

## Work-Package 7: "Toolchain"

## Event-B Model of Subset 026, Section 3.5.3

Matthias Güdemann

May 2013



## Funded by:


 Federal Ministry  
 of Education  
 and Research

 Région de  
 Bruxelles-  
 Capitale

 GOBIERNO DE ESPAÑA  
 MINISTERIO DE INDUSTRIA, ENERGÍA  
 Y TURISMO


This page is intentionally left blank

**Work-Package 7: “Toolchain”**

**OETCS  
May 2013**

## Event-B Model of Subset 026, Section 3.5.3

Matthias GÜdemann

Systemel  
Les Portes de l'Arbois, Bâtiment A  
1090 rue René Descartes  
13857 Aix-en-Provence Cedex 3, France

Model Description

Prepared for openETCS@ITEA2 Project

**Disclaimer:** This work is licensed under the "openETCS Open License Terms" (oOLT) dual Licensing: European Union Public Licence (EURL v.1.1+) AND Creative Commons Attribution-ShareAlike 3.0 – (cc by-sa 3.0)

THE WORK IS PROVIDED UNDER openETCS OPEN LICENSE TERMS (oOLT) WHICH IS A DUAL LICENSE AGREEMENT INCLUDING THE TERMS OF THE EUROPEAN UNION PUBLIC LICENSE (VERSION 1.1 OR ANY LATER VERSION) AND THE TERMS OF THE CREATIVE COMMONS PUBLIC LICENSE ("CCPL"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS OLT LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

<http://creativecommons.org/licenses/by-sa/3.0/>

<http://joinup.ec.europa.eu/software/page/eupl/licence-eupl>

# Table of Contents

1	Modeling Strategy .....	5
2	Model Overview .....	5
3	Model Benefits .....	6
4	Detailed Model Description.....	7
4.1	Context 0 - Entities.....	8
4.2	Machine 0 - Basic Communication.....	8
4.3	Machine 1 - Directional Communication.....	9
4.4	Context 1 - Entity Types .....	10
4.5	Machine 2 - On Board Modeling.....	10
4.6	Context 2 - System Version Compatibility .....	12
4.7	Machine 3 - Accepting RBC and System Version .....	13
4.8	Context 3 - ERTMS Levels .....	15
4.9	Machine 4 - ERTMS Level Changes .....	16
4.10	Machine 5 - Safe Radio Connection.....	19
	References .....	28

# Figures and Tables

**Figures**

Figure 1. Overview on State Machine and Context Hierarchy ..... 6

Figure 2. Traceability in ReqIf file using ProR..... 7

**Tables**

Table 1. Glossary ..... 5

This document describes a formal model of the requirements of section 3.5.3 of the subset 026 of the ETCS specification 3.3.0 [Eur12]. This section describes the establishing of a communication connection between on-board and on-track equipment.

The model is expressed in the formal language Event-B [Abr10] and developed within the Rodin tool [Jas12]. This formalism allows an iterative modeling approach. In general, one starts with a very abstract description of the basic functionality and step-wise adds additional details until the desired level of accuracy of the model is reached. Rodin provides the necessary proof support to ensure the correctness of the refined behavior.

In this document we present an Event-B model of the protocol to initiate a communication session in an ETCS implementation, as implemented from the on-board unit. At first, we describe shortly the background of Event-B, then the overall approach taken to model this section and finally present the model in detail. For each of the iterative modeling steps, we describe the details added by the refinement.

For a short introduction on Event-B and the usage of Rodin with models on github see [https://github.com/openETCS/model-evaluation/blob/master/model/B-Systemrel/Event\\_B/rodin-projects-github.pdf?raw=true](https://github.com/openETCS/model-evaluation/blob/master/model/B-Systemrel/Event_B/rodin-projects-github.pdf?raw=true)

OBU	on board unit
RIU	radio in-fill unit
RBC	radio block centre
SRS	system requirements specification

**Table 1. Glossary**

## 1 Modeling Strategy

The section 3.5.3 of the SRS describes how a communication session is established. In its context, the low level EURORADIO network connection (cf. §3.5.1.1) is considered basic functionality and is not part of the modeling.

The basic modeling element are entities which represent one piece of equipment, either on-board, i.e., on the train, or on-track. The model is constructed from the local point of view of an OBU entity. On-track entities are only modeled as possible communication partners.

## 2 Model Overview

Figure 1 shows the structure of the Event-B model. The left column represents the abstract state machines, the right column the contexts. An arrow from one machine to another machine represents a refinement relation, an arrow from a machine to a context represents a sees relation and arrow from one context to another represents an extension relation.

The modeling starts with the very abstract possibility to establish and to terminate a communication session in the machine  $m0$ , the set of entities is defined in the context  $c0$ . This basic functionality is refined in the succeeding machines to incorporate the different stages of the protocol to establish a session. The contexts further refine the entities to on-track and on-board entities and limit the modeling to the point of view of an OBU.

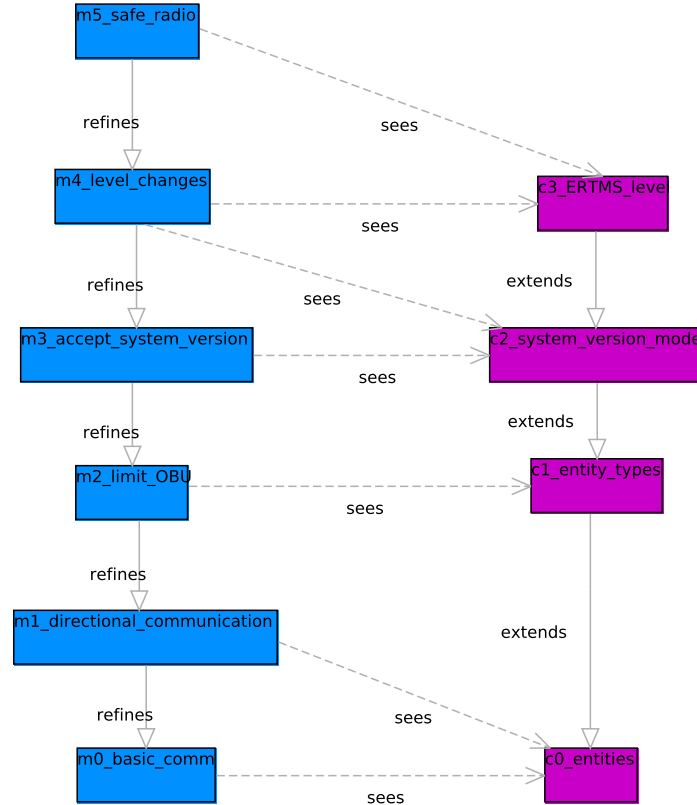


Figure 1. Overview on State Machine and Context Hierarchy

The machine *m1* discerns incoming and outgoing communication sessions, i.e., initiated by the modeled piece of equipment or by an external one. The context *c1* introduces the different types of equipment which are used in *m2* to refine the two different protocols for outgoing and incoming sessions and to limit the model to the OBU point of view. *c2* introduces the notion of compatible systems. This is used in *m3* to identify on-track equipment with a compatible system version. This machine also discerns between accepting and non-accepting RBCs to contact. *c3* adds the different ERTMS levels and the relevant train modes to the model. This is used in *m4* to model the different situations where a communication session must be established. *m5* adds the notion of safe radio connection as low-level prerequisite for a communication session.

The representation of the state machines of the modeled protocols for establishing a communication session is modeled implicitly. The model allows sessions with different partners in parallel (but respects the constraints of the specification like §3.5.3.5.2). The state of the protocol with different partners is tracked by adding / removing these partners from sets representing those different states of the protocol.

### 3 Model Benefits

The Event-B model in Rodin has some interesting properties which are highlighted here. Some stem from the fact that Rodin is well integrated into the Eclipse platform which renders many useful plugins available, both those explicitly developed for integration with Rodin, but also other without Rodin in mind. Other interesting properties stem from the fact that Rodin and Event-B provide an extensive proof support for properties.



- **Refinement** The Event-B approach allows iterative development based on refinement. This allows starting modeling with a very abstract machine and then step-wise adding more detailed behavior. Rodin generates all the necessary proof obligations which are required to assure correct refinement.
- **Requirements Tracing** Rodin provides an extensible EMF model, therefore it is easily possible to trace requirements using the requirements modeling framework of Eclipse (RMF) via the ProR plugin. This allows the usage of requirement documents in the OMG standardized Requirements Interchange Format (ReqIF). Figure 2 shows the requirements tracing using ProR in Rodin.

Section	Description	Source Change	Target Change	Link
1	3.5			
1.1	3.5.1.1			
1.2	3.5.2			
1.3	3.5.2.1			0 > 1
1.4	3.5.2.2			comm_sessions-/Subset_026_comm_session/m0_basic_cor
1.5	3.5.2.3			
1.6	3.5.3			
1.7	3.5.3.1			0 > 3
1.8	3.5.3.2			event outgoing_communication where @grd3 l_partner ∈ event incoming_communication where @grd3 l_partner ∈ axm4: my_entity ∈ on_board-/Subset_026_comm_session/h
1.9	3.5.3.3			0 > 1 event incoming_communication where @grd3 l_partner ∈
1.10	3.5.3.4			
1.11	3.5.3.4			0 > 1 event initiate_session_no_contact_SOM where @grd6 curr
1.12	3.5.3.4			0 > 2

Figure 2. Traceability in ReqIf file using ProR

- **Model Animation** The Event-B model can be animated via different plugins, e.g., ProB or AnimB. This allows the simulation of the model, by clicking on the activated events and tracking the resulting state of the variables. This technique allows to examine the run-time behavior of the model, e.g., for testing purposes. There is also ongoing development for a model-based testing plugin in Rodin, which will allow storing and replaying of event sequences.
- **Non-Testable Requirements** The Event-B model supports the specification of invariants which can be formally proven using the proof support of Rodin. This includes for example the non-testable requirement specified in the subset 076 for §3.5.3.2 (see Section 4.5).
- **Safety Properties** Using Rodin's proof support and the formalization as invariants, it is possible to formalize and prove the identified safety properties of the case study (see Section 4.7).

## 4 Detailed Model Description

This section describes in more detail the formal model, beginning from the most abstract Event-B machine. For each refinement, in general only the important changes will be shown, the complete model is available as a Rodin project. At each step the additional modeled functionality and its representation will be described. In particular the initialization event is not shown for the refined machines. If not mentioned explicitly, sets are initialized empty, integers with value 0 and Boolean variables with false.

#### 4.1 Context 0 - Entities

This context defines the type of entities with whom a communication session can be established. *my\_entity* represents the piece of equipment which is modeled.

**CONTEXT** c0\_entities

**SETS**

*entities*

**CONSTANTS**

*my\_entity*

**AXIOMS**

*axm1* : *my\_entity*  $\in$  *entities*

**END**

#### 4.2 Machine 0 - Basic Communication

This state machine represents the basic functionality. It allows for the creation and the termination of a communication session with another entity. The sessions are represented by the state variable *session* which can contain values of type *entities*. The respective events are triggered with a parameter *l\_partner* representing the communication partner.

##### Implemented Requirements

- each session allows for communication between two entities (cf. §3.5.2.1)

**SEES** c0\_entities

**VARIABLES**

*sessions*

**INVARIANTS**

*inv1* : *sessions*  $\subseteq$  *entities*  $\setminus$  {*my\_entity*}

**EVENTS**

**Initialisation**

**begin**

*act1* : *sessions* :=  $\emptyset$

**end**

**Event** *establish\_communication*  $\hat{=}$

**any**

*l\_partner*

**where**

*grd1* : *l\_partner*  $\notin$  *sessions*

*grd2* : *l\_partner*  $\neq$  *my\_entity*

**then**

*act1* : *sessions* := *sessions*  $\cup$  {*l\_partner*}

```

    end
Event terminate_communication  $\hat{=}$ 
    any
         $l\_partner$ 
    where
        grd1 :  $l\_partner \in sessions$ 
    then
        act1 :  $sessions := sessions \setminus \{l\_partner\}$ 
    end
END

```

### 4.3 Machine 1 - Directional Communication

The first refinement of the machine refines the notion of communication session to incoming sessions, i.e., where another entity initiates a session with *my\_entity* and outgoing sessions where *my\_entity* initiates the session.

The data refinement is proven by the invariant which states that *sessions* is equal to the disjoint union of *outgoing\_sessions* and *incoming\_sessions*. The abstract *establish\_session* event is refined to the two events *incoming\_session* and *outgoing\_session*.

**REFINES** m0\_basic\_comm

**SEES** c0\_entities

**VARIABLES**

*incoming\_sessions*

*outgoing\_sessions*

**INVARIANTS**

inv1 :  $partition(sessions, incoming\_sessions, outgoing\_sessions)$

**EVENTS**

**Event** incoming\_communication  $\hat{=}$

**refines** establish\_communication

any

$l\_partner$

where

grd1 :  $l\_partner \notin incoming\_sessions \cup outgoing\_sessions$

grd2 :  $l\_partner \neq my\_entity$

then

act1 :  $incoming\_sessions := incoming\_sessions \cup \{l\_partner\}$

end

**Event** outgoing\_communication  $\hat{=}$

**refines** establish\_communication

any

$l\_partner$

where

```

    grd2 : l_partner ≠ my_entity
    grd1 : l_partner ∉ incoming_sessions ∪ outgoing_sessions
  then
    act1 : outgoing_sessions := outgoing_sessions ∪ {l_partner}
  end
Event terminate_communication ≡
refines terminate_communication
  any
    l_partner
  where
    grd1 : l_partner ∈ incoming_sessions ∪ outgoing_sessions
  then
    act1 : incoming_sessions := incoming_sessions \ {l_partner}
    act2 : outgoing_sessions := outgoing_sessions \ {l_partner}
  end
END

```

#### 4.4 Context 1 - Entity Types

The first context extension introduces the different types of entities relevant in this requirement subset, i.e., on-board unit (OBU), radio in-fill unit (RIU) or radio block centre (RBC). Every entity has a unique type. The goal is to model the communication protocol from the point of view of an OBU, therefore the type of *my\_entity* is restricted to OBU.

**CONTEXT** c1\_entity\_types

**EXTENDS** c0\_entities

**CONSTANTS**

*RBC*

*RIU*

*OBU*

*on\_track*

*on\_board*

**AXIOMS**

axm1 : partition(entities, RBC, RIU, OBU)

axm2 : on\_track = RIU ∪ RBC

axm3 : on\_board = OBU

axm4 : my\_entity ∈ on\_board

**END**

#### 4.5 Machine 2 - On Board Modeling

The next machine refinement adds the notion of being contacted by an on-track entity to establish a communication session. It also adds the first state of the protocol, i.e., entities which should be contacted with the “Initiation of a communication session” message. On-track entities which

order *my\_entity* to contact are stored in the *contacted\_by* set, entities to which the first message is sent by *my\_entity* are stored in the set *contacted*, representing those which are in the first stage of the protocol.

The invariants prove that *my\_entity* will only be in contact with on-track entities and that any entities which are considered for a communication session are on-track entities. Any entity with whom there is already a communication session will not be considered for another session, and finally no radio in-fill unit can initiate a communication session with *my\_entity*.

### Implemented Requirements

- It shall be possible for OBU and RBC to initiate communication session (cf. §3.5.3.1)
- RIU cannot initiate a communication session (cf. §3.5.3.2)

This invariant is marked as non-testable in Subset-076.

The other invariants ensure that a communication partner is not in different states of the communication protocol at the same time. A session protocol can be started by the order to contact an RBC or directly by the OBU.

**REFINES** m1\_directional\_communication

**SEES** c1\_entity\_types

**VARIABLES**

*contacted*

*contacted\_by*

**INVARIANTS**

*inv1* :  $incoming\_sessions \cup outgoing\_sessions \subseteq on\_track$

*inv2* :  $contacted \subseteq on\_track$

*inv3* :  $contacted\_by \subseteq on\_track$

*inv4* :  $contacted\_by \cap (incoming\_sessions \cup outgoing\_sessions) = \emptyset$

*inv5* :  $contacted \cap (incoming\_sessions \cup outgoing\_sessions) = \emptyset$

*inv6* :  $incoming\_sessions \cap RIU = \emptyset$

*inv7* :  $contacted \cap contacted\_by = \emptyset$

**EVENTS**

**Event** *incoming\_communication*  $\widehat{=}$

**refines** *incoming\_communication*

**any**

*l\_partner*

**where**

*grd1* :  $l\_partner \notin incoming\_sessions \cup outgoing\_sessions$

*grd3* :  $l\_partner \in on\_track \setminus RIU$

*grd4* :  $l\_partner \notin contacted$

*grd5* :  $l\_partner \notin contacted\_by$

**then**

*act1* :  $incoming\_sessions := incoming\_sessions \cup \{l\_partner\}$

```

    end
  Event receive_contact_order  $\hat{=}$ 
    any
       $l\_partner$ 
    where
      grd1 :  $l\_partner \notin contacted \cup contacted\_by \cup incoming\_sessions \cup outgoing\_sessions$ 
      grd2 :  $l\_partner \in on\_track$ 
    then
      act1 :  $contacted\_by := contacted\_by \cup \{l\_partner\}$ 
    end
  Event initiate_session_after_contact  $\hat{=}$ 
    any
       $l\_partner$ 
    where
      grd2 :  $l\_partner \in contacted\_by$ 
    then
      act1 :  $contacted := contacted \cup \{l\_partner\}$ 
      act2 :  $contacted\_by := contacted\_by \setminus \{l\_partner\}$ 
    end
  Event initiate_session_no_contact  $\hat{=}$ 
    any
       $l\_partner$ 
    where
      grd5 :  $l\_partner \notin incoming\_sessions \cup outgoing\_sessions \cup contacted \cup contacted\_by$ 
      grd3 :  $l\_partner \in on\_track$ 
    then
      act2 :  $contacted := contacted \cup \{l\_partner\}$ 
    end
  END

```

#### 4.6 Context 2 - System Version Compatibility

The next context extension introduces the notion of compatible system versions. This is modeled as a static property of the on-track equipment wrt. *my\_entity*, i.e., the context axiom that *system\_version\_compatible* is a subset of all on-track entities. On this level of abstraction, there is no need for a finer grained notion of compatibility.

**EXTENDS** c1\_entity\_types

**CONSTANTS**

*system\_version\_compatible*

**AXIOMS**

axm1 :  $system\_version\_compatible \subseteq on\_track$

**END**

#### 4.7 Machine 3 - Accepting RBC and System Version

The next machine refines the contact order events by discerning between the orders to contact an accepting or a non-accepting RBC. The notion of being an accepting RBC is considered to be a dynamic property and therefore modeled as a variable, i.e., the set *accepting*.

The *receive\_contact\_order* event is refined by two separate events, one for orders for an accepting RBC and one for a non-accepting RBC. The *outgoing\_communication* event is refined by two events, one for a compatible system version and the other for an incompatible one. The events for *initiate\_session\_contact* and *initiate\_session\_no\_contact* are analogously refined to two version for accepting and non-accepting RBCs.

Furthermore, a just established communication session with on-track equipment with an incompatible system version will be terminated immediately after receiving this information. This is modeled by the set *terminating\_session* which holds values of type entities. Only those communication sessions in this set can be closed by the termination event.

#### Implemented Requirements

- In case of a non-accepting RBC, all existing communication sessions with other RBCs must be terminated (cf. §3.5.3.5.2)
- After the system version is received by the OBU, the communication session is considered established and (cf. §3.5.3.8)
  - if the system version is compatible, the OBU shall send the session established message to track-side (cf. 3.5.3.8.a)
  - if the system version is incompatible, the OBU shall terminate the session (cf. 3.5.3.8.b)
- Any RBC which is contacted and with whom a communication session is established has a compatible system version (safety requirement from requirements document).

**REFINES** m2\_limit\_OBU

**SEES** c2\_system\_version\_mode

**VARIABLES**

*terminating\_sessions*

*accepting*

**INVARIANTS**

**inv2** :  $RBC \cap outgoing\_sessions \setminus terminating\_sessions \subseteq system\_version\_compatible$

**inv3** :  $accepting \subseteq RBC$

**inv4** :  $terminating\_sessions \subseteq on\_track$

**inv5** :  $((outgoing\_sessions \cup contacted \cup contacted\_by) \setminus (accepting \cup terminating\_sessions)) \cap RBC = \emptyset \vee$

$(\exists entity \cdot entity \in ((outgoing\_sessions \cup contacted \cup contacted\_by) \setminus (accepting \cup terminating\_sessions)) \cap RBC$

$\Rightarrow (\forall entity2 \cdot entity2 \in ((outgoing\_sessions \cup contacted \cup contacted\_by) \setminus terminating\_sessions) \cap RBC \wedge entity2 \neq entity \Rightarrow entity2 \in accepting)$

)

**EVENTS****Event** *receive\_information\_compatible*  $\hat{=}$ **extends** *outgoing\_communication***any***l\_partner***where***grd3* : *l\_partner*  $\in$  *contacted**grd4* : *l\_partner*  $\in$  *system\_version\_compatible***then***act1* : *outgoing\_sessions* := *outgoing\_sessions*  $\cup$  {*l\_partner*}*act2* : *contacted* := *contacted*  $\setminus$  {*l\_partner*}**end****Event** *receive\_information\_incompatible*  $\hat{=}$ **extends** *outgoing\_communication***any***l\_partner***where***grd3* : *l\_partner*  $\in$  *contacted**grd4* : *l\_partner*  $\notin$  *system\_version\_compatible***then***act1* : *outgoing\_sessions* := *outgoing\_sessions*  $\cup$  {*l\_partner*}*act2* : *contacted* := *contacted*  $\setminus$  {*l\_partner*}*act3* : *terminating\_sessions* := *terminating\_sessions*  $\cup$  {*l\_partner*}**end****Event** *receive\_contact\_order\_accept*  $\hat{=}$ **refines** *receive\_contact\_order***any***l\_partner***where***grd1* : *l\_partner*  $\notin$  *contacted*  $\cup$  *contacted\_by*  $\cup$  *incoming\_sessions*  $\cup$  *outgoing\_sessions**grd3* : *l\_partner*  $\in$  *RIU*  $\cup$  (*RBC*  $\cap$  *accepting*)**then***act1* : *contacted\_by* := *contacted\_by*  $\cup$  {*l\_partner*}**end****Event** *receive\_contact\_order\_non\_accept*  $\hat{=}$ **refines** *receive\_contact\_order***any***l\_partner***where***grd1* : *l\_partner*  $\notin$  *contacted*  $\cup$  *contacted\_by*  $\cup$  *incoming\_sessions*  $\cup$  *outgoing\_sessions**grd3* : *l\_partner*  $\in$  *RIU*  $\cup$  (*RBC*  $\setminus$  *accepting*)**then***act1* : *contacted\_by* := *contacted\_by*  $\cup$  {*l\_partner*}*act2* : *terminating\_sessions* := *terminating\_sessions*  $\cup$  (*RBC*  $\cap$  (*incoming\_sessions*  $\cup$  *outgoing\_sessions*))**end**



```

Event terminate_communication  $\widehat{=}$ 
extends terminate_communication
  any
    l_partner
  where
    grd1 : l_partner  $\in$  incoming_sessions  $\cup$  outgoing_sessions
    grd2 : l_partner  $\in$  terminating_sessions
  then
    act1 : incoming_sessions := incoming_sessions  $\setminus$  {l_partner}
    act2 : outgoing_sessions := outgoing_sessions  $\setminus$  {l_partner}
    act3 : terminating_sessions := terminating_sessions  $\setminus$  {l_partner}
  end
Event make_RBC_accepting  $\widehat{=}$ 
  any
    l_partner
  where
    grd1 : l_partner  $\in$  RBC
  then
    act1 : accepting := accepting  $\cup$  {l_partner}
  end
Event make_RBC_non_accepting  $\widehat{=}$ 
  any
    l_partner
  where
    grd1 : l_partner  $\in$  accepting
  then
    act1 : accepting := accepting  $\setminus$  {l_partner}
  end
END

```

#### 4.8 Context 3 - ERTMS Levels

The third context introduces the notion of the different ERTMS and the notion of the mission status of a train. The modeled statuses are start of mission (SOM), end of mission (EOM) and the abstract notion of within a mission (MIS), i.e., anything between start and end of the current train mission. At this level of refinement, a more detailed modeling is not necessary.

**CONTEXT** *c3\_ERTMS\_level*

**SETS**

*ERTMS\_level*

*train\_status*

**CONSTANTS**

*NTC*

*L0*

*L1*  
*L2*  
*L3*  
*SOM* start of mission  
*EOM* end of mission  
*MIS* while mission

#### AXIOMS

*axm1* : *partition(ERTMS\_level, {NTC, L0, L1, L2, L3})*  
*axm2* : *partition(train\_status, {SOM, EOM, MIS})*

#### END

### 4.9 Machine 4 - ERTMS Level Changes

The next refined machine implements the different causes which can trigger the establishing of a communication session. The corresponding events refine the abstract *initiate\_session\_no\_contact* events. For this, the current ERTMS level of the train is tracked, as well as its current mission status.

The indication of a level change, a mission status change, a manual level change and an announced radio hole is modeled by events. These events modify the corresponding indicator variables to signal a change and they modify the corresponding state variables.

This can be illustrated using the manual level change event as example: the Boolean variable *signal\_manual\_level\_change* indicates that the driver manually changed the ERTMS level. It is changed by the *manual\_change\_level* event which is parametrized with the new level and which also modifies the *current\_level* variable which models the current ERTMS level. If the new level is 2 or 3, then the train is required to establish a communication session with trackside. This is realized in the *initiate\_session\_no\_contact\_manual\_change* events which reset the indication variable once the entity has been contacted. Similar events model the initiation because of non-manual level change, mission status change and announced radio holes, each in a version for accepting and non-accepting RBCs.

#### Implemented Requirements

- The on-board shall establish a communication session (cf. §3.5.3.4)
  - at start of mission (only if level 2 or 3) (cf. §3.5.3.4.a)
  - if ordered from trackside (cf. §3.5.3.4.b)
  - If a mode change, not considered as an End of Mission, has to be reported to the RBC (only if level 2 or 3) (cf. §3.5.3.4.c)
  - If the driver has manually changed the level to 2 or 3 (cf. §3.5.3.4.d)
  - When the train front reaches the end of an announced radio hole (cf. §3.5.3.4.e)

**REFINES** m3\_accept\_system\_version

**SEES** c3\_ERTMS\_level

**VARIABLES**

*current\_level*  
*signal\_level\_change*  
*current\_status*  
*signal\_status\_change*  
*signal\_manual\_level\_change*  
*position\_radio\_hole*  
*signal\_radio\_hole*

## INVARIANTS

*inv1* : *current\_level*  $\in$  *ERTMS\_level*  
*inv2* : *signal\_level\_change*  $\in$  *BOOL*  
*inv3* : *current\_status*  $\in$  *train\_status*  
*inv4* : *signal\_status\_change*  $\in$  *BOOL*  
*inv5* : *signal\_manual\_level\_change*  $\in$  *BOOL*  
*inv6* : *position\_radio\_hole*  $\in$  *BOOL*  
*inv7* : *signal\_radio\_hole*  $\in$  *BOOL*

## EVENTS

**Event** *manual\_change\_level*  $\hat{=}$

**any**

**where** *l\_level*

*grd1* : *l\_level*  $\in$  *ERTMS\_level*  
*grd2* : *signal\_manual\_level\_change* = *FALSE*  
*grd3* : *signal\_level\_change* = *FALSE*

**then**

*act1* : *signal\_manual\_level\_change* := *TRUE*  
*act2* : *current\_level* := *l\_level*

**end**

**Event** *change\_level*  $\hat{=}$

**any**

**where** *l\_level*

*grd1* : *l\_level*  $\in$  *ERTMS\_level*  
*grd2* : *signal\_manual\_level\_change* = *FALSE*  
*grd3* : *signal\_level\_change* = *FALSE*

**then**

*act1* : *current\_level* := *l\_level*  
*act2* : *signal\_level\_change* := *TRUE*

**end**

**Event** *initiate\_session\_no\_contact\_accept*  $\hat{=}$

**extends** *initiate\_session\_no\_contact\_accept*

**any**

**where** *l\_partner*

*grd5* : *l\_partner*  $\notin$  *incoming\_sessions*  $\cup$  *outgoing\_sessions*  $\cup$  *contacted*  $\cup$  *contacted\_by*  
*grd3* : *l\_partner*  $\in$  *RIU*  $\cup$  (*RBC*  $\cap$  *accepting*)

```

    then
        act2 : contacted := contacted  $\cup$  {l_partner}
    end
Event initiate_session_no_contact_non_accept  $\hat{=}$ 
extends initiate_session_no_contact_non_accept
any
    l_partner
where
    grd5 : l_partner  $\notin$  incoming_sessions  $\cup$  outgoing_sessions  $\cup$  contacted  $\cup$  contacted_by
    grd3 : l_partner  $\in$  RIU  $\cup$  (RBC  $\setminus$  accepting)
then
    act2 : contacted := contacted  $\cup$  {l_partner}
    act3 : terminating_sessions := terminating_sessions  $\cup$  (RBC  $\cap$  (incoming_sessions  $\cup$ 
        outgoing_sessions))
end
Event initiate_session_no_contact_manual_change_accept  $\hat{=}$ 
extends initiate_session_no_contact_accept
any
    l_partner
where
    grd5 : l_partner  $\notin$  incoming_sessions  $\cup$  outgoing_sessions  $\cup$  contacted  $\cup$  contacted_by
    grd3 : l_partner  $\in$  RIU  $\cup$  (RBC  $\cap$  accepting)
    grd6 : current_level  $\in$  {L2, L3}
    grd7 : signal_manual_level_change = TRUE
then
    act2 : contacted := contacted  $\cup$  {l_partner}
    act3 : signal_manual_level_change := FALSE
end
Event initiate_session_no_contact_manual_change_non_accept  $\hat{=}$ 
refines initiate_session_no_contact_non_accept
any
    l_partner
where
    grd5 : l_partner  $\notin$  incoming_sessions  $\cup$  outgoing_sessions  $\cup$  contacted  $\cup$  contacted_by
    grd3 : l_partner  $\in$  RIU  $\cup$  (RBC  $\setminus$  accepting)
    grd6 : current_level  $\in$  {L2, L3}
    grd7 : signal_manual_level_change = TRUE
then
    act2 : contacted := contacted  $\cup$  {l_partner}
    act3 : terminating_sessions := terminating_sessions  $\cup$  (RBC  $\cap$  (incoming_sessions  $\cup$ 
        outgoing_sessions))
end
END

```

#### 4.10 Machine 5 - Safe Radio Connection

The next machine refinement specifies handling of the safe radio connection which provides the necessary means to exchange protocol messages on a higher level. The existing established safe radio connections are represented by the set *ER\_connections* which holds values of type entities. Safe radio connections which must be established are modeled by the set *establish\_ER\_connections* while *terminated\_ER\_connections* holds those connections which timed-out. The indication variable *signal\_RBC\_border* signals the crossing of an RBC border which requires to establish a new safe radio connection with a new RBC.

Establishing a communication session then works as follows: if one of the conditions of §3.5.3.4 is fulfilled, the corresponding partner is added to the set *contacted*. This is a precondition of the events which open a safe radio connection to a communication partner. The initiation message of the protocol is considered to be sent when a communication partner is both *contacted* and *ER\_connections* set. The reception of the system version and the sending of the system established message is modeled via the *receive\_information\_compatible* or *receive\_information\_incompatible* events. Established sessions with incompatible system versions are therefore in the intersection of the *sessions* and *terminating\_sessions* sets.

#### Implemented Requirements

- Establish communication session after safe radio connection timeout (cf. §3.5.3.4.f)
- If the communication session is established by an OBU, it shall be preformed according to the following steps (cf. §3.5.3.7)
  - if part of ongoing start of mission procedure (cf. §3.5.3.7.a)
  - if safe radio connection is set up (cf. §3.5.3.7.i)
  - if order to terminate is received (cf. §3.5.3.7.ii)
  - if end of mission is performed (cf. §3.5.3.7.iii)
  - train passes level transition border (cf. §3.5.3.7.iv)
  - order to establish connection with different non-accepting RBC (cf. §3.5.3.7.v)
  - train passes RBC / RBC border (cf. §3.5.3.7.vi)
  - train enters announced radio hole (cf. §3.5.3.7.vii)
  - level 1 is left (RIU only) (cf. §3.5.3.7.viii)
- When the RBC initiates the establishing of a communication session, the OBU shall consider the session established after receiving the initiation message (cf. §3.5.3.10.c)

**REFINES** m4\_level\_changes

**SEES** c3\_ERTMS\_level

**VARIABLES**

*ER\_connections*

*terminated\_ER\_connections*

*establish\_ER\_connection*

*signal\_RBC\_border*

**INVARIANTS**

$inv1 : terminated\_ER\_connections \subseteq on\_track$   
 $inv2 : establish\_ER\_connection \subseteq on\_track$   
 $inv3 : (incoming\_sessions \cup outgoing\_sessions) \subseteq ER\_connections$   
 $inv4 : signal\_RBC\_border \in BOOL$

## EVENTS

**Event** *incoming\_communication*  $\hat{=}$

**extends** *incoming\_communication*

**any**

**where**  $l\_partner$

$grd1 : l\_partner \notin incoming\_sessions \cup outgoing\_sessions$   
 $grd3 : l\_partner \in on\_track \setminus RIU$   
 $grd4 : l\_partner \notin contacted$   
 $grd5 : l\_partner \notin contacted\_by$   
 $grd6 : l\_partner \in ER\_connections$

**then**

$act1 : incoming\_sessions := incoming\_sessions \cup \{l\_partner\}$

**end**

**Event** *receive\_information\_compatible*  $\hat{=}$

**extends** *receive\_information\_compatible*

**any**

**where**  $l\_partner$

$grd3 : l\_partner \in contacted$   
 $grd4 : l\_partner \in system\_version\_compatible$   
 $grd5 : l\_partner \in ER\_connections$

**then**

$act1 : outgoing\_sessions := outgoing\_sessions \cup \{l\_partner\}$   
 $act2 : contacted := contacted \setminus \{l\_partner\}$

**end**

**Event** *receive\_information\_incompatible*  $\hat{=}$

**extends** *receive\_information\_incompatible*

**any**

**where**  $l\_partner$

$grd3 : l\_partner \in contacted$   
 $grd4 : l\_partner \notin system\_version\_compatible$   
 $grd5 : l\_partner \in ER\_connections$

**then**

$act1 : outgoing\_sessions := outgoing\_sessions \cup \{l\_partner\}$   
 $act2 : contacted := contacted \setminus \{l\_partner\}$   
 $act3 : terminating\_sessions := terminating\_sessions \cup \{l\_partner\}$

**end**

**Event** *receive\_contact\_order\_accept*  $\hat{=}$

order to contact a RIU or accepting RBC

**extends** *receive\_contact\_order\_accept*

```

any
    l_partner
where
    grd1 : l_partner  $\notin$  contacted  $\cup$  contacted_by  $\cup$  incoming_sessions  $\cup$  outgoing_sessions
    grd3 : l_partner  $\in$  RIU  $\cup$  (RBC  $\cap$  accepting)
    grd4 : l_partner  $\notin$  terminated_ER_connections
then
    act1 : contacted_by := contacted_by  $\cup$  {l_partner}
end
Event receive_contact_order_non_accept  $\widehat{=}$ 
extends receive_contact_order_non_accept
any
    l_partner
where
    grd1 : l_partner  $\notin$  contacted  $\cup$  contacted_by  $\cup$  incoming_sessions  $\cup$  outgoing_sessions
    grd3 : l_partner  $\in$  RIU  $\cup$  (RBC  $\setminus$  accepting)
    grd4 : l_partner  $\notin$  terminated_ER_connections
then
    act1 : contacted_by := contacted_by  $\cup$  {l_partner}
    act2 : terminating_sessions := terminating_sessions  $\cup$  (RBC  $\cap$  (incoming_sessions  $\cup$  outgoing_sessions))
end
Event initiate_session_after_contact_accept  $\widehat{=}$ 
    (cf. 3.5.3.4 b) / (cf. 3.5.3.5.2)
extends initiate_session_after_contact
any
    l_partner
where
    grd2 : l_partner  $\in$  contacted_by
    grd3 : l_partner  $\notin$  terminated_ER_connections
then
    act1 : contacted := contacted  $\cup$  {l_partner}
    act2 : contacted_by := contacted_by  $\setminus$  {l_partner}
    act3 : establish_ER_connection := establish_ER_connection  $\cup$  {l_partner}
end
Event initiate_session_no_contact_SOM_accept  $\widehat{=}$ 
    no contact order, i.e., one of the other
    cases of 3.5.3.4
extends initiate_session_no_contact_SOM_accept
any
    l_partner
where
    grd5 : l_partner  $\notin$  incoming_sessions  $\cup$  outgoing_sessions  $\cup$  contacted  $\cup$  contacted_by
    grd3 : l_partner  $\in$  RIU  $\cup$  (RBC  $\cap$  accepting)
    grd6 : current_status = SOM
    grd7 : current_level  $\in$  {L2, L3}
    grd8 : l_partner  $\notin$  terminated_ER_connections

```

```

then

    act2 : contacted := contacted  $\cup$  {l_partner}
    act3 : establish_ER_connection := establish_ER_connection  $\cup$  {l_partner}
end
Event initiate_session_no_contact_SOM_non_accept  $\hat{=}$ 
extends initiate_session_no_contact_SOM_non_accept
any

    l_partner
where

    grd5 : l_partner  $\notin$  incoming_sessions  $\cup$  outgoing_sessions  $\cup$  contacted  $\cup$  contacted_by
    grd3 : l_partner  $\in$  RIU  $\cup$  (RBC  $\setminus$  accepting)
    grd6 : current_status = SOM
    grd7 : current_level  $\in$  {L2, L3}
    grd8 : l_partner  $\notin$  terminated_ER_connections
then

    act2 : contacted := contacted  $\cup$  {l_partner}
    act3 : terminating_sessions := terminating_sessions  $\cup$  (RBC  $\cap$  (incoming_sessions  $\cup$ 
    outgoing_sessions))
    act4 : establish_ER_connection := establish_ER_connection  $\cup$  {l_partner}
end
Event initiate_session_no_contact_mode_change_accept  $\hat{=}$ 
extends initiate_session_no_contact_mode_change_accept
any

    l_partner
where

    grd5 : l_partner  $\notin$  incoming_sessions  $\cup$  outgoing_sessions  $\cup$  contacted  $\cup$  contacted_by
    grd3 : l_partner  $\in$  RIU  $\cup$  (RBC  $\cap$  accepting)
    grd6 : current_level  $\in$  {L2, L3}
    grd7 : signal_mode_change = TRUE
    grd8 : current_status  $\neq$  EOM
    grd9 : l_partner  $\notin$  terminated_ER_connections
then

    act2 : contacted := contacted  $\cup$  {l_partner}
    act3 : signal_mode_change := FALSE
    act4 : establish_ER_connection := establish_ER_connection  $\cup$  {l_partner}
end
Event initiate_session_no_contact_mode_change_non_accept  $\hat{=}$ 
extends initiate_session_no_contact_mode_change_non_accept
any

    l_partner
where

    grd5 : l_partner  $\notin$  incoming_sessions  $\cup$  outgoing_sessions  $\cup$  contacted  $\cup$  contacted_by
    grd3 : l_partner  $\in$  RIU  $\cup$  (RBC  $\setminus$  accepting)
    grd6 : current_level  $\in$  {L2, L3}
    grd7 : signal_mode_change = TRUE
    grd8 : current_status  $\neq$  EOM
    grd9 : l_partner  $\notin$  terminated_ER_connections
then

```



```

    act2 : contacted := contacted  $\cup$  {l_partner}
    act3 : terminating_sessions := terminating_sessions  $\cup$  (RBC  $\cap$  (incoming_sessions  $\cup$ 
    outgoing_sessions))
    act4 : establish_ER_connection := establish_ER_connection  $\cup$  {l_partner}
end
Event initiate_session_no_contact_manual_change_accept  $\hat{=}$ 
extends initiate_session_no_contact_manual_change_accept
any
    l_partner
where
    grd5 : l_partner  $\notin$  incoming_sessions  $\cup$  outgoing_sessions  $\cup$  contacted  $\cup$  contacted_by
    grd3 : l_partner  $\in$  RIU  $\cup$  (RBC  $\cap$  accepting)
    grd6 : current_level  $\in$  {L2, L3}
    grd7 : signal_manual_level_change = TRUE
    grd8 : l_partner  $\notin$  terminated_ER_connections
then
    act2 : contacted := contacted  $\cup$  {l_partner}
    act3 : signal_manual_level_change := FALSE
    act4 : establish_ER_connection := establish_ER_connection  $\cup$  {l_partner}
end
Event initiate_session_no_contact_manual_change_non_accept  $\hat{=}$ 
extends initiate_session_no_contact_manual_change_non_accept
any
    l_partner
where
    grd5 : l_partner  $\notin$  incoming_sessions  $\cup$  outgoing_sessions  $\cup$  contacted  $\cup$  contacted_by
    grd3 : l_partner  $\in$  RIU  $\cup$  (RBC  $\setminus$  accepting)
    grd6 : current_level  $\in$  {L2, L3}
    grd7 : signal_manual_level_change = TRUE
    grd8 : l_partner  $\notin$  terminated_ER_connections
then
    act2 : contacted := contacted  $\cup$  {l_partner}
    act3 : terminating_sessions := terminating_sessions  $\cup$  (RBC  $\cap$  (incoming_sessions  $\cup$ 
    outgoing_sessions))
    act4 : establish_ER_connection := establish_ER_connection  $\cup$  {l_partner}
end
Event initiate_session_no_contact_leave_radio_hole_accept  $\hat{=}$ 
extends initiate_session_no_contact_leave_radio_hole_accept
any
    l_partner
where
    grd5 : l_partner  $\notin$  incoming_sessions  $\cup$  outgoing_sessions  $\cup$  contacted  $\cup$  contacted_by
    grd3 : l_partner  $\in$  RIU  $\cup$  (RBC  $\cap$  accepting)
    grd6 : position_radio_hole = FALSE
    grd7 : signal_radio_hole = TRUE
    grd8 : l_partner  $\notin$  terminated_ER_connections
then
    act2 : contacted := contacted  $\cup$  {l_partner}

```

```

    act3 : signal_radio_hole := FALSE
    act4 : establish_ER_connection := establish_ER_connection  $\cup$  {l_partner}
end
Event initiate_session_no_contact_leave_radio_hole_non_accept  $\hat{=}$ 
extends initiate_session_no_contact_leave_radio_hole_non_accept
any
    l_partner
where
    grd5 : l_partner  $\notin$  incoming_sessions  $\cup$  outgoing_sessions  $\cup$  contacted  $\cup$  contacted_by
    grd3 : l_partner  $\in$  RIU  $\cup$  (RBC  $\setminus$  accepting)
    grd6 : position_radio_hole = FALSE
    grd7 : signal_radio_hole = TRUE
    grd8 : l_partner  $\notin$  terminated_ER_connections
then
    act2 : contacted := contacted  $\cup$  {l_partner}
    act3 : terminating_sessions := terminating_sessions  $\cup$  (RBC  $\cap$  (incoming_sessions  $\cup$ 
    outgoing_sessions))
    act4 : establish_ER_connection := establish_ER_connection  $\cup$  {l_partner}
end
Event initiate_session_after_timeout_accept  $\hat{=}$ 
extends initiate_session_no_contact_accept
any
    l_partner
where
    grd5 : l_partner  $\notin$  incoming_sessions  $\cup$  outgoing_sessions  $\cup$  contacted  $\cup$  contacted_by
    grd3 : l_partner  $\in$  RIU  $\cup$  (RBC  $\cap$  accepting)
    grd6 : l_partner  $\in$  terminated_ER_connections
then
    act2 : contacted := contacted  $\cup$  {l_partner}
    act3 : terminated_ER_connections := terminated_ER_connections  $\setminus$  {l_partner}
    act4 : establish_ER_connection := establish_ER_connection  $\cup$  {l_partner}
end
Event initiate_session_after_timeout_non_accept  $\hat{=}$ 
extends initiate_session_no_contact_non_accept
any
    l_partner
where
    grd5 : l_partner  $\notin$  incoming_sessions  $\cup$  outgoing_sessions  $\cup$  contacted  $\cup$  contacted_by
    grd3 : l_partner  $\in$  RIU  $\cup$  (RBC  $\setminus$  accepting)
    grd6 : l_partner  $\in$  terminated_ER_connections
then
    act2 : contacted := contacted  $\cup$  {l_partner}
    act3 : terminating_sessions := terminating_sessions  $\cup$  (RBC  $\cap$  (incoming_sessions  $\cup$ 
    outgoing_sessions))
    act4 : terminated_ER_connections := terminated_ER_connections  $\setminus$  {l_partner}
    act5 : establish_ER_connection := establish_ER_connection  $\cup$  {l_partner}
end
Event establish_ER_connection_SOM  $\hat{=}$ 

```

```

any
    l_partner
where
    grd1 : l_partner ∈ contacted
    grd2 : l_partner ∈ establish_ER_connection
    grd3 : current_status = SOM
then
    act1 : establish_ER_connection := establish_ER_connection \ {l_partner}
    act2 : ER_connections := ER_connections ∪ {l_partner}
end
Event establish_ER_connection ≡
any
    l_partner
where
    grd1 : l_partner ∈ contacted
    grd2 : l_partner ∈ establish_ER_connection
    grd3 : current_status ≠ SOM
then
    act1 : establish_ER_connection := establish_ER_connection \ {l_partner}
    act2 : ER_connections := ER_connections ∪ {l_partner}
end
Event est_perform_end_of_mission ≡
any
    l_partner
where
    grd1 : l_partner ∈ contacted
    grd2 : l_partner ∈ establish_ER_connection
    grd3 : signal_status_change = TRUE
    grd4 : current_status = EOM
then
    act1 : establish_ER_connection := establish_ER_connection \ {l_partner}
end
Event est_terminate_order ≡
extends drop_contact
any
    l_partner
where
    grd1 : l_partner ∈ contacted
    grd2 : l_partner ∈ establish_ER_connection
    grd3 : current_status ≠ SOM
then
    act1 : contacted := contacted \ {l_partner}
    act2 : establish_ER_connection := establish_ER_connection \ {l_partner}
end
Event est_pass_level_transition ≡
any

```

```

    l_partner
where

    grd1 : l_partner ∈ contacted
    grd2 : l_partner ∈ establish_ER_connection
    grd3 : signal_level_change = TRUE
    grd4 : current_status ≠ SOM
    grd5 : current_level ∈ {L0, L1, NTC}

then

    act1 : establish_ER_connection := establish_ER_connection \ {l_partner}

end

Event est_pass_radio_hole ≡

any

    l_partner
where

    grd1 : l_partner ∈ contacted
    grd2 : l_partner ∈ establish_ER_connection
    grd3 : signal_radio_hole = TRUE ∧ position_radio_hole = TRUE
    grd4 : current_status ≠ SOM

then

    act1 : establish_ER_connection := establish_ER_connection \ {l_partner}

end

Event est_RIU_leave_L1 ≡

any

    l_partner
where

    grd1 : l_partner ∈ contacted
    grd2 : l_partner ∈ RIU
    grd3 : signal_level_change = TRUE
    grd5 : current_level ≠ L1
    grd4 : current_status ≠ SOM

then

    act1 : establish_ER_connection := establish_ER_connection \ {l_partner}

end

Event est_RBC_border ≡

any

    l_partner
where

    grd1 : l_partner ∈ contacted
    grd2 : l_partner ∈ RBC
    grd3 : signal_RBC_border = TRUE
    grd4 : current_status ≠ SOM

then

    act1 : establish_ER_connection := establish_ER_connection \ {l_partner}

end

Event indicate_RBC_border ≡

any

```

```

    l_flag
  where
    grd1 : l_flag ∈ BOOL
  then
    act1 : signal_RBC_border := l_flag
  end
Event est_other_RBC_non_accept ≡
  any
    l_partner
  where
    grd1 : l_partner ∈ contacted
    grd2 : l_partner ∈ RBC
    grd3 : RBC ∩ accepting ∩ contacted_by ≠ ∅
    grd4 : current_status ≠ SOM
  then
    act1 : establish_ER_connection := establish_ER_connection \ {l_partner}
  end
Event timeout_ER_connection ≡
extends drop_session
  any
    l_partner
  where
    grd1 : l_partner ∈ incoming_sessions ∪ outgoing_sessions
    grd3 : l_partner ∈ ER_connections
  then
    act1 : incoming_sessions := incoming_sessions \ {l_partner}
    act2 : outgoing_sessions := outgoing_sessions \ {l_partner}
    act3 : ER_connections := ER_connections \ {l_partner}
    act4 : terminated_ER_connections := terminated_ER_connections ∪ {l_partner}
  end
Event terminate_communication ≡
extends terminate_communication
  any
    l_partner
  where
    grd1 : l_partner ∈ incoming_sessions ∪ outgoing_sessions
    grd2 : l_partner ∈ terminating_sessions
    grd3 : l_partner ∉ terminated_ER_connections
  then
    act1 : incoming_sessions := incoming_sessions \ {l_partner}
    act2 : outgoing_sessions := outgoing_sessions \ {l_partner}
    act3 : terminating_sessions := terminating_sessions \ {l_partner}
    act4 : ER_connections := ER_connections \ {l_partner}
  end
Event make_RBC_accepting ≡
extends make_RBC_accepting
  any

```

```

       $l\_partner$ 
where

       $grd1 : l\_partner \in RBC$ 
then

       $act1 : accepting := accepting \cup \{l\_partner\}$ 
end
Event  $make\_RBC\_non\_accepting \hat{=}$ 
extends  $make\_RBC\_non\_accepting$ 
any

       $l\_partner$ 
where

       $grd1 : l\_partner \in accepting$ 
then

       $act1 : accepting := accepting \setminus \{l\_partner\}$ 
end
END

```

## References

- [Abr10] Jean-Raymond Abrial. *Modeling in Event-B - System and Software Engineering*. Cambridge University Press, 2010.
- [Eur12] European Railway Agency (ERA). System Requirements Specification - ETCS Subset 026. <http://www.era.europa.eu/Document-Register/Documents/Index00426.zip>, 2012.
- [Jas12] Michael Jastram, editor. *Rodin User's Handbook*. DEPLOY Project, 2012.