Advance Industry Day

WP1 : Railway Case Study

Fernando Mejia – Alstom Transport
Minh-Thang Khuu – Systerel
Michael Leuschel– University of Düsseldorf

SEVENTH FRAMEWORK PROGRAMME

23/10/2014

Overview

1. Goals and Motivations
2. Interlocking Dynamic Controller
3. Achievements
4. Conclusions

1 – Goals & Motivations

- Prove formally that an interlocking system (IXL) complies with system-level safety requirements
  - *Satisfy transport operators (e.g. Paris, New York) request*
- Develop a proof technique independent of the complexity and implementation technology of IXL
  - *Overcome model checking technology drawbacks*
- Develop an industrial system development process involving Advance methods and tools
  - *Satisfy European railway standards (CENELEC)*
- Apply and improve Advance methods and tools
  - *Increase quality & productivity*

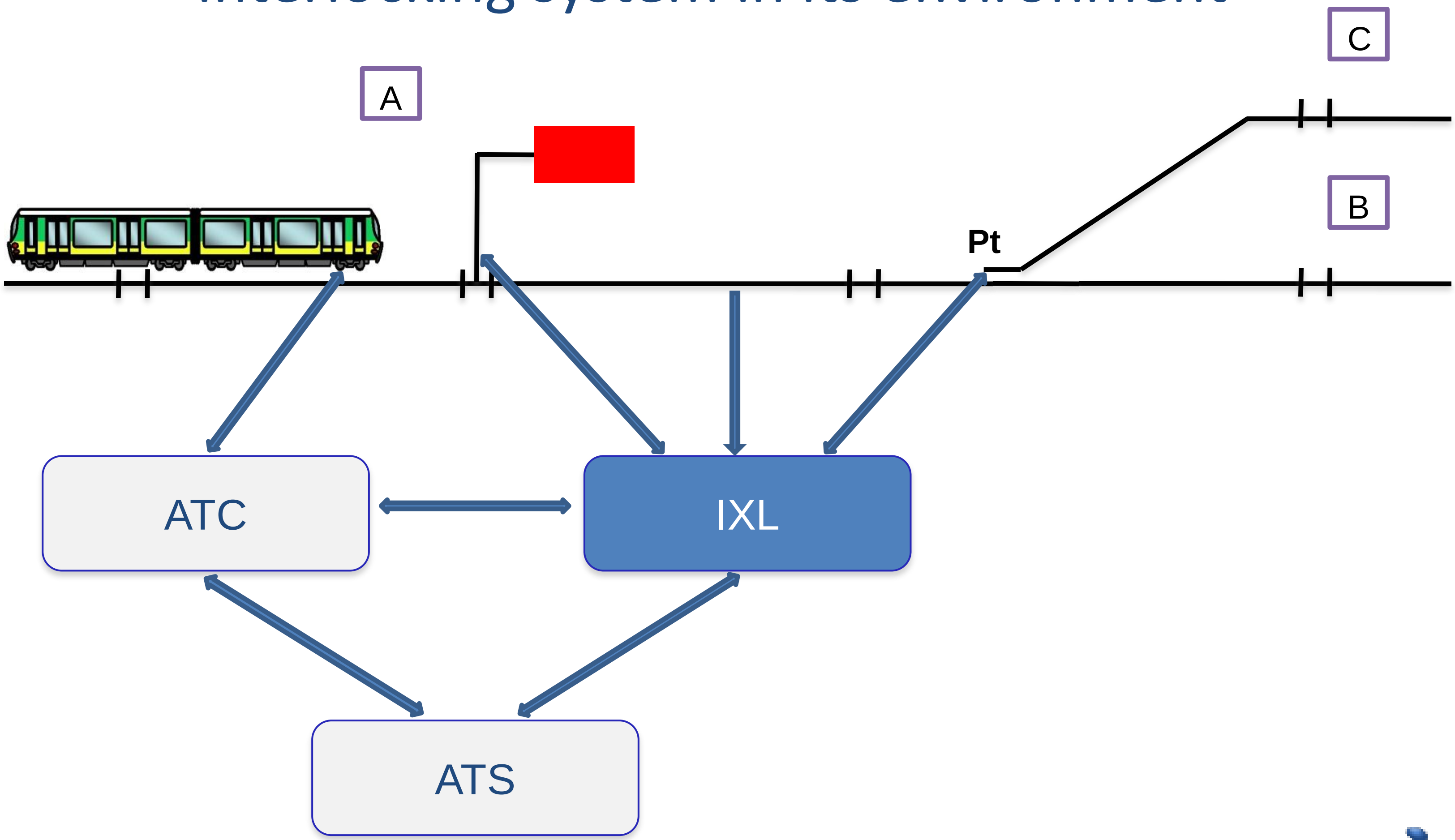
2 - Interlocking Dynamic Controller (IXL-DC)

- IXL is designed to set and lock the routes of trains in order to avoid:
  - Derailments,
  - Hurting of maintenance staff,
  - Head-on collisions,
  - Side-on collisions, and often but not systematically,
  - Rear-end collisions

SEVENTH FRAMEWORK PROGRAMME

2 - Interlocking Dynamic Controller (IXL-DC)

Interlocking system in its environment



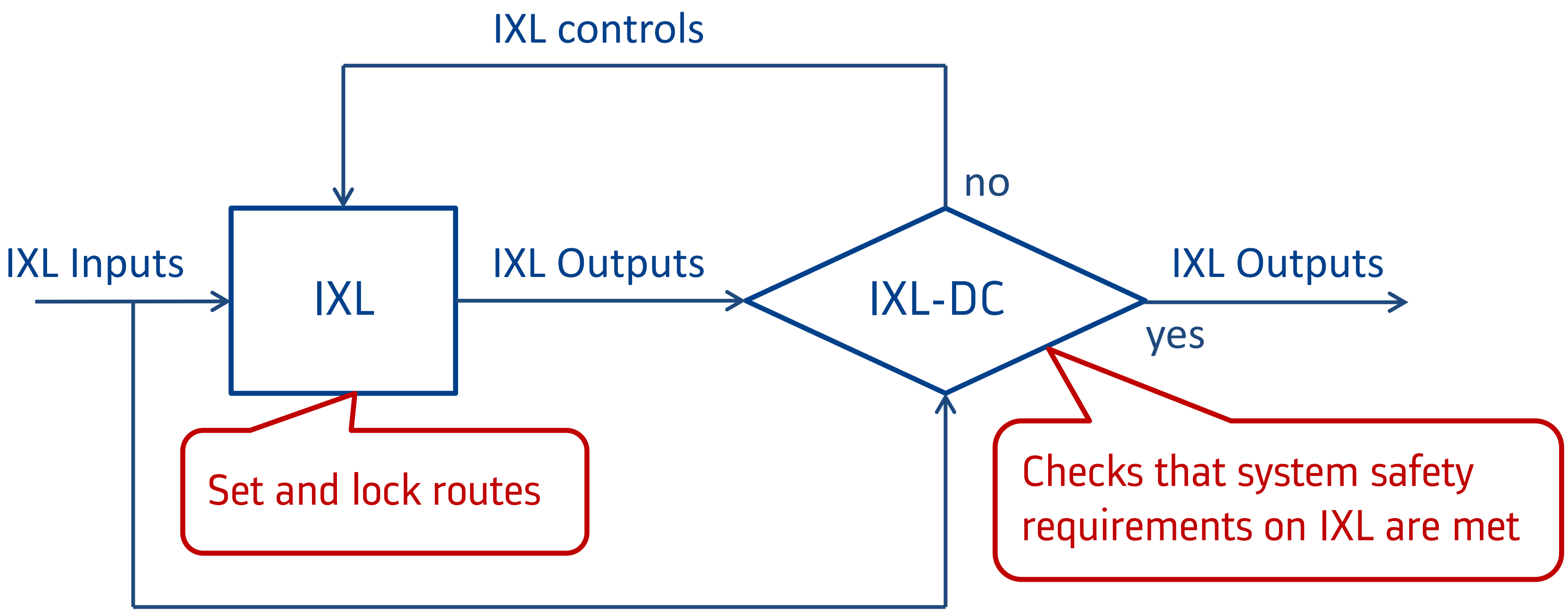
2 - Interlocking Dynamic Controller (IXL-DC)

- IXL-DC is designed to check at runtime that safety requirements on IXL are met:
  - No uncontrolled points in routes,
  - No incompatible routes are set at the same time,
  - No unsafe permissive signals,
  - No incompatible permissive signals at the same time,
  - …

SEVENTH FRAMEWORK PROGRAMME

2 - Interlocking Dynamic Controller (IXL-DC)

Interlocking and Interlocking Dynamic Controller



2 - Interlocking Dynamic Controller (IXL-DC)

Case study formalisms, methods and tools

- Safety analysis
  - Formalism: System Theory
  - Method : STAMP/STPA
  - Tool : ProR (for requirements management)
- Model creation
  - Formalism: Event-B
  - Method: Model refinement and decomposition
  - Tool: Rodin

2 - Interlocking Dynamic Controller (IXL-DC)

Case study formalisms, methods and tools

- Model verification
  - Formalism: Event-B
  - Method: Proof
  - Tool: Rodin
- Model validation
  - Formalism: B
  - Method: Animation
  - Tool: ProB

3 - Achievements

Hazard analysis with STAMP/STPA

- Identification of the potential accidents
- Identification of the system-level hazards
- Identification of the system-level requirements
- Creation of the control structure of the system
- Hazardous controls analysis
- Casual factor analysis
- Requirements management

3 - Achievements

Hazard Analysis with STAMP/STPA

- Identification of accidents

	Description	Link
1	Collision	
1.1	Rear-end collision	1 ▷ R ▷ 0
1.2	Side-on collision	1 ▷ R ▷ 0
1.3	Head-on collision	1 ▷ R ▷ 0
1.4	Collison with object on the track	1 ▷ R ▷ 0
1.5	Collision with system structure	2 ▷ R ▷ 0
2	Derailment	
2.1	Derailment due to train instability	1 ▷ R ▷ 0
2.2	Derailment due to loss of guidance	4 ▷ R ▷ 0
3	Hurting of passengers or maintenance staff	
3.1	Passengers hurt inside the train	
3.2	Passengers in danger cannot leave the train	
3.3	Passengers or staff fall from the train onto track	
3.4	Passengers or staff fall from the platform onto track	
3.5	Passengers fall at platform / vehicle gap	
3.6	Passengers struck on platform door by a train	
3.7	Passengers wounded by PSD	
3.8	Passengers wounded by train doors	
3.9	Passengers on track struck by a train	1 ▷ R ▷ 0
3.10	Maintenance staff on track struck by a train	1 ▷ R ▷ 0
3.11	Passengers hurt by an object	

3 - Achievements

Hazard Analysis with STAMP/STPA

- Identification of hazards

	ID	Description	Link
1	Ⓡ H1.1	The distance between two successive trains is less than the braking distance of the follower train.	2 ▷ Ⓡ ▷ 1
2	Ⓡ H2.1	The distance between a train running on a route which crosses the route of another train and the trajectory of t he latter train is less than the braking distance of the former train.	2 ▷ Ⓡ ▷ 1
3	Ⓡ H3.1	The distance between two trains running on the same track in opposite directions is less than the braking distan ce of one of the trains.	2 ▷ Ⓡ ▷ 1
4	Ⓡ H4.1	A hurtful object fell or has been left on the track.	2 ▷ Ⓡ ▷ 2
5	Ⓡ H5.1	The distance between a train and the end of line buffer is less than he braking distance of the train.	1 ▷ Ⓡ ▷ 1
6	Ⓡ H5.2	Signalling system equipment is misplaced.	1 ▷ Ⓡ ▷ 1
7	Ⓡ H6.1	A train runs at excessive speed according to the configuration or the structure of the track.	1 ▷ Ⓡ ▷ 1
8	Ⓡ H7.1	A train runs on a point locked in the wrong position.	1 ▷ Ⓡ ▷ 1
9	Ⓡ H7.2	A train runs on an unlocked point.	1 ▷ Ⓡ ▷ 1
10	Ⓡ H7.3	A rail is damaged.	1 ▷ Ⓡ ▷ 1
11	Ⓡ H8.1	Maintenance workers are on a non-protected track maintenance zone.	1 ▷ Ⓡ ▷ 1
12	Ⓡ H8.2	Passengers are on a non-protected track evacuation zone.	1 ▷ Ⓡ ▷ 1

SEVENTH FRAMEWORK PROGRAMME

3 - Achievements

Hazard Analysis with STAMP/STPA

- Identification of requirements

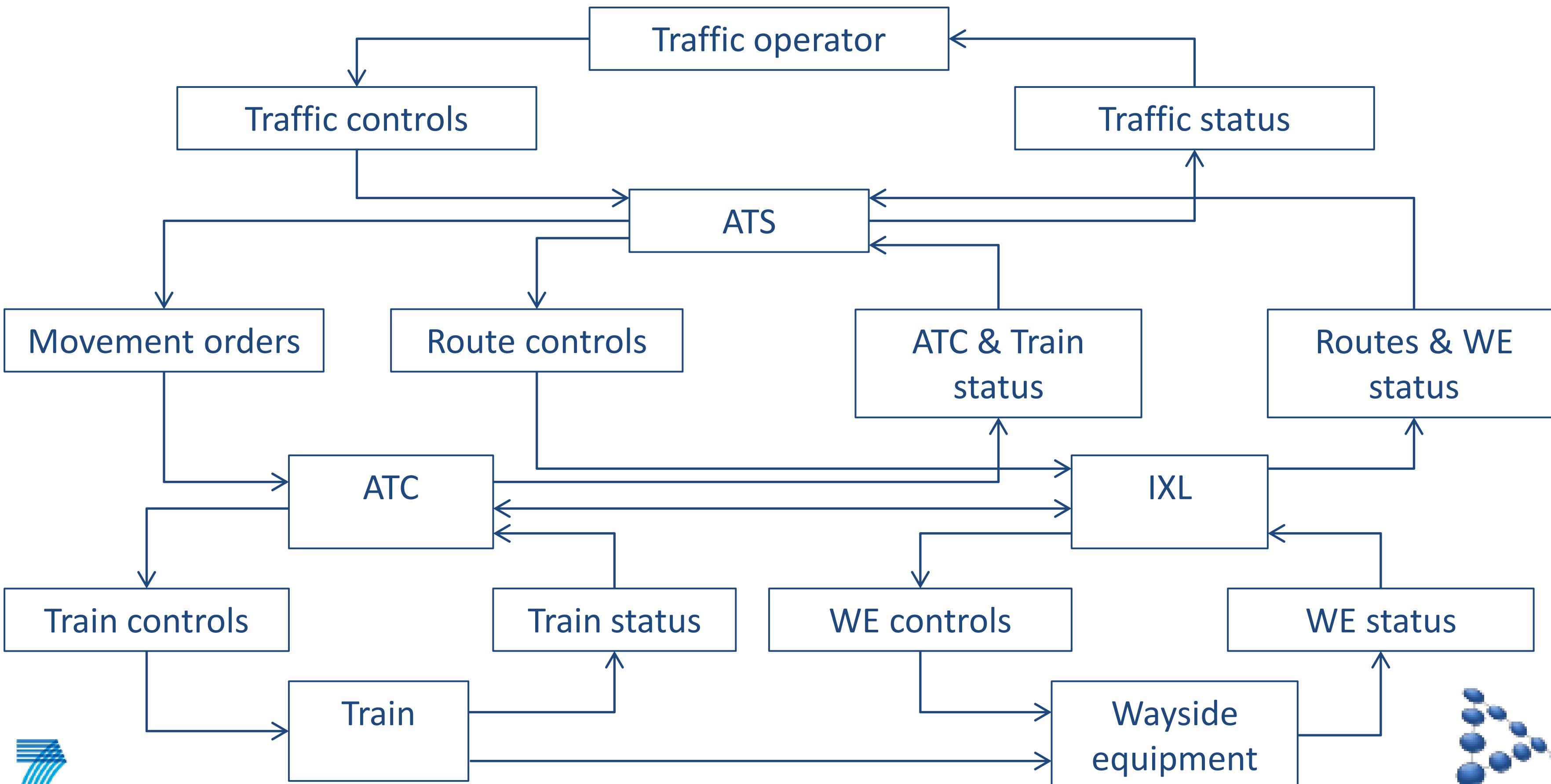
	ID	Description	Link
1	REQ-1	The system shall maintain in front of each train a track section free of obstacles longer than the braking distanc e of the train.	0 ▷ Ⓡ ▷ 4
2	REQ-2	The system shall prevent trains from running backwards.	0 ▷ Ⓡ ▷ 1
3	REQ-3	The system shall not authorise simultaneously routes that intersect.	0 ▷ Ⓡ ▷ 1
4	REQ-4	The system shall not authorise simultaneously opposite routes that overlap or end in the same place.	0 ▷ Ⓡ ▷ 1
5	REQ-5	Maintenance procedures must ensure that no hurtful object is left on the track after a maintenance operation.	0 ▷ Ⓡ ▷ 1
6	REQ-6	Operation procedures must ensure that no hurtful object is on the track during train operation.	0 ▷ Ⓡ ▷ 1
7	REQ-7	Commissioning and maintenance must ensure that signalling equipment is out of reach of trains.	0 ▷ Ⓡ ▷ 1
8	REQ-8	The system shall prevent trains from exceeding the maximum speed authorised by the configuration or the structure of the track sections.	0 ▷ Ⓡ ▷ 1
9	REQ-9	The system shall lock points in front of a train in the position required by the planned route of the train.	0 ▷ Ⓡ ▷ 1
10	REQ-10	The system shall ensure that points are locked in front of an approaching train or under a train.	0 ▷ Ⓡ ▷ 1
11	REQ-11	Commissioning and maintenance shall ensure that rails are safe.	0 ▷ Ⓡ ▷ 1
12	REQ-12	The system shall protect track maintenance zones.	0 ▷ Ⓡ ▷ 1
13	REQ-13	The system shall protect track evacuation zones.	0 ▷ Ⓡ ▷ 1

SEVENTH FRAMEWORK PROGRAMME

3 - Achievements

Hazard analysis with STAMP/STPA

- Control structure



3 - Achievements

Hazard analysis with STAMP/STPA

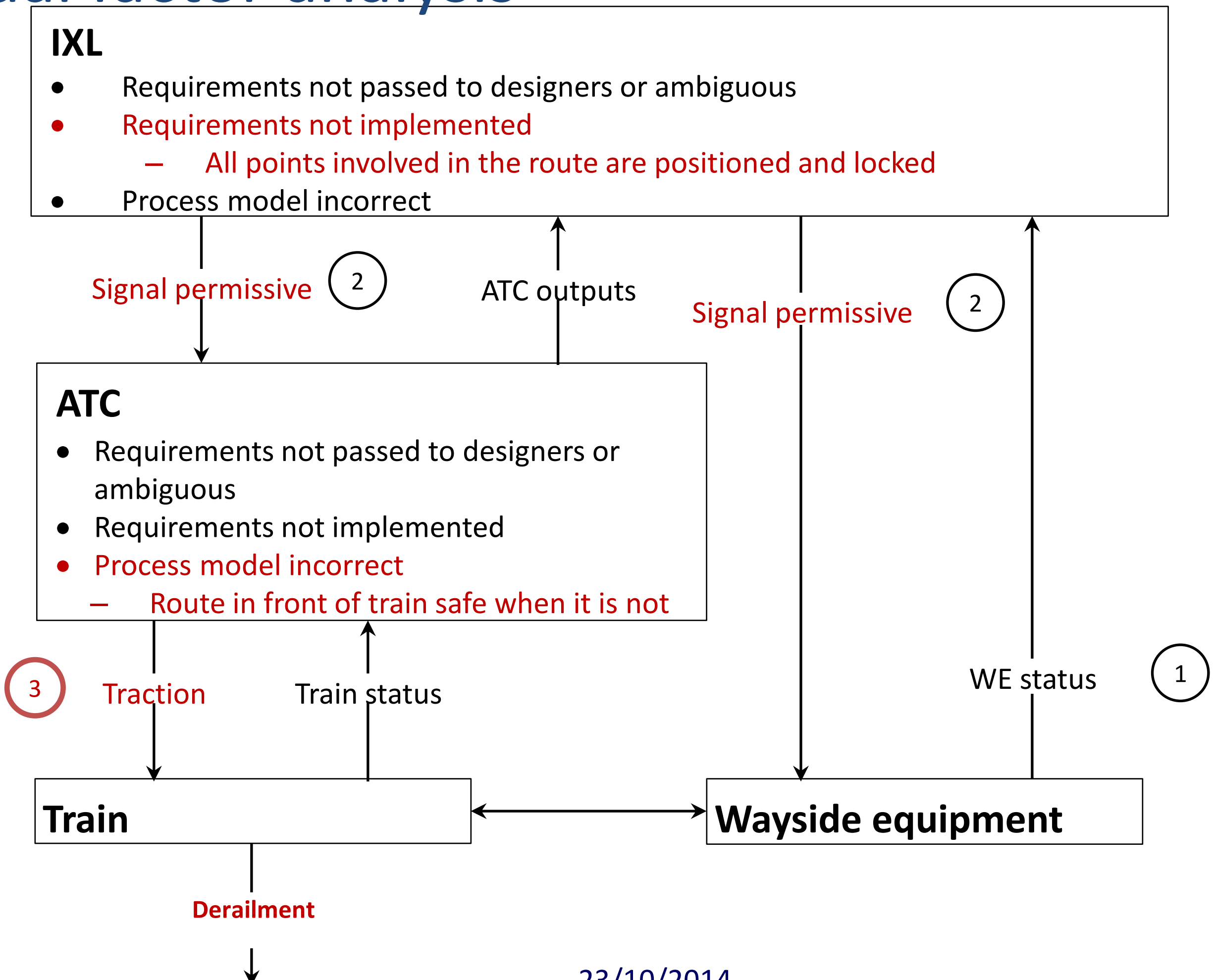
- Hazardous controls analysis

Control	Not providing causes hazard	Providing causes hazard	Wrong timing/order causes hazard	Stopped too soon/applied too long causes hazard
Signal Permissive	Not hazardous	Braking distance too short; unlocked or wrongly positioned point; excessive speed	Too early : cf. 2nd column	Too soon : not hazardous
			Too late : not hazardous	Too long : cf. 2nd column
Signal restrictive	Braking distance too short; unlocked or wrongly positioned point; excessive speed	Not hazardous	Too early : not hazardous	Too soon : cf. 2nd column
			Too late : cf. 2nd column	Too long : not hazardous
			Wrong order :	
Control point	Wrongly positioned point	Unlocked or wrongly positioned point; excessive speed	Too early : Unlocked point	Too soon : Unlocked point
			Too late : Unlocked point	Too long : not hazardous

3 - Achievements

Hazard analysis with STAMP/STPA

- Casual factor analysis



3 - Achievements

Modelling and proof with Rodin

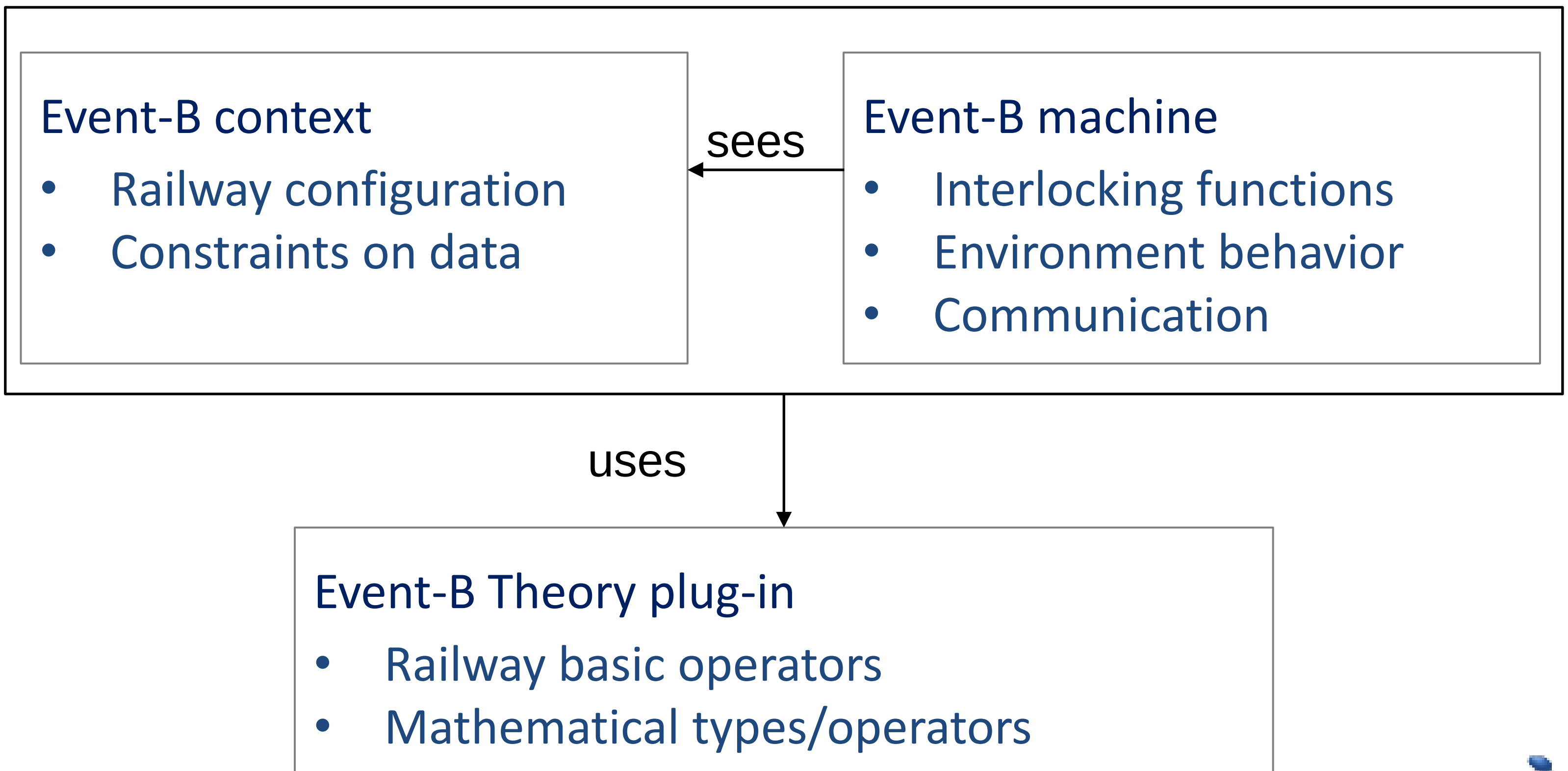
- Using refinement
  - From system overview to railway devices
- Using Event-B Theory plug-in
  - Defining mathematical and railway operators
- Using Composition/Decomposition plug-in
  - Separating environment, controller and communication
- Proving
  - Defining theorems and proof rules
  - Defining tactics for automatic PO discharge

SEVENTH FRAMEWORK PROGRAMME

3 - Achievements

Modelling and proof with Rodin

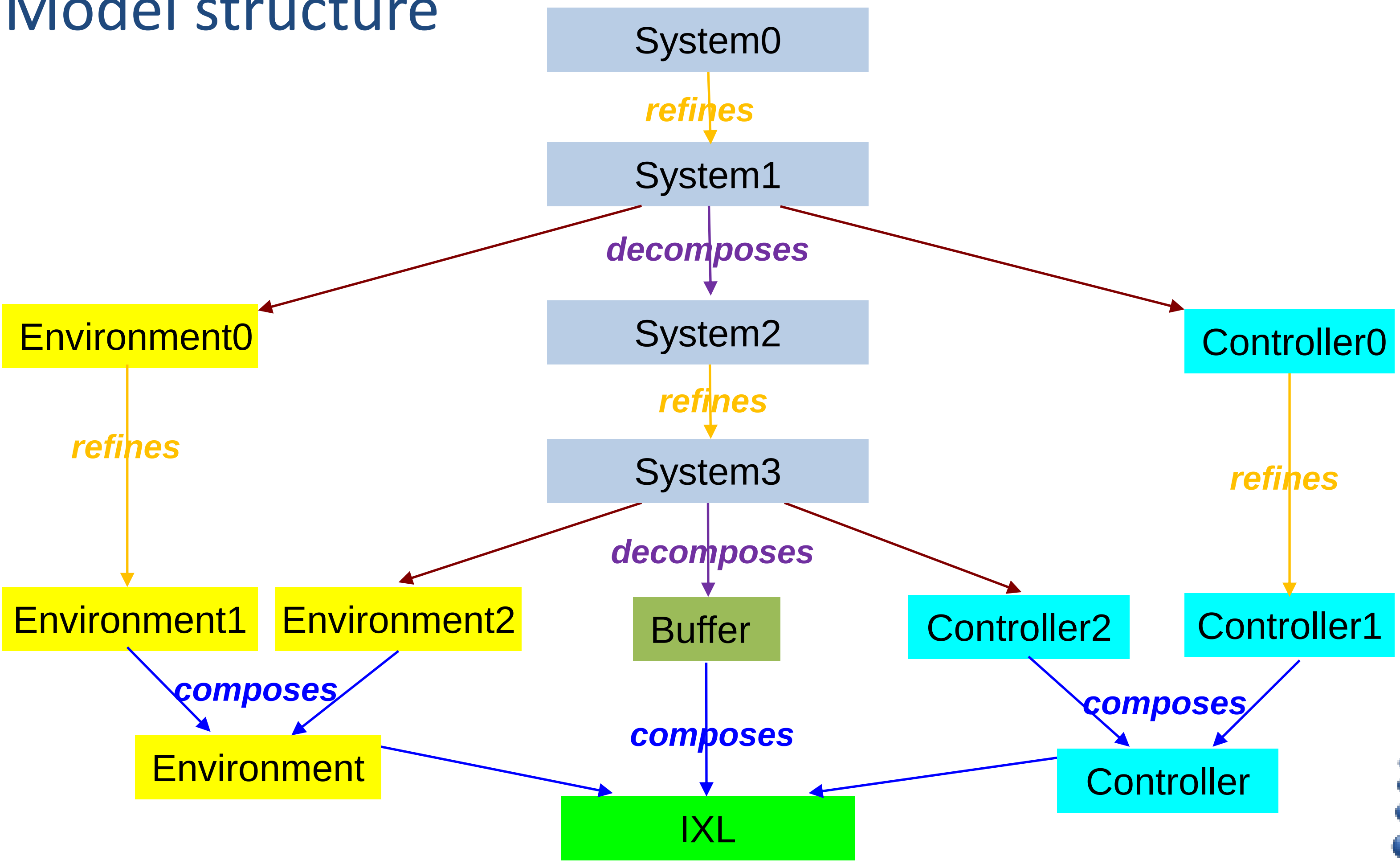
- Model structure



3 - Achievements

Modelling and proof with Rodin

- Model structure



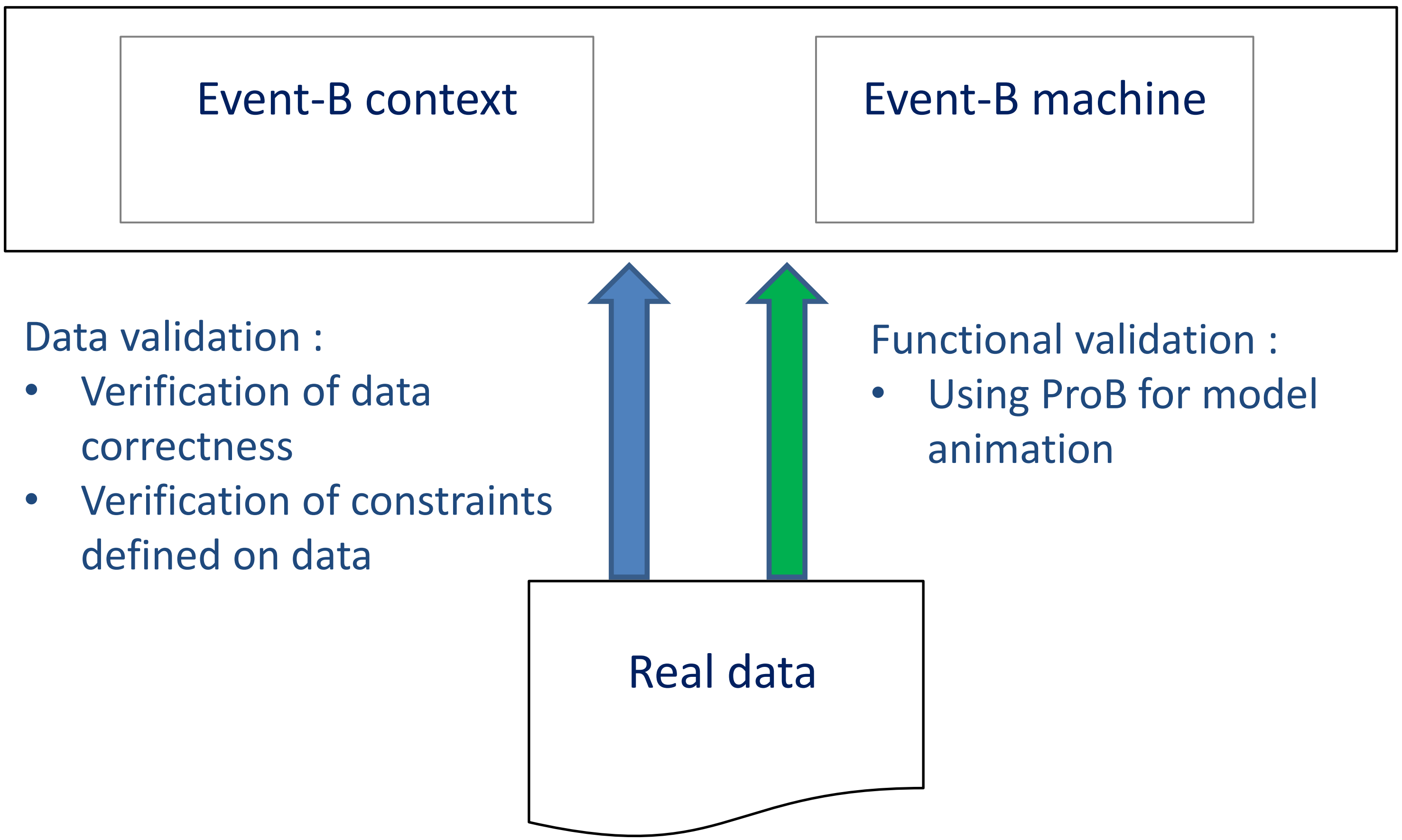
3 - Achievements

Modelling and proof with Rodin

- Proof
  - Automatic proof :
    - Using proof engines integrated in Rodin platform (SMT, AtelierB, etc.)
    - Defining proof tactics
  - Manual proof :
    - Proof of theorems and rules defined in Event-B Theory plug-in components
    - Proof of Event-B components :
      - Using theorems defined in Event-B Theory plug-in components
      - Using manual proof rules defined in Event-B Theory plug-in components

3 - Achievements

Model animation with ProB



Data validation :

- Verification of data correctness
- Verification of constraints defined on data

Functional validation :

- Using ProB for model animation

3 - Achievements

Model animation with ProB

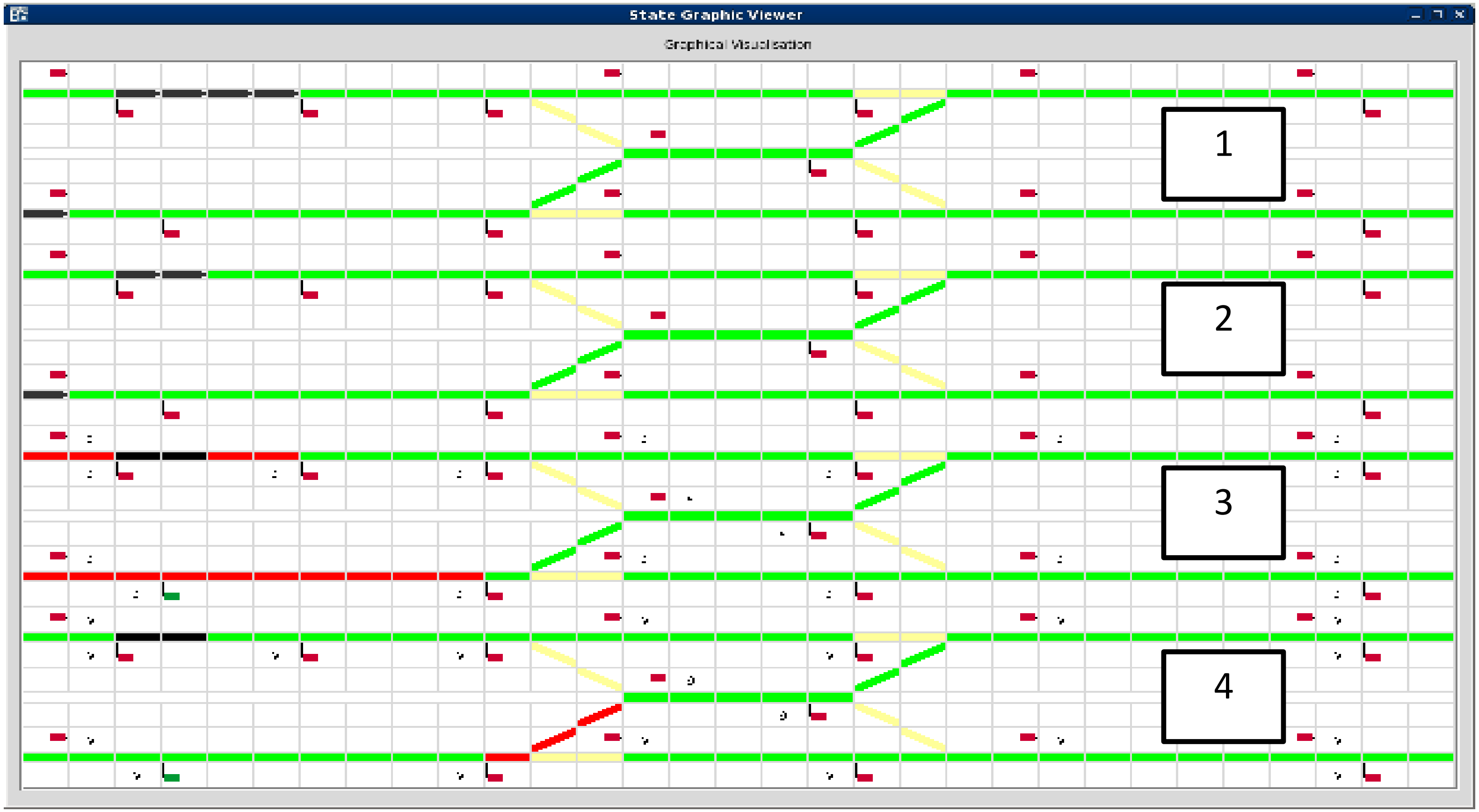
- Manual animation
  - Analysis of degraded modes
    - Track circuits, points and train shunting defaults
  - Analysis of asynchronies due to communication delays
  - Analysis of unsafe scenarios

SEVENTH FRAMEWORK PROGRAMME

3 - Achievements

Model animation with ProB

- Manual animation display



3 - Achievements

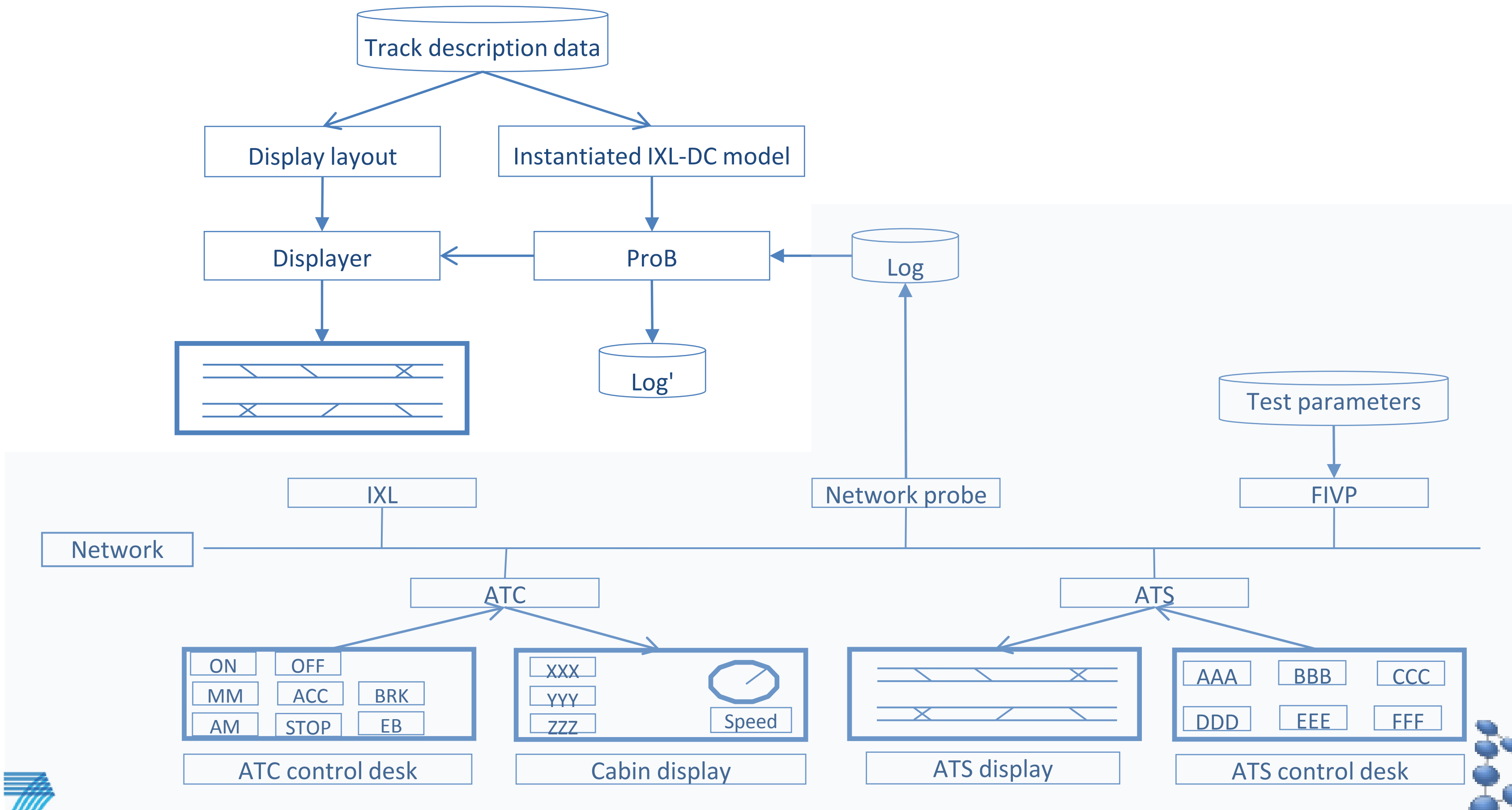
Model animation with ProB

- Automatic animation
  - Test IXL-DC model in realistic conditions
    - Revenue service line
    - Integrated with ATS, ATC and IXL systems
  - Test IXL-DC model with more comprehensive and diverse scenarios
  - Test IXL-DC model is not too restrictive

3 - Achievements

Model animation with ProB

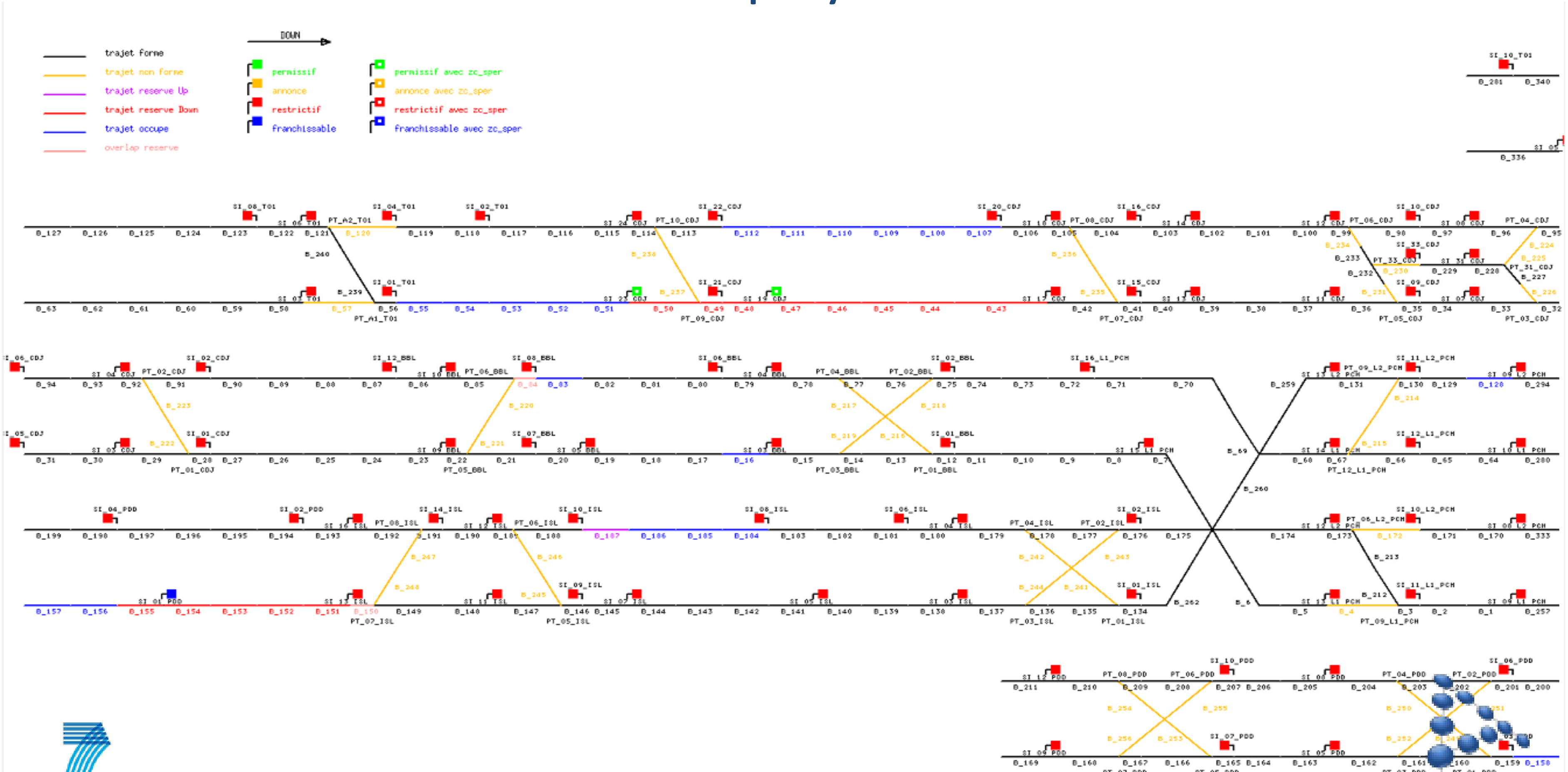
- Automatic animation architecture



3 - Achievements

Model animation with ProB

- Automatic animation display



SEVENTH FRAMEWORK PROGRAMME

3 - Achievements

System Development Process

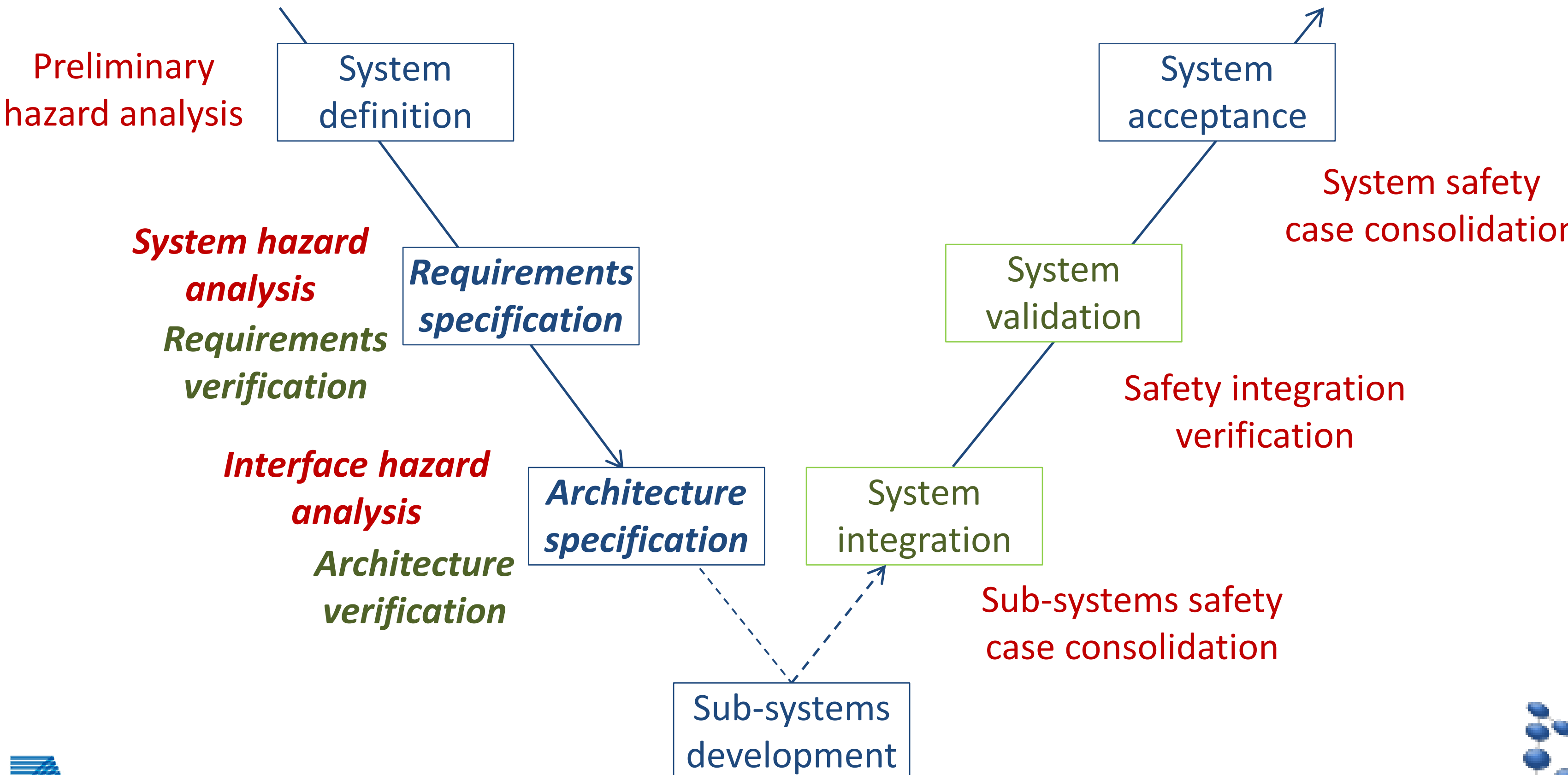
- Goal:
  - Introduce formal model development with Advance methods and tools in a system process compliant with CENELEC standards
- Motivations:
  - Improve quality of system definition
  - Improve V&V effectiveness
  - Reduce V&V costs & non conformity costs
  - Improve traceability with sub-system development and software development

SEVENTH FRAMEWORK PROGRAMME

3 - Achievements

System Development Process

- Flow of activities compliant with CENELEC standards



3 - Achievements

System Development Process

- System definition
  - No particular application of Advance M&T
- Preliminary hazard analysis
  - No particular application of Advance M&T
- Requirements specification
  - Event-B modelling (Rodin)
  - Tests definition by animation (ProB) and co-simulation (ProB – FMI)
  - Proof (Rodin)

3 - Achievements

System Development Process

- System hazard analysis
  - STAMP & STPA
- Requirements verification
  - Event-B model verification
  - Tests scenarios verification
  - Proof report verification
- Architecture specification
  - Sub-system modelling by refinement and decomposition (Rodin)
  - Proof (Rodin)

SEVENTH FRAMEWORK PROGRAMME

3 - Achievements

System Development Process

- Interface hazard analysis
  - STAMP & STPA
- Architecture verification
  - Sub-system models verification
  - Proof verification
- Sub-systems safety case consolidation
  - Reuse of safety cases of sub-systems
- System integration
  - Reuse of proofs to reduce testing

SEVENTH FRAMEWORK PROGRAMME

3 - Achievements

System Development Process

- Safety integration verification
  - Reuse of safety analysis and verifications
- System validation
  - Reuse of tests scenarios
- System safety case consolidation
  - Reuse of safety analysis and verifications

4 - Conclusions

- IXL-DC model has been proved
  - ✓ *Proof that IXL + IXL-DC comply with system safety requirements*
- IXL-DC model is made of a generic part proved once for all and a specific part verified formally for each project
  - ✓ *Proof technique is independent of the complexity and the implementation technology of IXL*
- IXL-DC model specified, created and validated following an integrated system development process
  - ✓ *Integration of Advance M&T in an industrial system development process*

4 - Conclusions

- Creation and proof of IXL-DC model improved the model construction and proof techniques of Event-B and Rodin
  - ✓ *Refinement and model decomposition methods applied*
  - ✓ *Composition/decomposition and "Theory" plugins of Rodin improved*
- Animation of the IXL-DC model improved and extended the capabilities of ProB
  - ✓ *Link with other development processes via scripting and I/O library*
  - ✓ *Performance of ProB's kernel improved*
  - ✓ *New visualisation capabilities of ProBMotion tested and improved*
  - ✓ *Tests of ProB 2's scripting architecture*

4 - Conclusions

- Advance methods and tools for formal system development are powerful and complementary :
  - ✓ *Hazard analysis + Formal modelling + Model animation + Proof*

    => System specification suited & safe by construction

    => Significant costs reduction & quality improvement
- But to be fully compliant with industrial needs :
  - A reliable and sustainable model of development, training and support of Advance methods and tools must be implemented

SEVENTH FRAMEWORK PROGRAMME