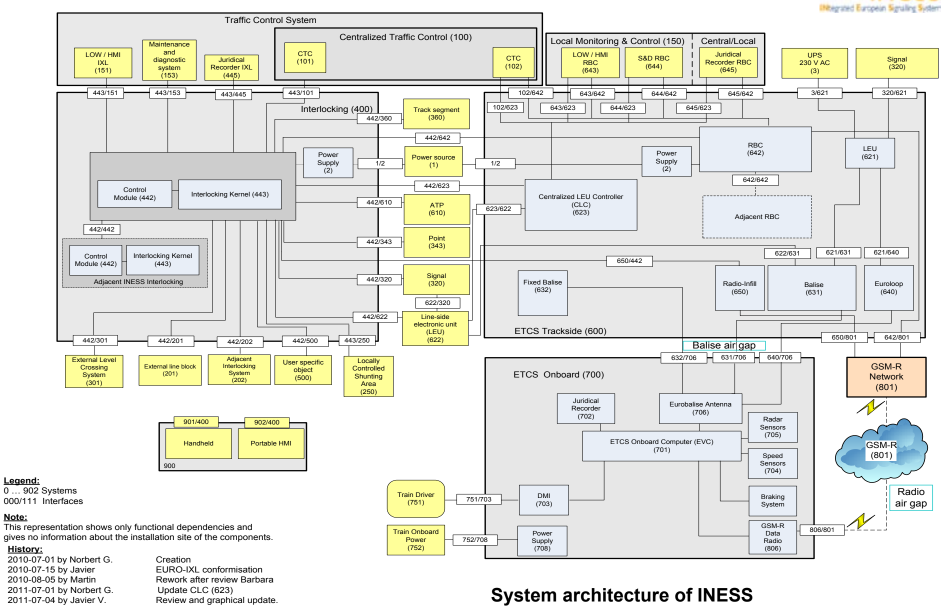
The scope of the analysis is ERTMS for which the ground has been prepared in the last 20 years with the comprehensive European R&D projects ETCS in the area of train control, GSM-R in the area of railway communication and Eur-Optirails in the area of international traffic management.
ETCS is based on different application levels which influence also the functionality and structure of the signalling and the GSM-R data transmission subsystems. It makes therefore sense to classify not only ETCS but the whole structure of ERTMS according to the levels NTC (national train control), 1, 2 and 3.



Compliance between INESS and ETCS in the 3 application levels



In the INESS system architecture the interlocking (unit 400) is linked among other with the ETCS track-side (unit 600). From here, the link to the ETCS on-board (unit 700) is based on different means for data transmission: fixed (passive) balises, active balises controlled by LEU's, Euroloops controlled by LEU's (optional) or GSM-R radio controlled by Radio Control Centres (RBC's). The way of using these devices depends on the application levels.



System architecture of INESS

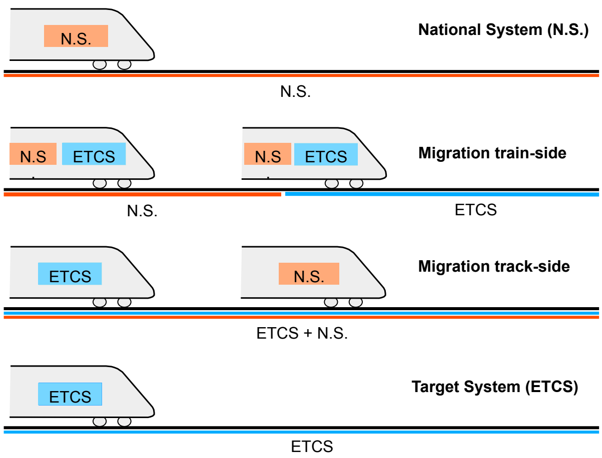
iness

What is migration, influencing factors

The term “migration” designates the process of implementing or upgrading parts of ERTMS on a network either in one or several steps. This means double equipment of national train control system and ETCS during a transition period either on track-side or on train-side (or on both sides).

The train-side solution seems more adequate when the network is big in comparison to the rolling-stock fleet; the track-side solution may be more favorable for smaller networks with a large amount of rolling stock. The optimal choice of the migration strategy depends on several technical, operational and financial aspects on track- and rolling-stock side. For defining and realizing successfully the migration, a close joint cooperation of infrastructure managers and train operators is a “must” despite the trend for separating their responsibilities.

Basic principle for ETCS migration strategies



iness

What is fallback, interdependency with the application levels

ERTMS is highly relevant for the safety and the quality of train operation. Fallback techniques and methods which are in part specific for the different application levels contribute to minimise the negative effect of failures and perturbations. The possibilities of fallback and their benefit are well described in the report E.4.2. It postulates that the fallback structure of the signalling system consists of three parts: upper rank, inner rank and lower rank. Regarding the nature of fallback solutions three types are considered: technical, rule-based and hybrid. Main conclusion of the report is that the future standardised INESS interlocking must be intrinsically redundant and support all the functions of the ERTMS system in normal and fallback running modes of the trains. Regarding train control and train communication, GSM-R and the RBC’s are part of the upper rank while the Eurobalises, the Euroloop and the associated LEU’s are part of the lower rank. This reflects the fact that failures in the GSM-R or the RBC’s affect major area’s of ETCS equipped lines and nodes and may therefore lead to serious operational difficulties, while failures of single balises or loops concern more limited area’s.

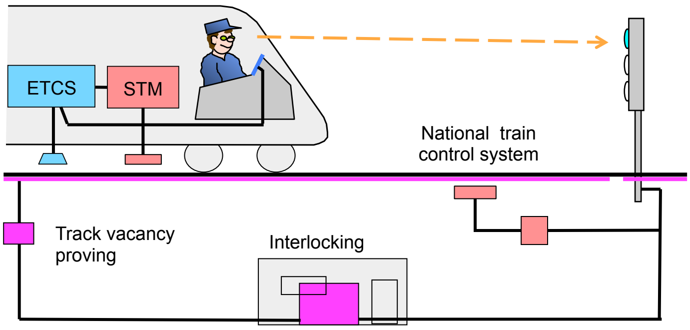
Options for track-side ERTMS implementation with corresponding fallback solutions

ERTMS level	Trackside configuration for normal train operation	Fallback methods or techniques
Level NTC	No trackside ETCS equipment exists (use of a national train control system)	Dedicated national operational rules and regulations
Level 1	- ETCS as single train control system - ETCS overlaid to a national train control system	Dedicated national operational rules and regulations
Level 2	- ETCS as single train control system - ETCS overlaid to a national train control system	ETCS level 1 parallel equipment or vital parts redundant or special operational rules
Level 3	ETCS as single train control system	European operational rules and regulations, ETCS level 2 in parallel ?

ETCS level NTC - ETCS equipped train driving on lines with legacy train control system

In the application level NTC the network is equipped on the trackside exclusively with a national train control system. On these line-sections and nodes line-side signals are used and the train control system does not deliver continuous target information to be displayed on the DMI. ETCS equipped trains need specific STM-devices which pick up the information in a national format from the track-side and fulfil the conversion into ETCS format. For the fallback train operation (national train control system not working) the same procedures may be used as for the national train control system.

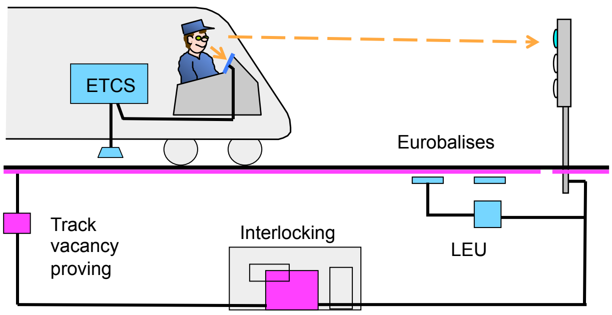
Example of successful application: Swedish conventional main line network equipped with the legacy train control system EBICAB. All ETCS equipped trains need an STM for EBICAB.



ETCS train driving in mode Full Supervision on track equipped with ETCS level 1

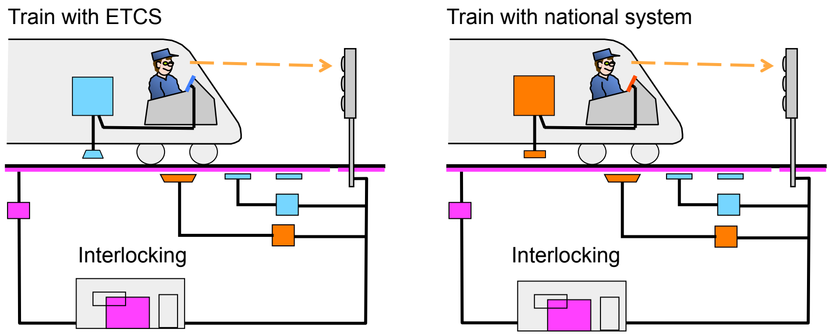
In the ERTMS application level 1 the line-side signals, which are based on national rules and regulations, are kept in the majority of the cases. ETCS can be installed and operated either as single train control system or in parallel to a national train control system. This juxtaposition is obtained by adding physically the ETCS equipment to the already existing track-side components of the national system or by transmitting with the ETCS devices not only the ETCS telegrams but also telegrams for the national train control systems. In the latter case the trains must be equipped with a device for reading the national telegrams transmitted by the trackside ETCS.

In mode Full Supervision the driver gets in parallel to the information from the line-side signalling all relevant target information also on the DMI.
Example of successful application with level 1 Full Supervision: Network of Luxemburg Railways.



ETCS level 1 Limited Supervision overlaid to a national train control system

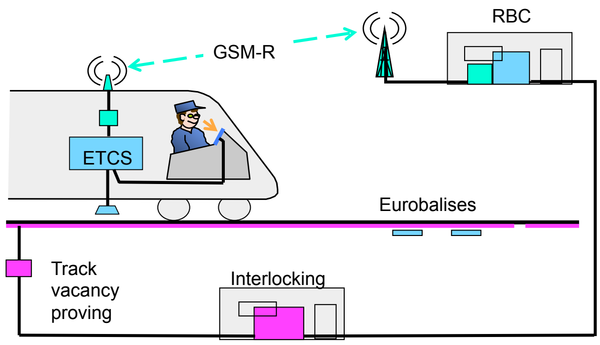
The driver does not get target information from ETCS and is therefore obliged to observe in the traditional way the line-side signals and other information panels placed along the line. ETCS protects the train in the background. As the safety results from both in parallel, the driver observing the signals and ETCS monitoring the speed in the background, the safety integrity level of the ETCS path may be lower than SIL 4. Compared to train operation with Full Supervision the costs for engineering, installation and test of the ETCS track-side equipment may therefore be significantly lowered. Also, the line capacity is slightly higher. Example of ongoing implementation: Network of Swiss Railways.



ETCS train driving on line with ETCS level 2 equipment

In the ERTMS level 2, ETCS is installed in general on trackside as single train control system whereby no line side signals are used and the mode Full Supervision is applied. This means that the driver gets all target information on the DMI and is seamlessly supervised. In certain cases ETCS level 2 on trackside is operated in parallel to a national train control system. This approach requires a specific engineering especially for the interfacing of the ETCS RBC with the interlocking. As fallback for the train operation in disturbed situations special national operational rules and regulations may be used. Another approach consists in using level 1 as fallback level – however there is a clear trend to abandon this.

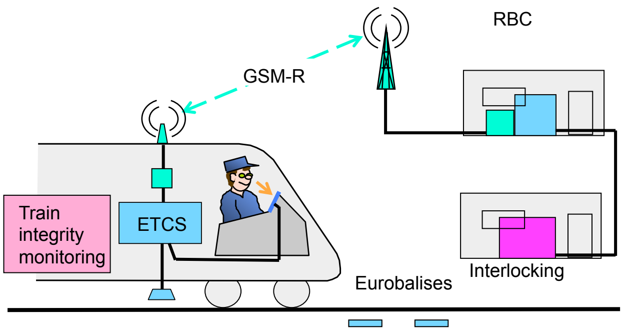
Examples of successful applications:
New high-speed lines in Italy (without fallback level 1), Spain (originally fallback with level 1 which is gradually disappearing) and Switzerland (without fallback level 1).



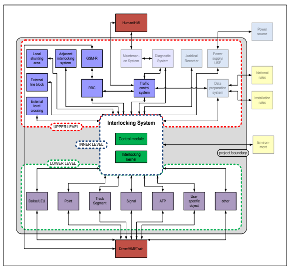
Future perspectives with level 3

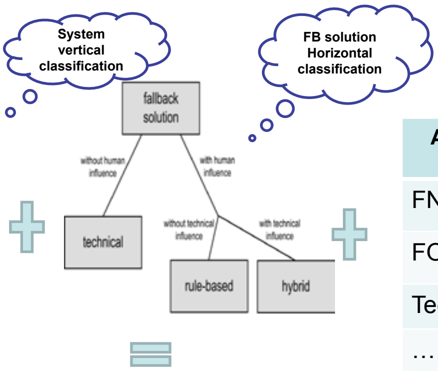
A first realisation of the most innovative application level 3 is in commercial operation on a Swedish regional line of 130 km length. This concept called ERTMS Regional is conceived with an integration of the ETCS RBC, the interlocking and the remote control in one single computer whereby no technical fallback level is used. For a universally applicable track-side ERTMS level 3 equipment, it will be necessary to develop a harmonised concept with open interfaces between the various subsystems. A major problem to be solved for the on-board part by the train operators is the Train Integrity Monitoring including the detection of the train length.

The universal level 3 concept will still need interlockings. These will not only control points and level crossings but also the train spacing based on the position detected by the trains. It seems advantageous to introduce optionally the possibility for track-side vacancy proving devices at certain locations like station area's.



Fallback methodology use





Appropriate criteria?
- FNC
- FOB
- TechSi
- …

System FB benefits classification matrix

	FB solution 1	FB solution 2	…	FB solution N
System upper level	[FB1 C.1, FB1 C2...FB1 Cj]u	[FB2 C.1, FB1 C2...FB1 Cj]u		[FBN C.1, FB1 C2...FB1 Cj]u
System inner level	[FB1 C.1, FB1 C2...FB1 Cj]i	...		...
System lower level	[FB1 C.1, FB1 C2...FB1 Cj]l	...		[FBN C.1, FB1 C2...FB1 Cj]u

Using the above classification methodology with the "appropriate" criteria's, it is possible to evaluate the best fitting FB method of any system!

Discussion

INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012

Closing remarks & discussion

INESS - INtegrated European Signalling System
EU 7th FRAMEWORK PROGRAMME - THEME 7 – TRANSPORT
INESS Training–7,8 & 9 Mar. 2012