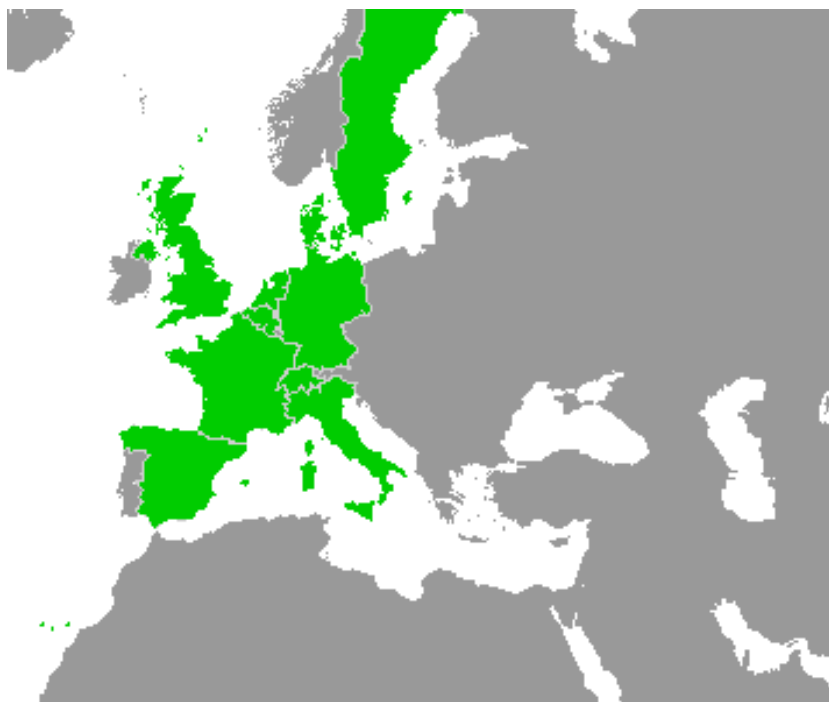


Work-Package 7: “Toolchain”

## Event-B Model of Subset 026, Section 5.9

Matthias Güdemann  
Systerel, France

April 2013



This page is intentionally left blank

**Work-Package 7: “Toolchain”**

**OETCS  
April 2013**

## Event-B Model of Subset 026, Section 5.9

Matthias GÜdemann  
Systerel, France  
Systerel

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	Short Introduction to Event-B .....	5
2	Modeling Strategy .....	5
3	Model Overview .....	6
4	Model Benefits .....	6
5	Detailed Model Description.....	7
5.1	Machine 0 - Basic Flowchart .....	7
5.2	Context 0 - Train Modes .....	8
5.3	Machine 1 - Train Modes .....	9
5.4	Context 1 - Mode Profiles .....	11
5.5	Machine 2 - Mode Profiles .....	12
5.6	Machine 3 - Driver Acknowledge .....	14
5.7	Machine 4 - Timeout.....	17
5.8	Machine 5 - Speed Supervision .....	18
	References .....	19

# Figures and Tables

## Figures

Figure 1. Overview on State Machine and Context Hierarchy .....	6
Figure 2. Flowchart for "On-Sight" Procedure [Eur12] .....	7
Figure 3. Basic Flowchart Representation .....	8
Figure 4. First Refinement with Train Modes .....	9
Figure 5. Second Refinement .....	13
Figure 6. Third Refinement with Driver Acknowledge .....	14
Figure 7. Fourth Refinement State Machine .....	17

## Tables

Table 1. Glossary .....	5
-------------------------	---

This document describes a formal model of the requirements of section 5.9 of the subset 026 of the ETCS specification 3.3.0 [Eur12]. This section describes the on-sight procedure.

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 procedure on-sight. We use the iUML plugin which allows for modeling in UML state-charts to create a graphical model of the procedure which is as close as possible as its description as flowchart in the section 5.9. The state machine is iteratively developed using the refinement feature of Event-B. At each refinement step, we present the reasoning for the step, together with newly introduced variables and events.

**Table 1. Glossary**

## **1 Short Introduction to Event-B**

The formal language Event-B is based on a set-theoretic approach. It is a variant of the B language, with a focus on system level modeling [Abr10]. An Event-B model is separated into a static and a dynamic part.

The dynamic part of an Event-B model describes abstract state machines. The state is represented by a set of state variables. A transition from one state to another is represented by parametrized events which assign new values to the state variables. Event-B allows unbounded state spaces. They are constrained by invariants expressed in first order logic with equality which must be fulfilled in any case. The initial state is created by a special initialization event.

The static part of an Event-B model is represented by contexts. These consist of carrier sets, constants and axioms. The type system of a model is described by means of carrier sets and constraints expressed by axioms.

Event-B is not only comprised of descriptions of abstract state machines and contexts, but also includes a development approach. This approach consists of iterative refinement of the machines until the desired level of detail is reached. In the Rodin tool, proof obligations are automatically created which ensure correct refinement.

Together with the machine invariants, the proof obligations for the refinement are formally proven, creating proof trees. To accomplish this, there are different options: many proof obligations can be discharged by automated provers (e.g., AtelierB, NewPP, Rodin's SMT-plugin), but as the underlying logic is in general undecidable, it is sometimes necessary to use the interactive proof support of Rodin.

Any external actions, e.g., mode changes by the driver or train level changes are modeled via parametrized events. Only events can modify the variables of a machine. An Event-B model is on the system level, events are assumed to be called from a software system into which the functional model is embedded. The guards of the events assure that any event can only be called when appropriate.

## 2 Modeling Strategy

The section 5.9 of the SRS describes the procedure on-sight, in particular it describes the sequence of mode changes, necessary driver acknowledge and train brake to enter OS mode, dependent on the current train mode.

For better understanding and to automate many tasks for state based modeling, we use the iUML plugin [?] which automatically generates Event-B code representing a state machine specification.

## 3 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.

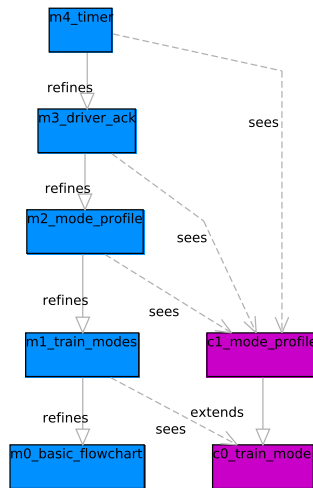


Figure 1. Overview on State Machine and Context Hierarchy

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 a more detailed description of the flowchart.

## 4 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.

- **Graphical Modeling** Through the iUML plugin, Rodin supports graphical modeling of UML/SysML state machines. Transitions are labeled with events and a fully automatic transformation [SBS09] creates an Event-B representation of the state machine models.



- **Refinement** In addition to the general refinement which is possible in the Event-B approach, the graphical modeling allows to refine the graphical state chart models too. For each refinement step, the new details are graphically emphasized.
- **Model Animation** Through the ProB plugin, the graphical models can be animated just as textual Event-B models. In this case active transitions can be highlighted which helps understand model behavior.
- **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 ??).

## 5 Detailed Model Description

This section describes in more detail the formal model, beginning from the most abstract Event-B machine. For each refinement, the state machine will be shown and in general only the important manual changes in the model generated from the state machine. The full generated code and the manual changes are 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.

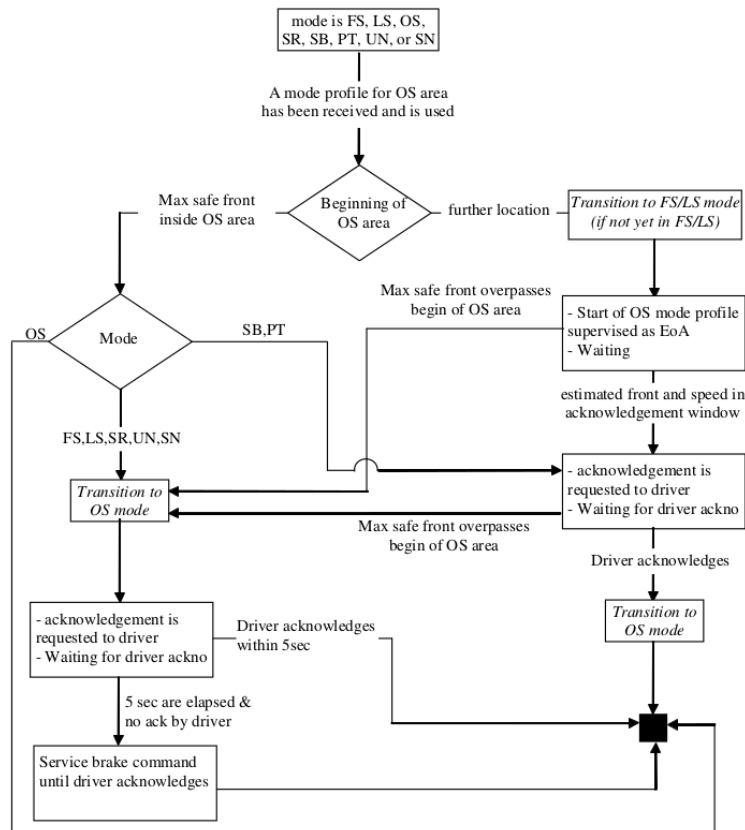
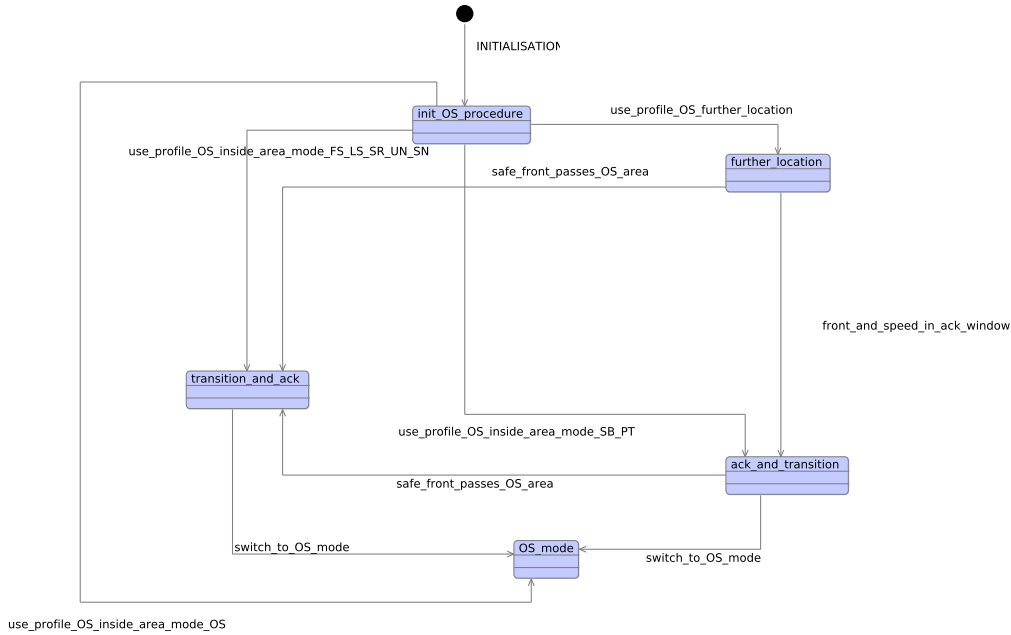


Figure 2. Flowchart for "On-Sight" Procedure [Eur12]

### 5.1 Machine 0 - Basic Flowchart

The first state machine  $m0$  (see Fig. 3) represents an abstract view of the flowchart describing the on-sight procedure which is shown in §5.9.7 of the SRS [Eur12] (see Fig. 2).



**Figure 3. Basic Flowchart Representation**

The flowchart is translated into a iUML state machine as follows: the initial state represents the initial situation of the procedure flowchart. The diamonds of the flowchart represent different cases and are therefore into transitions with different target states in the state chart. The nodes of the flowchart are combined for abstraction by combining nodes with multiple incoming flows (or an initial node) with direct successor nodes.

For example the state *ack\_and\_transition* can be reached from the initial state via the event *use\_profile\_OS\_inside\_area\_mode\_SB\_PT* and corresponds to the two lower right nodes of the flowchart. This is justified, as the flow passes two diamonds in the flowchart, verifying that the i) max safe front of the train is inside the OS area and ii) the train mode is *BS* or *PT*. The complete model is automatically generated from this state machine. Note however, that in this abstraction level, there is no concrete notion of train modes, these appear in the first refinement.

The transitions *switch\_to\_OS\_mode* signal the completion of the on-sight procedure, the internal switch to OS mode in the train happens elsewhere. The state *OS\_mode* signals the final state.

## 5.2 Context 0 - Train Modes

The first context *c0* specifies the possible modes of the train, these are of type *t\_train\_modes*. There is one Event-B constant for each possible mode. The constant *c\_initial\_mode* represents the initial mode of the train when the procedure on-sight is started. The constant *c\_supervision\_mode* is one mode from the supervision modes.

### SETS

*t\_train\_modes*

### CONSTANTS

- c\_FS* full supervision
- c\_LS* limited supervision
- c\_OS* on sight
- c\_SR* staff responsible

$c\_SB$  stand-by  
 $c\_PT$  post-trip  
 $c\_UN$  unfitted  
 $c\_SN$  national system  
 $c\_initial\_mode$   
 $c\_supervision\_mode$

#### AXIOMS

$axm1 : partition(t\_train\_modes, \{c\_FS\}, \{c\_LS\}, \{c\_OS\}, \{c\_SR\},$   
 $\{c\_SB\}, \{c\_PT\}, \{c\_UN\}, \{c\_SN\})$   
 $axm2 : c\_initial\_mode \in \{c\_FS, c\_OS, c\_PT\}$   
 $axm3 : c\_supervision\_mode \in \{c\_LS, c\_FS\}$

END

### 5.3 Machine 1 - Train Modes

The first machine refinement adds the variable *current\_mode* which tracks the current mode of the train. This variable is initialized with the value of  $c\_initial\_mode$ .

The state of this variable is used to constrain the guards of the events that depend on the train modes, i.e., corresponding to those that lead from the “Mode” diamond in the flowchart (see Fig. 2). Its state is changed in the *transition\_to\_supervision\_mode* event which assigns the value of  $c\_supervision\_mode$  or in the *transition\_to\_OS\_mode* event which assigns the on-sight mode.

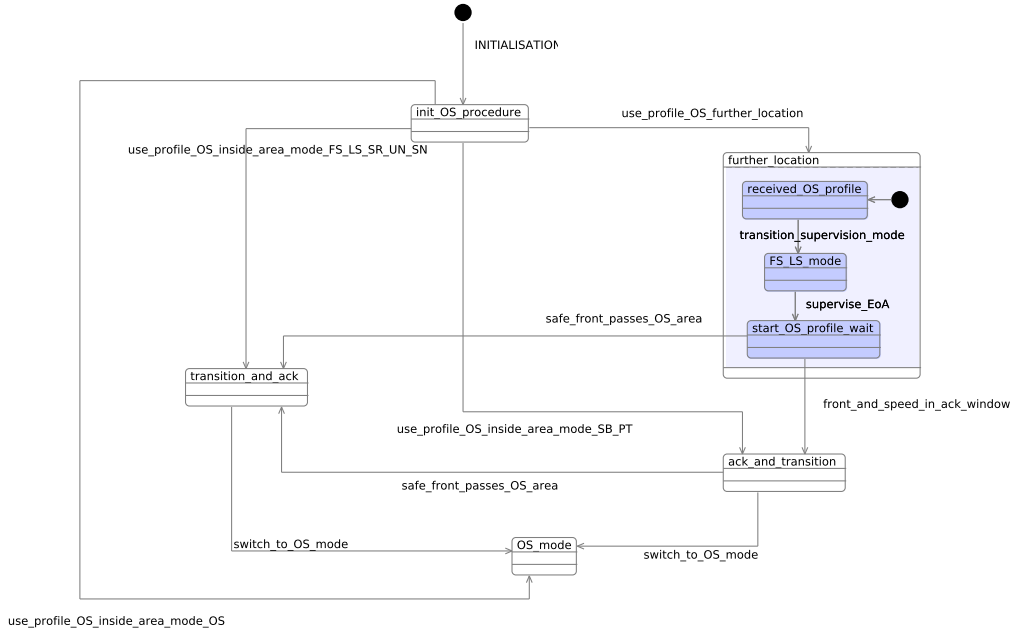


Figure 4. First Refinement with Train Modes

The refined state chart is shown in Fig. 4. The state *further\_location* is refined to contain three sub-states and two events. This switches the train to supervision mode, and starts EoA supervision. The train stays in this state until either the maximal safe front passes the OS area or the estimated front and speed leave the acknowledge window. The exiting transitions are changed to originate from the *start\_OS\_profile\_wait* state instead of its super-state. This is possible as the sub-states correctly refine the super-state.

**MACHINE** m1\_train\_modes

**REFINES** m0\_basic\_flowchart

**SEES** c0\_train\_mode

**VARIABLES**

*current\_mode*

**INVARIANTS**

*inv1* : *current\_mode* ∈ *t\_train\_modes*

**EVENTS**

**Event** *safe\_front\_passes\_OS\_area* ≡

**extends** *safe\_front\_passes\_OS\_area*

**when**

*isin\_ack\_and\_transition\_or\_isin\_further\_location* : *ack\_and\_transition* = TRUE ∨  
*further\_location* = TRUE

**then**

*isin\_start\_OS\_profile\_wait* : *start\_OS\_profile\_wait* = TRUE

*enter\_transition\_and\_ack* : *transition\_and\_ack* := TRUE

*leave\_ack\_and\_transition* : *ack\_and\_transition* := FALSE

*leave\_further\_location* : *further\_location* := FALSE

*leave\_start\_OS\_profile\_wait* : *start\_OS\_profile\_wait* := FALSE

**end**

**Event** *switch\_to\_OS\_mode* ≡

**extends** *switch\_to\_OS\_mode*

**when**

*isin\_ack\_and\_transition\_or\_isin\_transition\_and\_ack* : *ack\_and\_transition* = TRUE ∨  
*transition\_and\_ack* = TRUE

**then**

*leave\_ack\_and\_transition* : *ack\_and\_transition* := FALSE

*enter\_OS\_mode* : *OS\_mode* := TRUE

*leave\_transition\_and\_ack* : *transition\_and\_ack* := FALSE

**end**

**Event** *front\_and\_speed\_in\_ack\_window* ≡

**extends** *front\_and\_speed\_in\_ack\_window*

**when**

*isin\_further\_location* : *further\_location* = TRUE  
*isin\_start\_OS\_profile\_wait* : *start\_OS\_profile\_wait* = TRUE

**then**

*enter\_ack\_and\_transition* : *ack\_and\_transition* := TRUE

*leave\_further\_location* : *further\_location* := FALSE

*leave\_start\_OS\_profile\_wait* : *start\_OS\_profile\_wait* := FALSE

**end**

**Event** *use\_profile\_OS\_further\_location* ≡

**extends** *use\_profile\_OS\_further\_location*

**when**

*isin\_init\_OS\_procedure* : *init\_OS\_procedure* = TRUE

**then**

*leave\_init\_OS\_procedure* : *init\_OS\_procedure* := FALSE

*enter\_further\_location* : *further\_location* := TRUE

*enter\_received\_OS\_profile* : *received\_OS\_profile* := TRUE

**end**

**Event** *use\_profile\_OS\_inside\_area\_mode\_OS* ≡

**extends** *use\_profile\_OS\_inside\_area\_mode\_OS*

**when**

*isin\_init\_OS\_procedure* : *init\_OS\_procedure* = TRUE

**then**

*grd1* : *current\_mode* = *c\_OS*

*enter\_OS\_mode* : *OS\_mode* := TRUE

*leave\_init\_OS\_procedure* : *init\_OS\_procedure* := FALSE

```

    end
Event use_profile_OS_inside_area_mode_SB_PT ≡
extends use_profile_OS_inside_area_mode_SB_PT
    when
        isin_init_OS_procedure : init_OS_procedure = TRUE
        grd1 : current_mode ∈ {c_SB, c_PT}
    then
        enter_ack_and_transition : ack_and_transition := TRUE
        leave_init_OS_procedure : init_OS_procedure := FALSE
    end
Event use_profile_OS_inside_area_mode_FS_LS_SR_UN_SN ≡
extends use_profile_OS_inside_area_mode_FS_LS_SR_UN_SN
    when
        isin_init_OS_procedure : init_OS_procedure = TRUE
        grd1 : current_mode ∈ {c_FS, c_LS, c_SR, c_UN, c_SN}
    then
        leave_init_OS_procedure : init_OS_procedure := FALSE
        enter_transition_and_ack : transition_and_ack := TRUE
    end
Event transition_supervision_mode ≡
    when
        then
            isin_received_OS_profile : received_OS_profile = TRUE
            leave_received_OS_profile : received_OS_profile := FALSE
            act1 : current_mode := c_supervision_mode
            enter_FS_LS_mode : FS_LS_mode := TRUE
        end
Event transition_to_OS_mode ≡
    begin
        act1 : current_mode := c_OS
    end
END

```

## 5.4 Context 1 - Mode Profiles

This context extension introduces the type *t\_mode\_profile* for mode profiles, *t\_train\_fronts* for train fronts (e.g., max safe front, estimated front), *t\_speed* for train speed and *t\_locations* for on track locations.

The context also defines several functions, notably one which signals whether a mode profile specifies an OS area, one which signals whether a given train front overpasses the OS area for a specific mode profile, one that signals whether a train front and train speed are in the acknowledge window for a specific mode profile, one that signals whether a given train front is in the OS area of a given mode profile and finally a function that returns the EoA from a given profile.

```

CONTEXT c1_mode_profile
EXTENDS c0_train_mode
SETS

```

```

    t_mode_profile
    t_train_fronts
    t_speed
    t_locations

```

```

CONSTANTS

```

*f\_mode\_profile\_OS\_mode* indicates whether mode profile demands OS mode  
*f\_safe\_train\_front\_overpasses*  
*f\_estimated\_train\_front\_speed\_in\_window*  
*c\_profile0*  
*f\_safe\_front\_in\_OS\_area*  
*f\_EoA\_from\_profile*  
*c\_loc0*  
*c\_front0*

#### AXIOMS

**axm1** :  $f\_mode\_profile\_OS\_mode \in t\_mode\_profile \rightarrow BOOL$   
**axm2** :  $f\_safe\_train\_front\_overpasses \in t\_train\_fronts \times t\_mode\_profile \rightarrow BOOL$   
 train front overpasses begin OS area  
**axm3** :  $f\_estimated\_train\_front\_speed\_in\_window \in t\_train\_fronts \times t\_mode\_profile \times t\_speed \rightarrow BOOL$   
 est. train front and speed in ack window  
**axm4** :  $c\_profile0 \in t\_mode\_profile$   
**axm5** :  $f\_safe\_front\_in\_OS\_area \in t\_train\_fronts \times t\_mode\_profile \rightarrow BOOL$   
**axm6** :  $f\_EoA\_from\_profile \in t\_mode\_profile \rightarrow t\_locations$   
**axm7** :  $c\_loc0 \in t\_locations$   
**axm10** :  $c\_front0 \in t\_train\_fronts$

#### END

### 5.5 Machine 2 - Mode Profiles

The second refinement of the machine introduces the notion of mode profiles, train fronts (max safe and estimated) and the end of authority (EoA) location into the model. These are represented by the variables *EoA\_loc*, *mode\_profile\_OS*, *safe\_train\_front* and *estimated\_train\_front*.

The train fronts can be changed by the events *update\_estimated\_front* and *update\_safe\_front*. The current values of the fronts, the current mode profile and its corresponding EoA are used as parameters for the Boolean functions that guard the events, e.g., for the event *safe\_front\_passes\_OS\_area* or for the event *front\_and\_speed\_in\_ack\_window*.

The second refinement of the state machine is shown in Fig. 5. Here the state *transition\_and\_ack* is refined with two sub-states. The transition between the two new sub-states is *transition\_to\_OS\_mode* which sets the current train mode to on-sight.

**MACHINE** m2\_mode\_profile  
**REFINES** m1\_train\_modes  
**SEES** c1\_mode\_profile  
**VARIABLES**

*EoA\_loc*  
*mode\_profile\_OS*  
*safe\_train\_front*  
*estimated\_train\_front*

#### INVARIANTS

**inv1** :  $EoA\_loc \in t\_locations$   
**inv2** :  $mode\_profile\_OS \in t\_mode\_profile$   
**inv3** :  $safe\_train\_front \in t\_train\_fronts$   
**inv4** :  $estimated\_train\_front \in t\_train\_fronts$

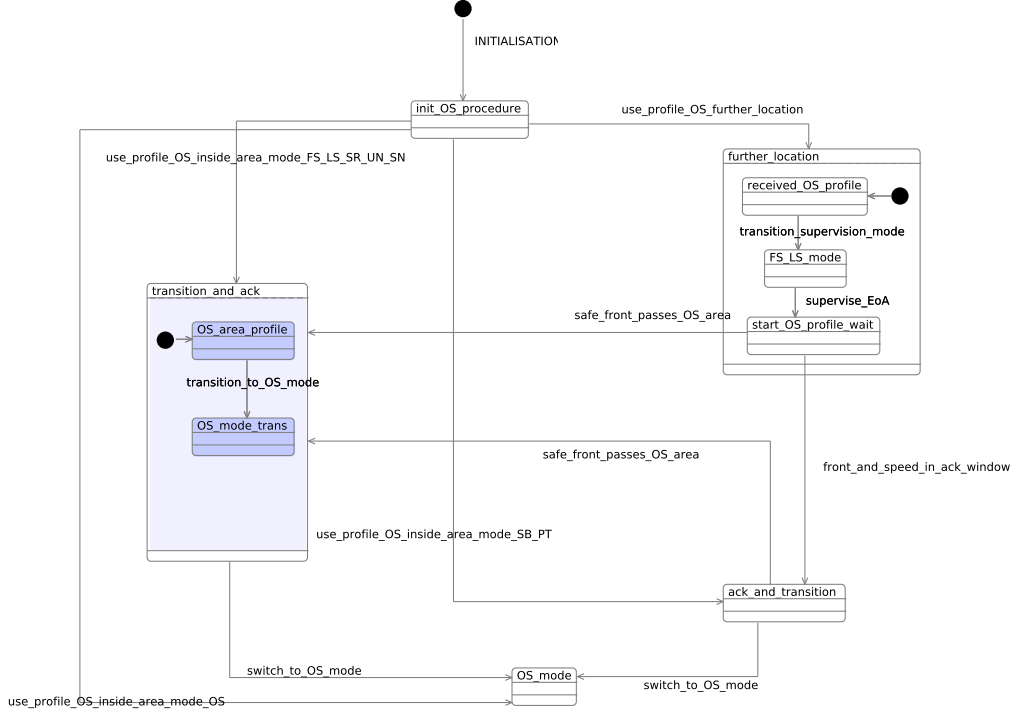


Figure 5. Second Refinement

**EVENTS**

**Event** *safe\_front\_passes\_OS\_area*  $\hat{=}$

**extends** *safe\_front\_passes\_OS\_area*

**where**

*isin\_ack\_and\_transition\_or\_isin\_further\_location* : *ack\_and\_transition* = TRUE  $\vee$

*further\_location* = TRUE

*isin\_start\_OS\_profile\_wait* : *start\_OS\_profile\_wait* = TRUE

*grd1* : *f\_safe\_train\_front\_overpasses*(*safe\_train\_front*  $\mapsto$  *mode\_profile\_OS*) = TRUE

*grd2* : *l\_safe\_train\_front*  $\in$  *t\_train\_fronts*

**then**

*enter\_transition\_and\_ack* : *transition\_and\_ack* := TRUE

*leave\_ack\_and\_transition* : *ack\_and\_transition* := FALSE

*leave\_further\_location* : *further\_location* := FALSE

*leave\_start\_OS\_profile\_wait* : *start\_OS\_profile\_wait* := FALSE

*enter\_OS\_area\_profile* : *OS\_area\_profile* := TRUE

**end**

**Event** *front\_and\_speed\_in\_ack\_window*  $\hat{=}$

**extends** *front\_and\_speed\_in\_ack\_window*

**any**

*l\_train\_speed*

**where**

*isin\_further\_location* : *further\_location* = TRUE

*isin\_start\_OS\_profile\_wait* : *start\_OS\_profile\_wait* = TRUE

*grd3* : *l\_train\_speed*  $\in$  *t\_speed*

*grd1* : *f\_estimated\_train\_front\_speed\_in\_window*(*estimated\_train\_front*  $\mapsto$  *mode\_profile\_OS*  $\mapsto$  *l\_train\_speed*) = TRUE

**then**

*enter\_ack\_and\_transition* : *ack\_and\_transition* := TRUE

*leave\_further\_location* : *further\_location* := FALSE

*leave\_start\_OS\_profile\_wait* : *start\_OS\_profile\_wait* := FALSE

**end**

**Event** *update\_estimated\_front*  $\hat{=}$

```

any
  where
    l_front
  where
    grd1 : l_front ∈ t_train_fronTs
  then
    act1 : estimated_train_front := l_front
  end
Event update_safe_front ≡
  any
    where
      l_front
    where
      grd1 : l_front ∈ t_train_fronTs
    then
      act1 : safe_train_front := l_front
    end
END

```

## 5.6 Machine 3 - Driver Acknowledge

The third machine refinement introduces the driver acknowledgment. In two cases, the driver is asked to acknowledge. This is modeled by additional Boolean variables, two for acknowledging OS mode and two for acknowledging the service brake. Each time, one variable signals that the driver has been informed that he has to acknowledge, e.g., for the service brake this is the *currently\_asking\_driver\_brake\_ack* variable, and to signal the completed acknowledge there is the *driver\_responded\_brake\_ack* variable. There is also the Boolean variable *service\_brake* which signals the active service brake of the train.

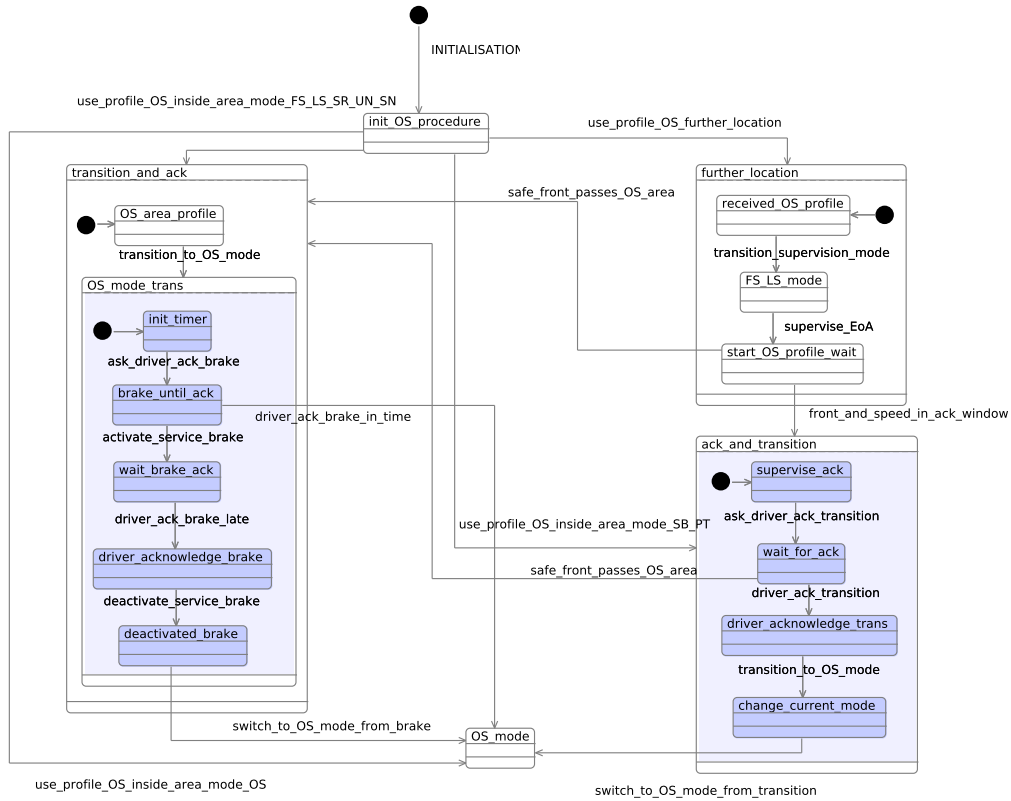


Figure 6. Third Refinement with Driver Acknowledge



The third refinement of the state machine is shown in Fig. 6. Here the two states *ack\_and\_transition* and *OS\_mode\_trans* are refined.

For *ack\_and\_transition* there are four new sub-states defined. There is first an event to ask the driver to acknowledge the switch to on-sight mode, then the OBU waits for the driver acknowledgment. If the max safe train front passes the OS area without driver acknowledge, then the *transition\_and\_ack* state is entered, else the train mode is switched to on-sight and the final state is entered. Here the outgoing transitions from the abstract *ack\_and\_transition* state are change to originate from *wait\_for\_ack* or *change\_current\_mode* respectively. Again this is possible as the sub-states correctly refine the abstract behavior of the super state.

The abstract *OS\_mode\_trans* state is refined by five sub-states. First the driver is asked to acknowledge the imminent service brake. If he does so in time, then the procedure finishes and the final state is entered, else the service brake is activated and stays activated until the driver acknowledges and the final state is entered.

At this refinement stage, it is possible to prove that whenever the final state is reached, the mode of the train is on-sight (*inv6*).

**MACHINE** m3\_driver\_ack  
**REFINES** m2\_mode\_profile  
**SEES** c1\_mode\_profile  
**VARIABLES**

*currently\_asking\_driver\_OS\_ack*  
*driver\_responded\_OS\_ack*  
*service\_brake\_active*  
*currently\_asking\_driver\_brake\_ack*  
*driver\_responded\_brake\_ack*

**INVARIANTS**

*inv6* : *OS\_mode* = *TRUE*  $\Rightarrow$  *current\_mode* = *c\_OS*

**EVENTS**

**Event** *ask\_driver\_ack\_brake*  $\hat{=}$

**when**

*isin\_init\_timer* : *init\_timer* = *TRUE*

*grd1* : *currently\_asking\_driver\_brake\_ack* = *FALSE*

**then**

*act1* : *currently\_asking\_driver\_brake\_ack* := *TRUE*

*enter\_brake\_until\_ack* : *brake\_until\_ack* := *TRUE*

*act2* : *driver\_responded\_brake\_ack* := *FALSE*

*leave\_init\_timer* : *init\_timer* := *FALSE*

**end**

**Event** *ask\_driver\_ack\_transition*  $\hat{=}$

**when**

*isin\_supervise\_ack* : *supervise\_ack* = *TRUE*

*grd1* : *currently\_asking\_driver\_OS\_ack* = *FALSE*

**then**

*act1* : *currently\_asking\_driver\_OS\_ack* := *TRUE*

*leave\_supervise\_ack* : *supervise\_ack* := *FALSE*

*enter\_wait\_for\_ack* : *wait\_for\_ack* := *TRUE*

*act2* : *driver\_responded\_OS\_ack* := *FALSE*

**end**

**Event** *driver\_ack\_brake\_in\_time*  $\hat{=}$

**extends** *switch\_to\_OS\_mode*

**when**

```

    isin_ack_and_transition_or_isin_transition_and_ack : ack_and_transition = TRUE ∨
    transition_and_ack = TRUE
    isin_brake_until_ack : brake_until_ack = TRUE
    grd1 : currently_asking_driver_brake_ack = TRUE
  then
    leave_ack_and_transition : ack_and_transition := FALSE
    enter_OS_mode : OS_mode := TRUE
    leave_transition_and_ack : transition_and_ack := FALSE
    leave_OS_mode_trans : OS_mode_trans := FALSE
    leave_OS_area_profile : OS_area_profile := FALSE
    act2 : driver_responded_brake_ack := TRUE
    leave_brake_until_ack : brake_until_ack := FALSE
    act1 : currently_asking_driver_brake_ack := FALSE
  end
Event driver_ack_brake_late ≡
  when
    grd1 : currently_asking_driver_brake_ack = TRUE
    isin_wait_brake_ack : wait_brake_ack = TRUE
  then
    act1 : currently_asking_driver_brake_ack := FALSE
    enter_driver_acknowledge_brake : driver_acknowledge_brake := TRUE
    act2 : driver_responded_brake_ack := TRUE
    leave_wait_brake_ack : wait_brake_ack := FALSE
  end
Event driver_ack_transition ≡
  when
    grd1 : currently_asking_driver_OS_ack = TRUE
    isin_wait_for_ack : wait_for_ack = TRUE
  then
    act2 : driver_responded_OS_ack := TRUE
    enter_driver_acknowledge_trans : driver_acknowledge_trans := TRUE
    leave_wait_for_ack : wait_for_ack := FALSE
    act1 : currently_asking_driver_OS_ack := FALSE
  end
Event activate_service_brake ≡
  when
    grd1 : service_brake_active = FALSE
    isin_brake_until_ack : brake_until_ack = TRUE
  then
    act1 : service_brake_active := TRUE
    leave_brake_until_ack : brake_until_ack := FALSE
    enter_wait_brake_ack : wait_brake_ack := TRUE
  end
Event deactivate_service_brake ≡
  when
    grd1 : service_brake_active = TRUE
    isin_driver_acknowledge_brake : driver_acknowledge_brake = TRUE
  then
    enter_deactivated_brake : deactivated_brake := TRUE
    act2 : service_brake_active := FALSE
    act3 : driver_responded_brake_ack := FALSE
    leave_driver_acknowledge_brake : driver_acknowledge_brake := FALSE
  end
END

```

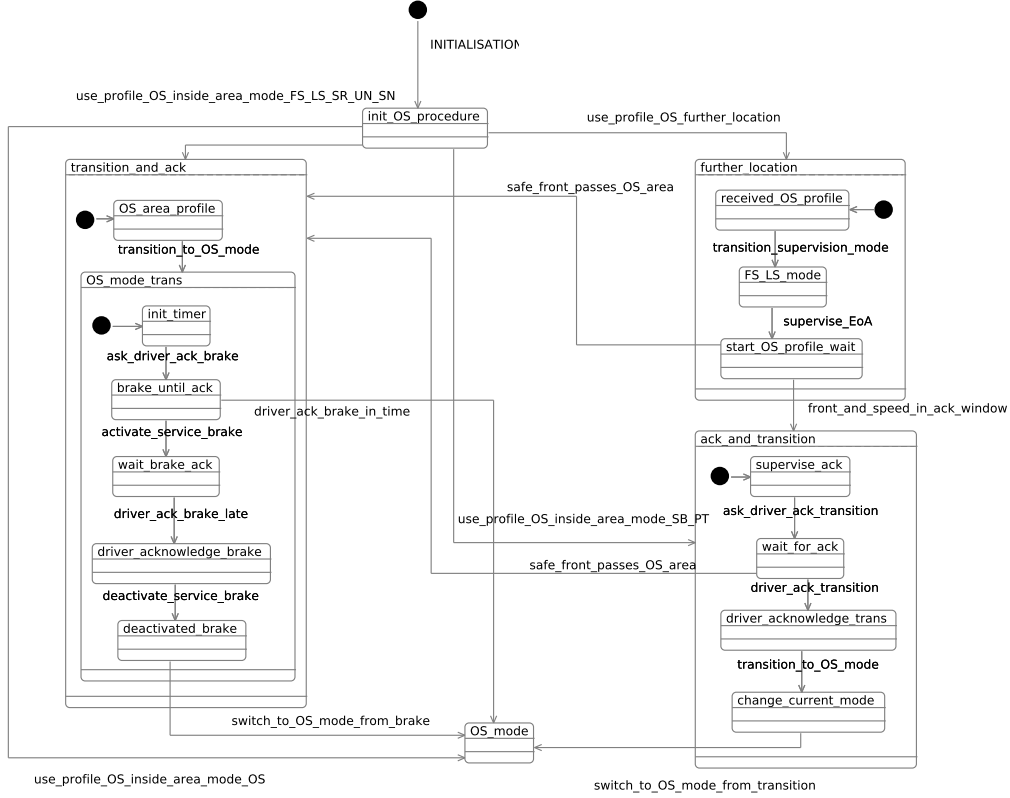


Figure 7. Fourth Refinement State Machine

## 5.7 Machine 4 - Timeout

**MACHINE** m4\_timeout

**REFINES** m3\_driver\_ack

**SEES** c1\_mode\_profile

**VARIABLES**

*timer\_expired*

**INVARIANTS**

**inv2** :  $timer\_expired = TRUE \wedge OS\_mode\_trans = TRUE \Rightarrow$   
 $\neg(ack\_and\_transition = TRUE \vee transition\_and\_ack = TRUE) \wedge$   
 $brake\_until\_ack = TRUE \wedge$   
 $currently\_asking\_driver\_brake\_ack = TRUE \wedge$   
 $timer\_expired = FALSE)$   
 PROPERTY\_5.9\_02, timer expired and in OS\_mode\_trans state disables  
 other transition than service brake

**EVENTS**

**Event** *driver\_ack\_brake\_in\_time*  $\hat{=}$

**extends** *driver\_ack\_brake\_in\_time*

**when**

**isin\_ack\_and\_transition\_or\_isin\_transition\_and\_ack** :  $ack\_and\_transition = TRUE \vee$   
 $transition\_and\_ack = TRUE$   
**isin\_brake\_until\_ack** :  $brake\_until\_ack = TRUE$   
**grd1** :  $currently\_asking\_driver\_brake\_ack = TRUE$   
**grd2** :  $timer\_expired = FALSE$

**then**

**leave\_ack\_and\_transition** :  $ack\_and\_transition := FALSE$   
**enter\_OS\_mode** :  $OS\_mode := TRUE$   
**leave\_transition\_and\_ack** :  $transition\_and\_ack := FALSE$   
**leave\_OS\_mode\_trans** :  $OS\_mode\_trans := FALSE$

```

    leave_OS_area_profile : OS_area_profile := FALSE
    act2 : driver_responded_brake_ack := TRUE
    leave_brake_until_ack : brake_until_ack := FALSE
    act1 : currently_asking_driver_brake_ack := FALSE
  end
Event driver_ack_brake_late ≡
extends driver_ack_brake_late
  when
    grd1 : currently_asking_driver_brake_ack = TRUE
    isin_wait_brake_ack : wait_brake_ack = TRUE
    grd2 : timer_expired = TRUE
  then
    act1 : currently_asking_driver_brake_ack := FALSE
    enter_driver_acknowledge_brake : driver_acknowledge_brake := TRUE
    act2 : driver_responded_brake_ack := TRUE
    leave_wait_brake_ack : wait_brake_ack := FALSE
  end
Event activate_service_brake ≡
extends activate_service_brake
  when
    grd1 : service_brake_active = FALSE
    isin_brake_until_ack : brake_until_ack = TRUE
    grd2 : timer_expired = TRUE
  then
    act1 : service_brake_active := TRUE
    leave_brake_until_ack : brake_until_ack := FALSE
    enter_wait_brake_ack : wait_brake_ack := TRUE
  end
Event expire_timer ≡
  when
    then
      grd1 : timer_expired = FALSE
    then
      act1 : timer_expired := TRUE
    end
END

```

## 5.8 Machine 5 - Speed Supervision

**MACHINE** m5\_speed\_supervision

**REFINES** m4\_timeout

**SEES** c2\_speed\_limit

**VARIABLES**

*current\_speed*

**INVARIANTS**

**inv1** :  $current\_speed \in t\_speed$

**inv2** :  $(driver\_acknowledge\_brake = TRUE \wedge$   
 $f\_speed\_exceeds(current\_speed \mapsto c\_OS\_speed\_limit) = TRUE \wedge$   
 $driver\_responded\_brake\_ack = TRUE) \Rightarrow$   
 $service\_brake\_active = TRUE$

PROPERTY\_5.9\_03 driver acknowledge does not deactivate  
 service brake if train speed exceeds OS speed limit

**inv10** :  $transition\_and\_ack = TRUE \Rightarrow$   
 $((f\_speed\_exceeds(current\_speed \mapsto c\_OS\_speed\_limit) = TRUE \wedge$   
 $current\_mode = c\_OS) \Rightarrow$   
 $service\_brake\_active = TRUE)$   
 PROPERTY\_5.9\_01, brake is activated if mode is OS and current speed exceeds limit

**EVENTS****Event** *deactivate\_service\_brake*  $\hat{=}$ **extends** *deactivate\_service\_brake***when***grd1* : *service\_brake\_active* = *TRUE**isin\_driver\_acknowledge\_brake* : *driver\_acknowledge\_brake* = *TRUE**grd2* : *f\_speed\_exceeds*(*current\_speed*  $\mapsto$  *c\_OS\_speed\_limit*) = *FALSE***then***enter\_deactivated\_brake* : *deactivated\_brake* := *TRUE**act2* : *service\_brake\_active* := *FALSE**act3* : *driver\_responded\_brake\_ack* := *FALSE**leave\_driver\_acknowledge\_brake* : *driver\_acknowledge\_brake* := *FALSE***end****Event** *update\_train\_speed\_brake*  $\hat{=}$ 

if brake is on new speed cannot exceed current speed

**any***l\_speed***where***grd1* : *l\_speed*  $\in$  *t\_speed**grd2* : *service\_brake\_active* = *TRUE**grd3* : *f\_speed\_exceeds*(*l\_speed*  $\mapsto$  *current\_speed*) = *FALSE**grd4* : *init\_OS\_procedure* = *TRUE*  $\vee$  *OS\_mode* = *TRUE***then***act1* : *current\_speed* := *l\_speed***end****Event** *update\_train\_speed\_no\_brake*  $\hat{=}$ **any***l\_speed***where***grd1* : *service\_brake\_active* = *FALSE**grd2* : *l\_speed*  $\in$  *t\_speed**grd3* : *driver\_acknowledge\_brake* = *FALSE**grd4* : *init\_OS\_procedure* = *TRUE*  $\vee$  *OS\_mode* = *TRUE***then***act1* : *current\_speed* := *l\_speed***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.
- [SBS09] Mar Yah Said, Michael Butler, and Colin Snook. Language and tool support for class and state machine refinement in uml-b. In *FM 2009: Formal Methods*, pages 579–595. Springer, 2009.