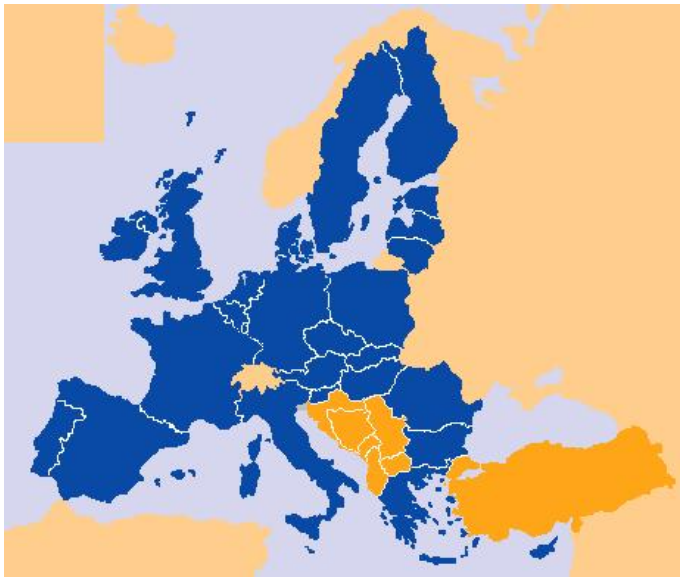
Event-B for Safety Analysis of Critical Systems

Matthias Güdemann and Marielle Petit-Doche

Systerel, Aix-en-Provence

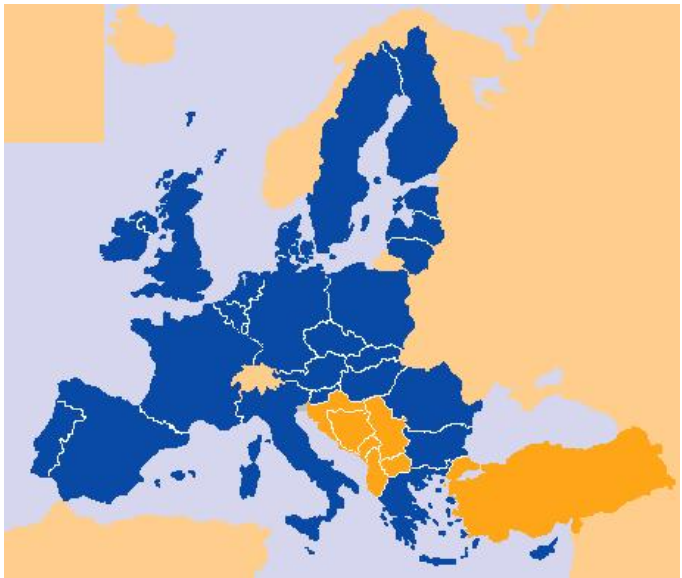
June 3rd, 2014

Contents



[1] [2]

1. http ://www.disputeabout.eu/dwn/1003/25767en_USI_enlargementmapsm.jpg
2. http ://www.omanewsu.com/wp-content/uploads/2012/10/EU-map-large.jpg



1

2

1. http ://www.disputeabout.eu/dwn/1003/25767en_USI_enlargementmapsm.jpg
2. http ://www.omanewsu.com/wp-content/uploads/2012/10/EU-map-large.jpg

European Train Control System (ETCS) Specification (ERA)

- Facilitation of Cross-Border Trains
- Data Transfer over Wireless Technique (GPRS)
- Goal : Homogenization of Train Signalling (up to $500\frac{km}{h}$)

Challenge : Informal Specification with room for interpretation. Very different detail level (requirements, implementation detail, notes etc.)

openETCS

Aims at providing a formal model, open proof and open source toolchain for ETCS.

European Train Control System (ETCS) Specification (ERA)

- Facilitation of Cross-Border Trains
- Data Transfer over Wireless Technique (GPRS)
- Goal : Homogenization of Train Signalling (up to $500\frac{km}{h}$)

Challenge : Informal Specification with room for interpretation. Very different detail level (requirements, implementation detail, notes etc.)

openETCS

Aims at providing a formal model, open proof and open source toolchain for ETCS.

sterel

Overview

- Functional Model for Management of Radio Communication (MoRC)
- Safety Activities with Rodin
- Conclusion

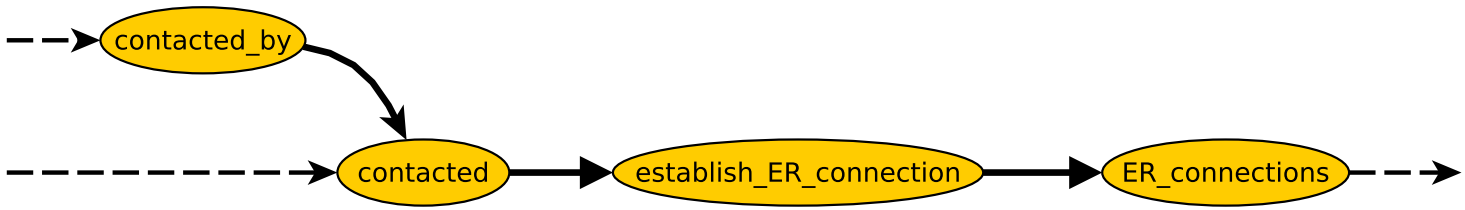
Contents

Management of Radio Communication

- Participants
  - On-Board Units (OBU)
  - Radio Infill Units (RIU)
  - Radio Block Centers (RBC)
- Section §3.5 of ETCS spec
  - Initiate, Maintain and Terminate Radio Communication
- Critical Function : Radio Communication for Movement Authority / Speed Limits

Event-B Model for MoRC

- Type *entities*
  - partitioned into set of OBU, RIU and RBC entities
- State of Communication
  - Communication direction (incoming, outgoing)
  - Protocol stage for each communication session

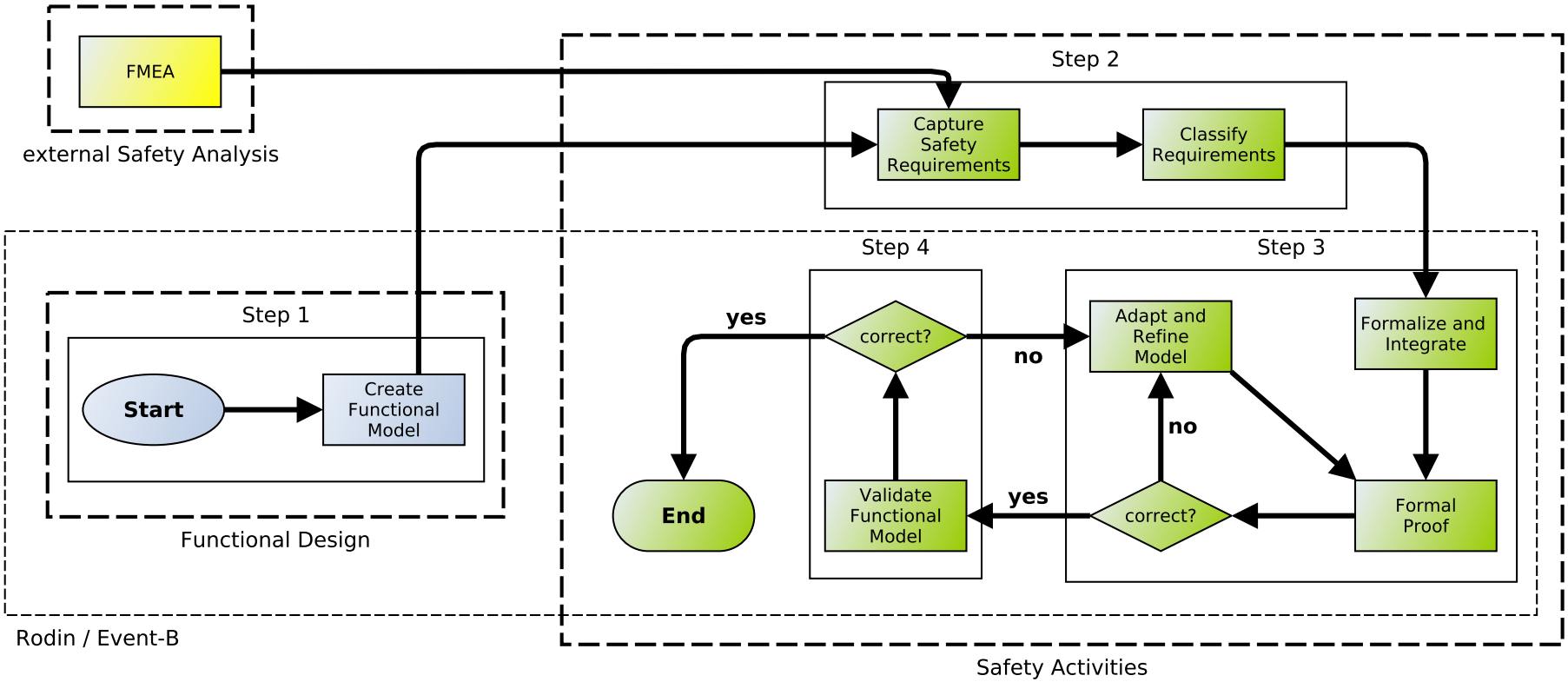


Event-B Machine Refinement

- Machine 0 - *Basic Communication*
- Machine 1 - *Directional Communication*
- Machine 2 - *Limit to OBU viewpoint*
- Machine 3 - *System Level Compatibility*
- Machine 4 - *Level Changes Support*
- Machine 5 - *Safe Radio Communication*

Contents

Safety Support with Event-B



Safety Requirements

Failure Modes and Effects Analysis (FMEA)

Hazard

"Exceeding the safe speed or distance as advised to ETCS."

- **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.
- **REQ_FMEA_ID_007** Establishment of communication session shall be performed when no communication is active. Exception in case of handover with RBC.

Safety Requirements

Failure Modes and Effects Analysis (FMEA)

Hazard

"Exceeding the safe speed or distance as advised to ETCS."

- **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.
- **REQ_FMEA_ID_007** Establishment of communication session shall be performed when no communication is active. Exception in case of handover with RBC.

Safety Requirements

Failure Modes and Effects Analysis (FMEA)

Hazard

"Exceeding the safe speed or distance as advised to ETCS."

- **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.
- **REQ_FMEA_ID_007** Establishment of communication session shall be performed when no communication is active. Exception in case of handover with RBC.

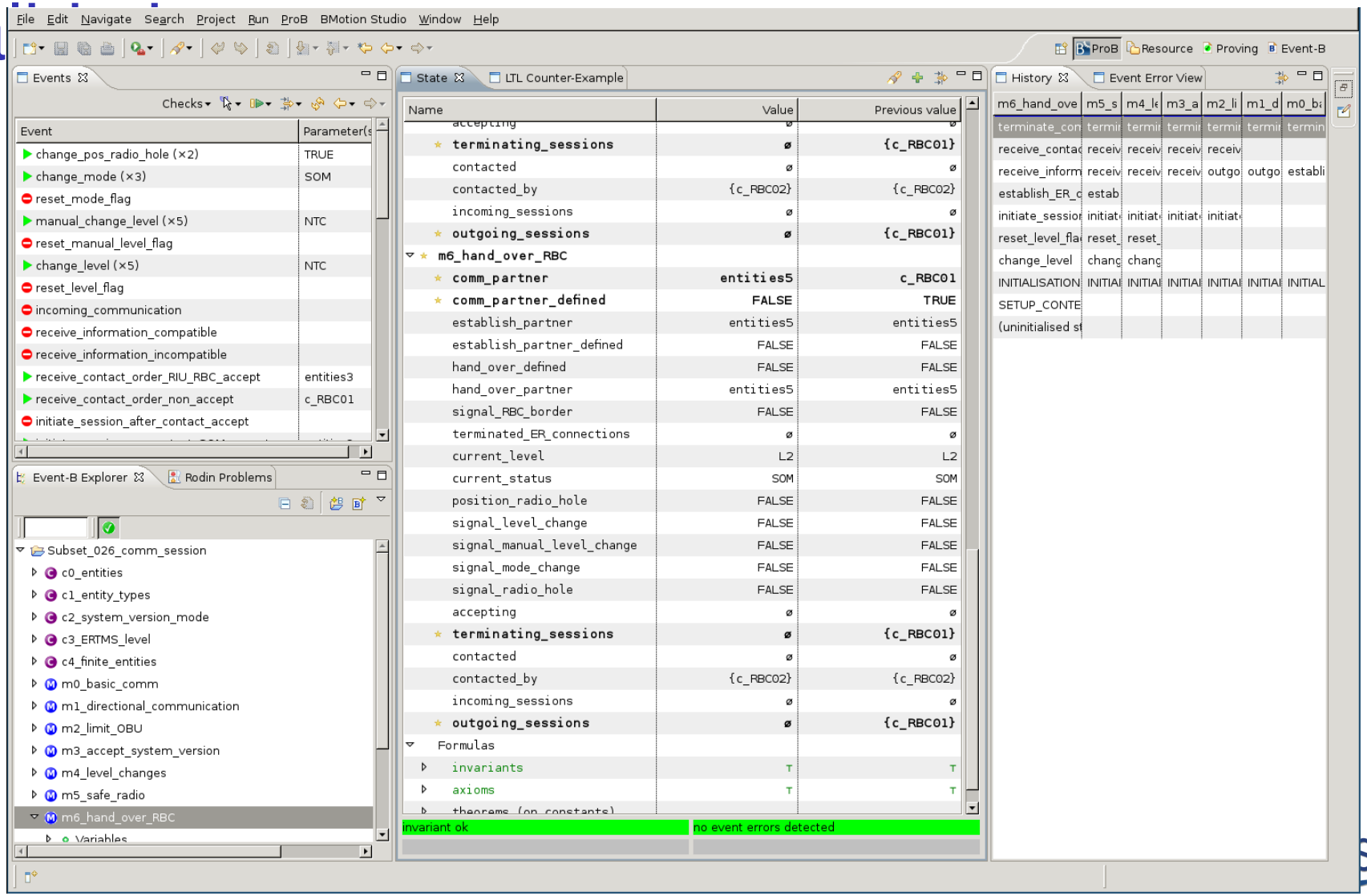
Integration into Model

- Machine 3
  - Establish additional connection only with RBC for hand-over
- Machine 6 - *Explicit hand-over RBC*
  - Refine set *establish_ER_connections* with one variable
  - Refine set *ER_connections* with two variables
  - Invariants to show size limitations and correct hand-over with RBC

Validation

- Establish communication with on-track equipment
- Establish hand-over with two RBCs
- Terminate and re-establish a communication session

Va


File Edit Navigate Search Project Run ProB BMotion Studio Window Help
ProB Resource Proving Event-B
Events
Checks
Event
Parameter(s
change_pos_radio_hole (×2)
TRUE
change_mode (×3)
SOM
reset_mode_flag
manual_change_level (×5)
NTC
reset_manual_level_flag
change_level (×5)
NTC
reset_level_flag
incoming_communication
receive_information_compatible
receive_information_incompatible
receive_contact_order_RIU_RBC_accept
entities3
receive_contact_order_non_accept
c_RBC01
initiate_session_after_contact_accept
Event-B Explorer
Rodin Problems
Subset_026_comm_session
c0_entities
c1_entity_types
c2_system_version_mode
c3_ERTMS_level
c4_finite_entities
m0_basic_comm
m1_directional_communication
m2_limit_OBU
m3_accept_system_version
m4_level_changes
m5_safe_radio
m6_hand_over_RBC
Variables
State
LTL Counter-Example
Name
Value
Previous value
terminating_sessions
ø
{c_RBC01}
contacted
ø
ø
contacted_by
{c_RBC02}
{c_RBC02}
incoming_sessions
ø
ø
outgoing_sessions
ø
{c_RBC01}
m6_hand_over_RBC
comm_partner
entities5
c_RBC01
comm_partner_defined
FALSE
TRUE
establish_partner
entities5
entities5
establish_partner_defined
FALSE
FALSE
hand_over_defined
FALSE
FALSE
hand_over_partner
entities5
entities5
signal_RBC_border
FALSE
FALSE
terminated_ER_connections
ø
ø
current_level
L2
L2
current_status
SOM
SOM
position_radio_hole
FALSE
FALSE
signal_level_change
FALSE
FALSE
signal_manual_level_change
FALSE
FALSE
signal_mode_change
FALSE
FALSE
signal_radio_hole
FALSE
FALSE
accepting
ø
ø
terminating_sessions
ø
{c_RBC01}
contacted
ø
ø
contacted_by
{c_RBC02}
{c_RBC02}
incoming_sessions
ø
ø
outgoing_sessions
ø
{c_RBC01}
Formulas
invariants
T
T
axioms
T
T
invariant ok
no event errors detected
History
Event Error View
m6_hand_ove
m5_s
m4_k
m3_a
m2_li
m1_d
m0_ba
terminate_con
receive_contac
receive_inform
establish_ER_c
initiate_sessio
reset_level_fla
change_level
INITIALISATION
SETUP_CONTE
(uninitialised st

Contents

Conclusion

- Possibility to identify problems in the specification / requirements
- Provides strong link of the model to the specification
- Importance of Traceability of Requirements
- Possibility to validate the Intended Behavior (Functional and Risk Mitigation)

Questions

Collaboration / Diffs on models ?
Animation of decomposed models ?

Conclusion

- Possibility to identify problems in the specification / requirements
- Provides strong link of the model to the specification
- Importance of Traceability of Requirements
- Possibility to validate the Intended Behavior (Functional and Risk Mitigation)

Questions

Collaboration / Diffs on models ?
Animation of decomposed models ?