Rodin / Event-B and V&V Activities

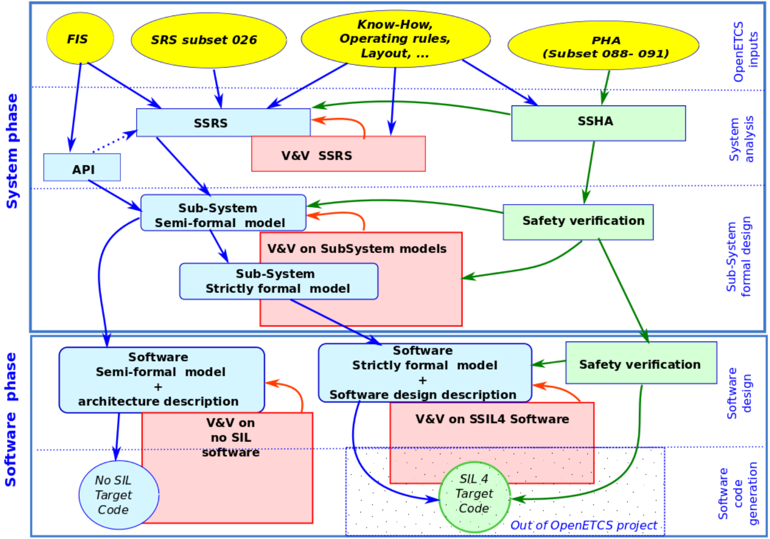
Systerel, Aix-en-Provence

December 5th, 2013

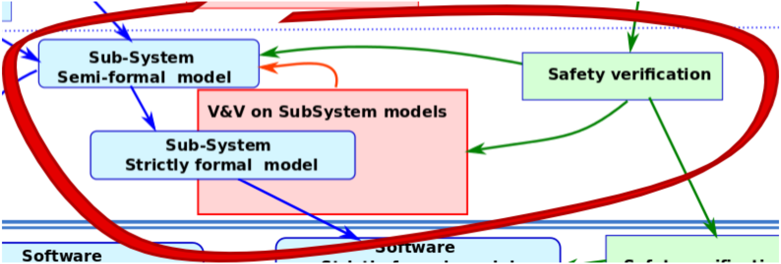
Event-B — System Level B-Method

- **System Level Specifications** states, invariants, observable events, guards, actions. . .
- **Refinement** iterative modeling, from abstract to detailed
- **Proof** automatic generation of proof obligations, tool support for proofs
- **Tool** Rodin — open source tool, developed in RODIN, DEPLOY, ADVANCE EU-projects, several universities and industrial partners

Event-B in openETCS



Event-B in openETCS



Event-B in V&V

Why ?

Event-B allows for reasoning on a high level view of a system. A formalized specification is connected to a (formal) functional system behavior.

Goal : Increase the confidence in the correctness and completeness of safety requirements by formalizing them and providing a formally proven link to a functional system model.

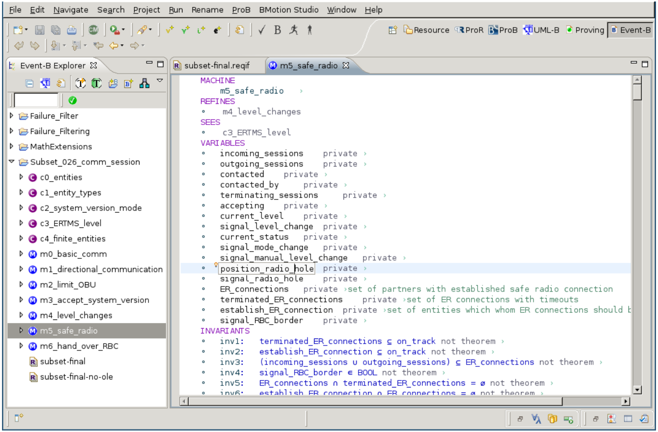
Event-B in V&V

Event-B in V&V for Safety :

- Ensures non-contradicting safety requirements
- Provides a proven correct integration of safety requirements in the model
- Allows to observe the behavior of the system model (simulation)
- Allows for validation of intended effects of safety requirements on the functional behavior
- Provides strong arguments and evidence for certification bodies

Starting Point

Formal Model of Section 3.5.3 (MorC)

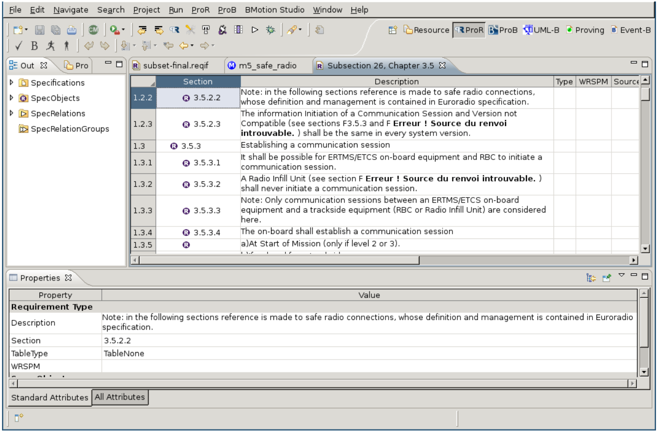


```
MACHINE
    m5_safe_radio   ›
REFINES
•   m4_level_changes
SEES
•   c3_ERTMS_level
VARIABLES
•   incoming_sessions    private ›
•   outgoing_sessions    private ›
•   contacted    private ›
•   contacted_by     private ›
•   terminating_sessions     private ›
•   accepting    private ›
•   current_level    private ›
•   signal_level_change  private ›
•   current_status   private ›
•   signal_mode_change   private ›
•   signal_manual_level_change   private ›
•   position_radio_hole  private ›
•   signal_radio_hole    private ›
•   ER_connections   private ›set of partners with established safe radio connection
•   terminated_ER_connections    private ›set of ER connections with timeouts
•   establish_ER_connection  private ›set of entities which whom ER connections should b
•   signal_RBC_border    private ›
INVARIANTS
•   inv1:   terminated_ER_connections ⊆ on_track not theorem ›
•   inv2:   establish_ER_connection ⊆ on_track not theorem ›
•   inv3:   (incoming_sessions ∪ outgoing_sessions) ⊆ ER_connections not theorem ›
•   inv4:   signal_RBC_border ∈ BOOL not theorem ›
•   inv5:   ER_connections ∩ terminated_ER_connections = ∅ not theorem ›
•   inv6:   establish_ER_connection ∩ ER_connections = ∅ not theorem ›
```

FIGURE: Formal Model Functional Behavior

Starting Point

Requirements with ProR



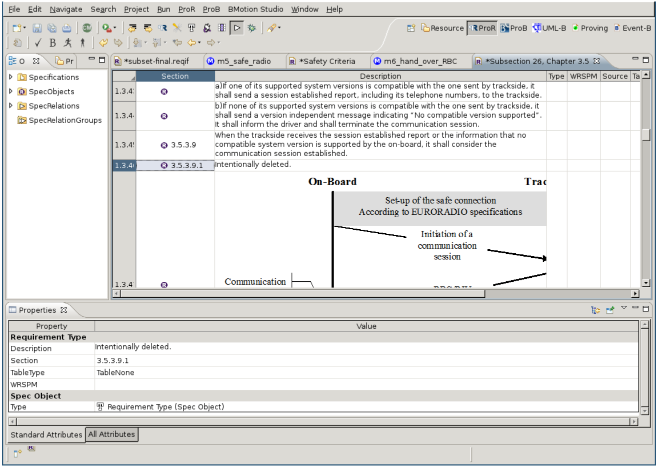
	Section	Description	Type	WRSPM	Sourc
1.2.2	Ⓡ 3.5.2.2	Note: in the following sections reference is made to safe radio connections, whose definition and management is contained in Euroradio specification.			
1.2.3	Ⓡ 3.5.2.3	The information Initiation of a Communication Session and Version not Compatible (see sections F3.5.3 and F **Erreur ! Source du renvoi introuvable.**) shall be the same in every system version.			
1.3	Ⓡ 3.5.3	Establishing a communication session			
1.3.1	Ⓡ 3.5.3.1	It shall be possible for ERTMS/ETCS on-board equipment and RBC to initiate a communication session.			
1.3.2	Ⓡ 3.5.3.2	A Radio Infill Unit (see section F **Erreur ! Source du renvoi introuvable.**) shall never initiate a communication session.			
1.3.3	Ⓡ 3.5.3.3	Note: Only communication sessions between an ERTMS/ETCS on-board equipment and a trackside equipment (RBC or Radio Infill Unit) are considered here.			
1.3.4	Ⓡ 3.5.3.4	The on-board shall establish a communication session			
1.3.5	Ⓡ	a)At Start of Mission (only if level 2 or 3).			

Property	Value
Requirement Type	
Description	Note: in the following sections reference is made to safe radio connections, whose definition and management is contained in Euroradio specification.
Section	3.5.2.2
TableType	TableNone
WRSPM	

FIGURE: ProR Integration in Rodin

Starting Point

Tracing Requirements in Model using ProR



	Section	Description	Type	WRSPM	Source	Ta
1.3.4	Ⓡ	a)If one of its supported system versions is compatible with the one sent by trackside, it shall send a session established report, including its telephone numbers, to the trackside.				
1.3.4	Ⓡ	b)If none of its supported system versions is compatible with the one sent by trackside, it shall send a version independent message indicating "No compatible version supported". It shall inform the driver and shall terminate the communication session.				
1.3.4	Ⓡ 3.5.3.9	When the trackside receives the session established report or the information that no compatible system version is supported by the on-board, it shall consider the communication session established.				
1.3.4	Ⓡ 3.5.3.9.1	Intentionally deleted.				
1.3.4	Ⓡ					

Property	Value
Requirement Type	
Description	Intentionally deleted.
Section	3.5.3.9.1
TableType	TableNone
WRSPM	
Spec Object	
Type	Requirement Type (Spec Object)

Proposed Approach in Safety Verification

- Capture requirements from Safety Analysis
- Classify requirements for low / high (implementation / system) level
- Formalize safety requirements
- Adapt model if necessary
- Validate functionality of the model

Prepare Safety Requirements

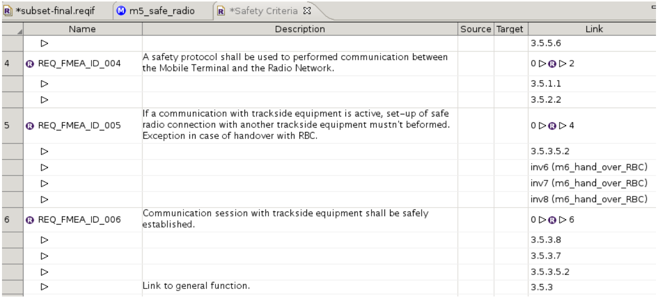
- Capture safety requirements from safety analysis
- Classify low / high level requirements

Example :

REQ_FMEA_ID_005

If a communication with trackside equipment is active, set-up of safe radio connection with another trackside equipment mustn't be performed. Exception in case of handover with RBC.

Prepare Safety Requirements



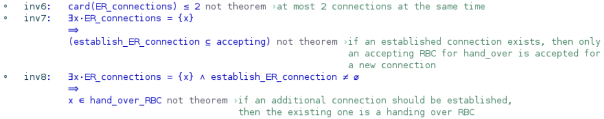
	Name	Description	Source	Target	Link
	▷				3.5.5.6
4	Ⓡ REQ_FMEA_ID_004	A safety protocol shall be used to performed communication between the Mobile Terminal and the Radio Network.			0 ▷ Ⓡ ▷ 2
	▷				3.5.1.1
	▷				3.5.2.2
5	Ⓡ REQ_FMEA_ID_005	If a communication with trackside equipment is active, set-up of safe radio connection with another trackside equipment mustn't beformed. Exception in case of handover with RBC.			0 ▷ Ⓡ ▷ 4
	▷				3.5.3.5.2
	▷				inv6 (m6_hand_over_RBC)
	▷				inv7 (m6_hand_over_RBC)
	▷				inv8 (m6_hand_over_RBC)
6	Ⓡ REQ_FMEA_ID_006	Communication session with trackside equipment shall be safely established.			0 ▷ Ⓡ ▷ 6
	▷				3.5.3.8
	▷				3.5.3.7
	▷				3.5.3.5.2
	▷	Link to general function.			3.5.3

FIGURE: Safet Requirements in ReqIf (ProR)

Formalize Requirements

REQ_FMEA_ID_005 breakdown :

- At most 2 communication connections at the same time.
- If an active connection exists, only an accepting RBC can establish a new connection.
- If a new connection must be established, then the existing connection is with a handing-over RBC.

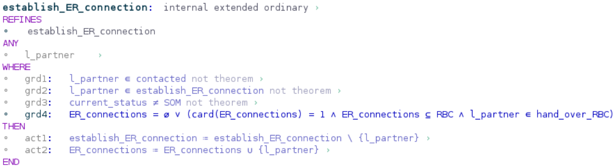


```
∘  inv6:   card(ER_connections) ≤ 2 not theorem ›at most 2 connections at the same time
∘  inv7:   ∃x·ER_connections = {x}
           ⇒
           (establish_ER_connection ⊆ accepting) not theorem ›if an established connection exists, then only
                                                               an accepting RBC for hand_over is accepted for
                                                               a new connection
∘  inv8:   ∃x·ER_connections = {x} ∧ establish_ER_connection ≠ ∅
           ⇒
           x ∈ hand_over_RBC not theorem ›if an additional connection should be established,
                                          then the existing one is a handing over RBC
```

FIGURE: Formalized Safety Requirements

Proof / Adapt Model

- Safety Requirements not fulfilled on initial model (**Reason** Limits on simultaneous connections not completely specified in SS 026)
- Formal Proofs give insight into Reasons (**Feedback** for model adaptation)
- Model Refinement (**Restriction** of behavior to respect safety requirements)

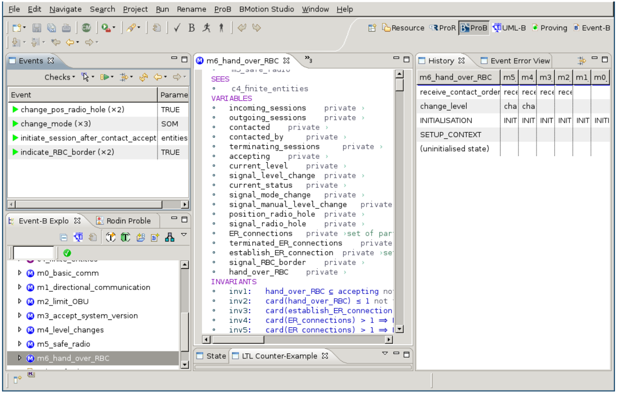


```
establish_ER_connection:  internal extended ordinary ›
REFINES
∘    establish_ER_connection
ANY
∘   l_partner    ›
WHERE
∘   grd1:    l_partner ∈ contacted not theorem ›
∘   grd2:    l_partner ∈ establish_ER_connection not theorem ›
∘   grd3:    current_status ≠ SOM not theorem ›
∘   grd4:    ER_connections = ∅ ∨ (card(ER_connections) = 1 ∧ ER_connections ⊆ RBC ∧ l_partner ∈ hand_over_RBC)
THEN
∘   act1:    establish_ER_connection ≔ establish_ER_connection \ {l_partner} ›
∘   act2:    ER_connections ≔ ER_connections ∪ {l_partner} ›
END
```

FIGURE: Model Refinement for Safety Requirements

Validate Functionality

Is the refined model still functional ?



Event	Parame
change_pos_radio_hole (×2)	TRUE
change_mode (×3)	SOM
initiate_session_after_contact_accept	entities
indicate_RBC_border (×2)	TRUE

```
m6_hand_over_RBC
SEES
∘   c4_finite_entities
VARIABLES
∘   incoming_sessions    private ›
∘   outgoing_sessions    private ›
∘   contacted    private ›
∘   contacted_by    private ›
∘   terminating_sessions    private ›
∘   accepting    private ›
∘   current_level    private ›
∘   signal_level_change  private ›
∘   current_status   private ›
∘   signal_mode_change   private ›
∘   signal_manual_level_change   private
∘   position_radio_hole  private ›
∘   signal_radio_hole    private ›
∘   ER_connections   private ›set of par
∘   terminated_ER_connections   private
∘   establish_ER_connection  private ›se
∘   signal_RBC_border    private ›
∘   hand_over_RBC    private ›
INVARIANTS
∘   inv1:   hand_over_RBC ⊆ accepting no
∘   inv2:   card(hand_over_RBC) ≤ 1 not
∘   inv3:   card(establish_ER_connection
∘   inv4:   card(ER_connections) > 1 ⇒
∘   inv5:   card(ER_connections) > 1 ⇒
```

m6_hand_over_RBC	m5	m4	m3	m2	m1	m0
receive_contact_order	rece	rece	rece	rece		
change_level	cha	cha				
INITIALISATION	INIT	INIT	INIT	INIT	INIT	INITI
SETUP_CONTEXT						
(uninitialised state)						

FIGURE: Formal Model Animation with ProB

Conclusion

- Formalized safety (or other additional) requirements
  - derive properties for later implementation
  - proof completeness of these properties
  - detection of contradictions / missing elements in specification
- Validation of functional requirements after safety requirements integration
- Technical Point of View
  - Excellent integration of Rodin with ProR (both based on Eclipse)
  - Requirements in standardized ReqIf format