Event-B and Rodin

Matthias Güdemann

Systerel, Aix-en-Provence

April 15th, 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

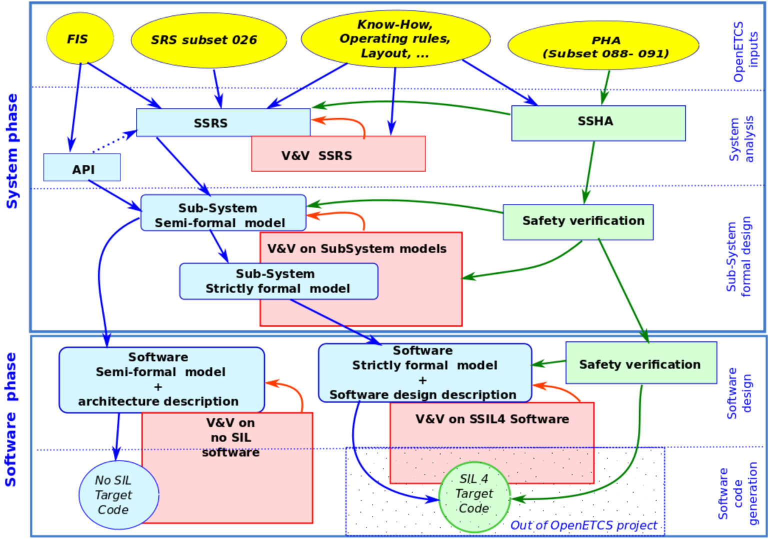
Event-B vs. B

B describes **how does it work ?**
Event-B describes **why does it work ?**

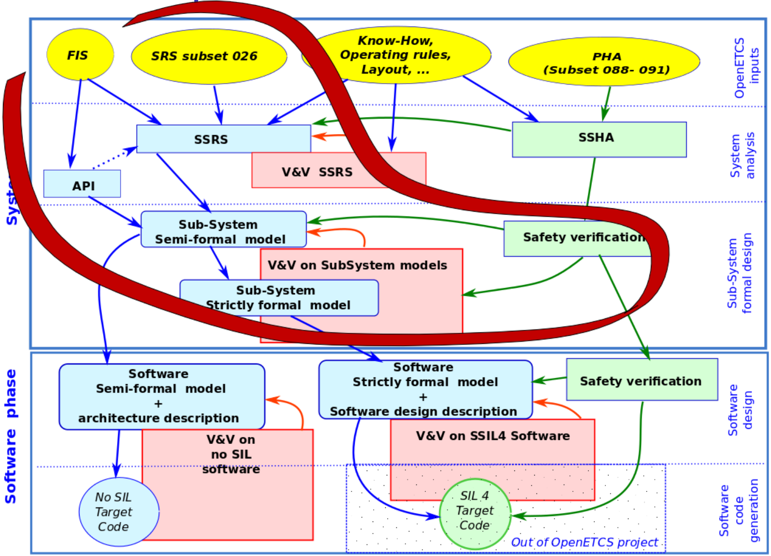
Overview

- Event-B in openETCS
- model-evaluation benchmark modeling
- Event-B Tool Rodin
- Benchmark results
- Conclusion

Event-B in openETCS



Event-B in openETCS



OpenETCS inputs

System analysis

Sub-System formal design

Software design

Software code generation

Syst

Software phase

FIS

SRS subset 026

Know-How, Operating rules, Layout, ...

PHA (Subset 088- 091)

SSRS

V&V SSRS

SSHA

API

Sub-System Semi-formal model

Safety verification

V&V on SubSystem models

Sub-System Strictly formal model

Software Semi-formal model + architecture description

Software Strictly formal model + Software design description

Safety verification

V&V on no SIL software

V&V on SSIL4 Software

No SIL Target Code

SIL 4 Target Code

Out of OpenETCS project

Benchmark Items Covered

- §3.5.3 Establishing a communication session (OBU)

  github - model/B-Systerel/Event_B/Subset_026_comm_session
- §3.13 Speed and distance monitoring (subset)

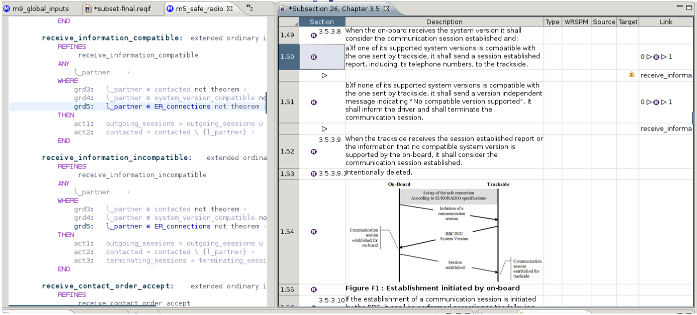
  github - model/B-Systerel/Event_B/Section_3_13
- §4.6.2 Transition Table (subset)

  github - model/B-Systerel/Event_B/Subset_026_Chap_4_6
- §5.9 Procedure On-Sight

  github - model/B-Systerel/Event_B/SubSet_026_5_9
- Using Rodin with github projects

  github - pdf documentation

§3.5.3 Establishing a communication session



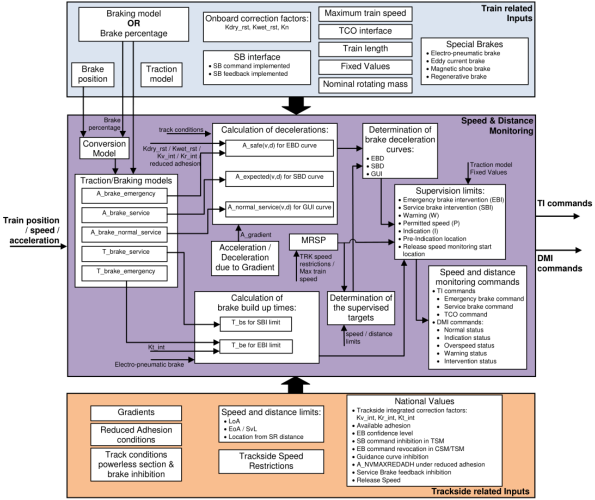
```
        END

    receive_information_compatible:  extended ordinary i
        REFINES
              receive_information_compatible
        ANY
            l_partner    ›
        WHERE
            grd3:   l_partner ∈ contacted not theorem ›
            grd4:   l_partner ∈ system_version_compatible no
            grd5:   l_partner ∈ ER_connections not theorem ›
        THEN
            act1:   outgoing_sessions ≔ outgoing_sessions ∪
            act2:   contacted ≔ contacted \ {l_partner} ›
        END

    receive_information_incompatible:   extended ordina
        REFINES
              receive_information_incompatible
        ANY
            l_partner    ›
        WHERE
            grd3:   l_partner ∈ contacted not theorem ›
            grd4:   l_partner ∉ system_version_compatible no
            grd5:   l_partner ∈ ER_connections not theorem ›
        THEN
            act1:   outgoing_sessions ≔ outgoing_sessions ∪
            act2:   contacted ≔ contacted \ {l_partner} ›
            act3:   terminating_sessions ≔ terminating_sessi
        END

    receive_contact_order_accept:   extended ordinary i
        REFINES
              receive_contact_order_accept
```

	Section	Description	Type	WRSPM	Source	Target	Link
1.49	R 3.5.3.8	When the on-board receives the system version it shall consider the communication session established and:					
1.50	R	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.					0 ▷ R ▷ 1
	▷					⚠	receive_informa
1.51	R	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.					0 ▷ R ▷ 1
	▷						receive_informa
1.52	R 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.					
1.53	R 3.5.3.9.1	Intentionally deleted.					
1.54	R						
1.55	R	**Figure F1 : Establishment initiated by on-board**					
	3.5.3.10	If the establishment of a communication session is initiated					

On-Board
Trackside
Set-up of the safe connection
According to EURORADIO specifications
Initiation of a communication session
RBC/RIU System Version
Communication session established for on-board
Session established
Communication session established for trackside

- **Proof** Connection to at most one non-accepting RBC
- **Proof** Active connections have compatible system version
- **Proof** RIUs do not initiate communication (non-testable)
- 116 of 118 POs automatic, typing, sound modeling. . .

§3.13 Speed and distance monitoring



Train related Inputs

Braking model
OR
Brake percentage

Brake position

Traction model

Onboard correction factors:
Kdry_rst, Kwet_rst, Kn

SB interface
- SB command implemented
- SB feedback implemented

Maximum train speed

TCO interface

Train length

Fixed Values

Nominal rotating mass

Special Brakes
- Electro-pneumatic brake
- Eddy current brake
- Magnetic shoe brake
- Regenerative brake

Speed & Distance Monitoring

Brake percentage

Conversion Model

track conditions

Kdry_rst / Kwet_rst / Kv_int / Kr_int / reduced adhesion

Calculation of decelerations:
A_safe(v,d) for EBD curve
A_expected(v,d) for SBD curve
A_normal_service(v,d) for GUI curve

Determination of brake deceleration curves:
- EBD
- SBD
- GUI

Traction model
Fixed Values

Traction/Braking models
A_brake_emergency
A_brake_service
A_brake_normal_service
T_brake_service
T_brake_emergency

A_gradient

Acceleration / Deceleration due to Gradient

MRSP

TRK speed restrictions / Max train speed

Supervision limits:
- Emergency brake intervention (EBI)
- Service brake intervention (SBI)
- Warning (W)
- Permitted speed (P)
- Indication (I)
- Pre-Indication location
- Release speed monitoring start location

Train position / speed / acceleration

TI commands

DMI commands

Calculation of brake build up times:
T_bs for SBI limit
T_be for EBI limit

Kt_int

Electro-pneumatic brake

Determination of the supervised targets

speed / distance limits

Speed and distance monitoring commands
- TI commands
  - Emergency brake command
  - Service brake command
  - TCO command
- DMI commands:
  - Normal status
  - Indication status
  - Overspeed status
  - Warning status
  - Intervention status

Gradients

Reduced Adhesion conditions

Track conditions powerless section & brake inhibition

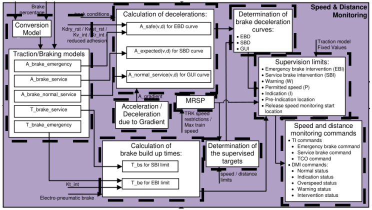
Speed and distance limits:
- LoA
- EoA / SvL
- Location from SR distance

Trackside Speed Restrictions

National Values
- Trackside integrated correction factors: Kv_int, Kr_int, Kt_int
- Available adhesion
- EB confidence level
- SB command inhibition in TSM
- EB command revocation in CSM/TSM
- Guidance curve inhibition
- A_NVMAXREDADH under reduced adhesion
- Service Brake feedback inhibition
- Release Speed

Trackside related Inputs

§3.13 Speed and distance monitoring



Speed & Distance Monitoring

Brake percentage

Conversion Model

track conditions

Kdry_rst / Kwet_rst / Kv_int / Kr_int / reduced adhesion

Traction/Braking models
- A_brake_emergency
- A_brake_service
- A_brake_normal_service
- T_brake_service
- T_brake_emergency

Calculation of decelerations:
- A_safe(v,d) for EBD curve
- A_expected(v,d) for SBD curve
- A_normal_service(v,d) for GUI curve

A_gradient

Acceleration / Deceleration due to Gradient

MRSP

TRK speed restrictions / Max train speed

Determination of brake deceleration curves:
- EBD
- SBD
- GUI

Traction model Fixed Values

Supervision limits:
- Emergency brake intervention (EBI)
- Service brake intervention (SBI)
- Warning (W)
- Permitted speed (P)
- Indication (I)
- Pre-Indication location
- Release speed monitoring start location

Calculation of brake build up times:
- T_bs for SBI limit
- T_be for EBI limit

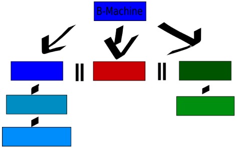
Kt_int

Electro-pneumatic brake

Determination of the supervised targets

speed / distance limits

Speed and distance monitoring commands
- TI commands
  - Emergency brake command
  - Service brake command
  - TCO command
- DMI commands:
  - Normal status
  - Indication status
  - Overspeed status
  - Warning status
  - Intervention status

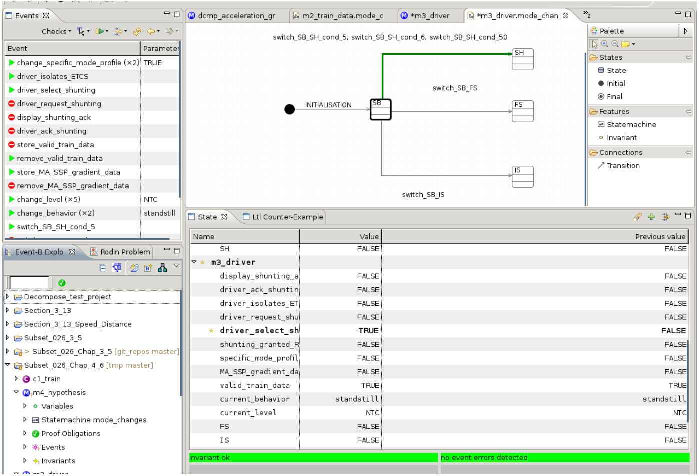


decomposition

refinement

- Model decomposition
- Decomposed Refinement up to functional level

§4.6.2 Transition table



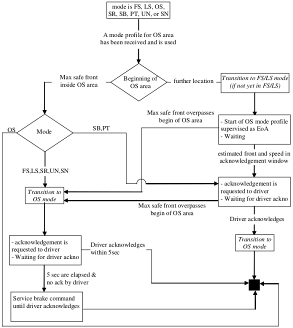
Event	Parameter
change_specific_mode_profile (×2)	TRUE
driver_isolates_ETCS	
driver_select_shunting	
driver_request_shunting	
display_shunting_ack	
driver_ack_shunting	
store_valid_train_data	
remove_valid_train_data	
store_MA_SSP_gradient_data	
remove_MA_SSP_gradient_data	
change_level (×5)	NTC
change_behavior (×2)	standstill
switch_SB_SH_cond_5	

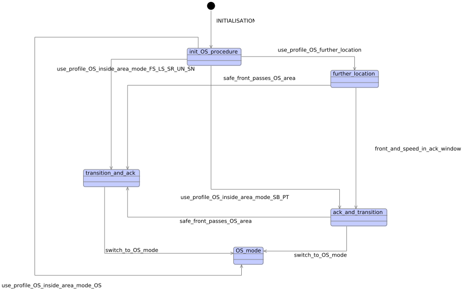
- Decompose_test_project
- Section_3_13
- Section_3_13_Speed_Distance
- Subset_026_3_5
- > Subset_026_Chap_3_5 [git_repos master]
- Subset_026_Chap_4_6 [tmp master]
  - c1_train
  - m4_hypothesis
    - Variables
    - Statemachine mode_changes
    - Proof Obligations
    - Events
    - Invariants

Name	Value	Previous value
SH	FALSE	FALSE
m3_driver		
display_shunting_a	FALSE	FALSE
driver_ack_shuntin	FALSE	FALSE
driver_isolates_ET	FALSE	FALSE
driver_request_shu	FALSE	FALSE
driver_select_sh	**TRUE**	**FALSE**
shunting_granted_R	FALSE	FALSE
specific_mode_profil	FALSE	FALSE
MA_SSP_gradient_da	FALSE	FALSE
valid_train_data	TRUE	TRUE
current_behavior	standstill	standstill
current_level	NTC	NTC
FS	FALSE	FALSE
IS	FALSE	FALSE

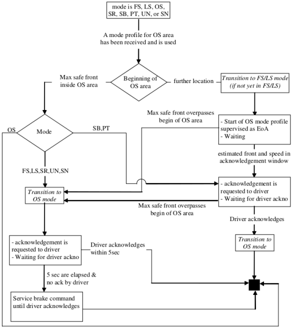
invariant ok
no event errors detected

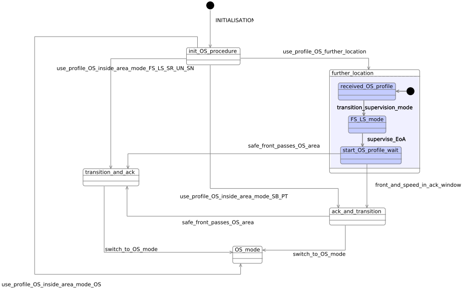
§5.9 Procedure on-sight


mode is FS, LS, OS, SR, SB, PT, UN, or SN
A mode profile for OS area has been received and is used
Beginning of OS area
Max safe front inside OS area
further location
Transition to FS/LS mode (if not yet in FS/LS)
Max safe front overpasses begin of OS area
- Start of OS mode profile supervised as EoA
- Waiting
OS
Mode
SB,PT
FS,LS,SR,UN,SN
estimated front and speed in acknowledgement window
Transition to OS mode
- acknowledgement is requested to driver
- Waiting for driver ackno
Max safe front overpasses begin of OS area
Driver acknowledges
Transition to OS mode
- acknowledgement is requested to driver
- Waiting for driver ackno
Driver acknowledges within 5sec
5 sec are elapsed & no ack by driver
Service brake command until driver acknowledges

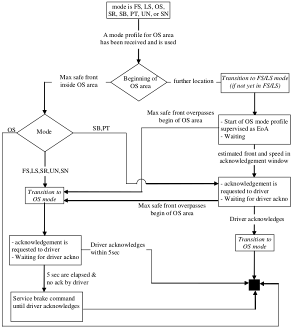

INITIALISATION
init_OS_procedure
use_profile_OS_further_location
use_profile_OS_inside_area_mode_FS_LS_SR_UN_SN
further_location
safe_front_passes_OS_area
front_and_speed_in_ack_window
transition_and_ack
use_profile_OS_inside_area_mode_SB_PT
ack_and_transition
safe_front_passes_OS_area
switch_to_OS_mode
OS_mode
switch_to_OS_mode
use_profile_OS_inside_area_mode_OS

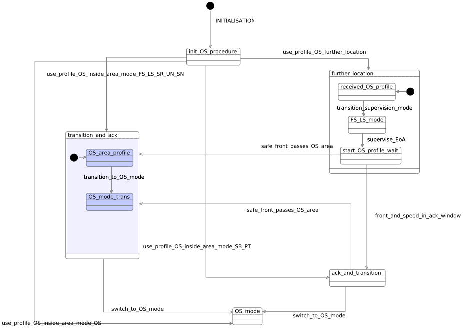
§5.9 Procedure on-sight


mode is FS, LS, OS, SR, SB, PT, UN, or SN
A mode profile for OS area has been received and is used
Beginning of OS area
Max safe front inside OS area
further location
Transition to FS/LS mode (if not yet in FS/LS)
Max safe front overpasses begin of OS area
- Start of OS mode profile supervised as EoA
- Waiting
OS
Mode
SB,PT
estimated front and speed in acknowledgement window
FS,LS,SR,UN,SN
- acknowledgement is requested to driver
- Waiting for driver ackno
Transition to OS mode
Max safe front overpasses begin of OS area
Driver acknowledges
- acknowledgement is requested to driver
- Waiting for driver ackno
Driver acknowledges within 5sec
Transition to OS mode
5 sec are elapsed & no ack by driver
Service brake command until driver acknowledges

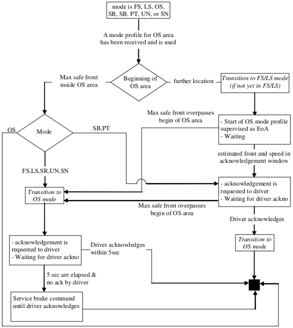

INITIALISATION
init_OS_procedure
use_profile_OS_further_location
use_profile_OS_inside_area_mode_FS_LS_SR_UN_SN
further_location
received_OS_profile
transition_supervision_mode
FS_LS_mode
supervise_EoA
safe_front_passes_OS_area
start_OS_profile_wait
transition_and_ack
front_and_speed_in_ack_window
use_profile_OS_inside_area_mode_SB_PT
ack_and_transition
safe_front_passes_OS_area
switch_to_OS_mode
OS_mode
switch_to_OS_mode
use_profile_OS_inside_area_mode_OS

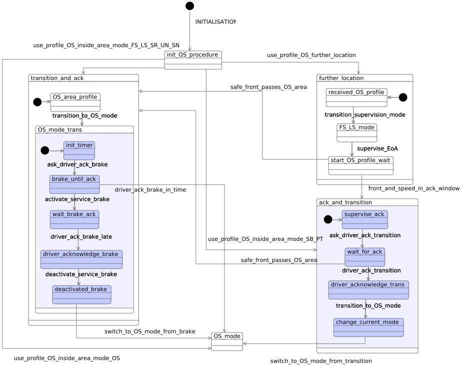
§5.9 Procedure on-sight


mode is FS, LS, OS, SR, SB, PT, UN, or SN
A mode profile for OS area has been received and is used
Beginning of OS area
further location
Max safe front inside OS area
Transition to FS/LS mode (if not yet in FS/LS)
Mode
OS
SB,PT
FS,LS,SR,UN,SN
Max safe front overpasses begin of OS area
- Start of OS mode profile supervised as EoA
- Waiting
estimated front and speed in acknowledgement window
- acknowledgement is requested to driver
- Waiting for driver ackno
Transition to OS mode
Max safe front overpasses begin of OS area
Driver acknowledges
Transition to OS mode
- acknowledgement is requested to driver
- Waiting for driver ackno
Driver acknowledges within 5sec
5 sec are elapsed & no ack by driver
Service brake command until driver acknowledges


INITIALISATION
init_OS_procedure
use_profile_OS_further_location
use_profile_OS_inside_area_mode_FS_LS_SR_UN_SN
further_location
received_OS_profile
transition_supervision_mode
FS_LS_mode
supervise_EoA
start_OS_profile_wait
safe_front_passes_OS_area
transition_and_ack
OS_area_profile
transition_to_OS_mode
OS_mode_trans
safe_front_passes_OS_area
front_and_speed_in_ack_window
use_profile_OS_inside_area_mode_SB_PT
ack_and_transition
switch_to_OS_mode
OS_mode
switch_to_OS_mode
use_profile_OS_inside_area_mode_OS

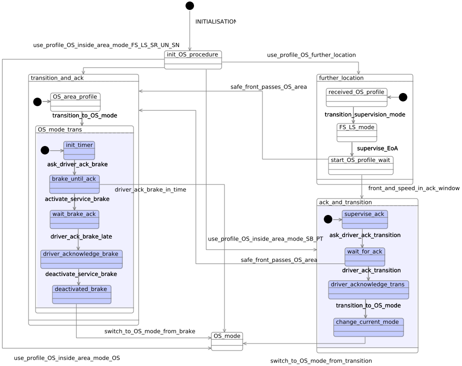
§5.9 Procedure on-sight


mode is FS, LS, OS, SR, SB, PT, UN, or SN
A mode profile for OS area has been received and is used
Max safe front inside OS area
Beginning of OS area
further location
Transition to FS/LS mode (if not yet in FS/LS)
Max safe front overpasses begin of OS area
OS
Mode
SB,PT
- Start of OS mode profile supervised as EoA
- Waiting
estimated front and speed in acknowledgement window
FS,LS,SR,UN,SN
Transition to OS mode
- acknowledgement is requested to driver
- Waiting for driver ackno
Max safe front overpasses begin of OS area
Driver acknowledges
- acknowledgement is requested to driver
- Waiting for driver ackno
Driver acknowledges within 5sec
Transition to OS mode
5 sec are elapsed & no ack by driver
Service brake command until driver acknowledges



§5.9 Procedure on-sight

- **Proof** Brake triggered when too fast in OS mode
- **Proof** Brake triggered if ack timeout.
- **Proof** OS ack does not release speed supervision brake.
- all 230 POs fully automatic



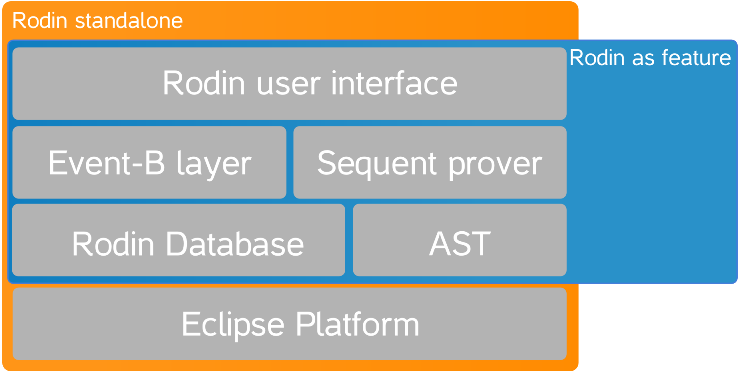
Missing elements / ongoing work

- Well-structured input documents
  - Similar level of abstraction in requirements
  - Explicit definition of global data
  - abstract architecture
  - high level safety requirements
- Semi-Formal graphical illustrations
  - Flowcharts, data-flow diagrams, statecharts
  - very helpful when modeling
  - requirements linking more difficult

Tools

- Rodin well applicable in openETCS
  - Available under EPL
  - B approach well established in railway (explicit in CENELEC)
  - Event-B already in use / ongoing development (ADVANCE EU project)
  - All tool documentation available
- Well integrated into Eclipse
  - EMF model
  - Proven interaction with various plug-ins

Tools


Rodin standalone
Rodin as feature
Rodin user interface
Event-B layer
Sequent prover
Rodin Database
AST
Eclipse Platform

Results of benchmark

- Pros
  - Abstraction through refinement
  - Graphical modeling (connection to semi-formal approaches)
  - Validation by model animation (ProB, AnimB)
  - Excellent proof support (manual and automatic)
  - Open Environment (extensible, e.g., for VnV tools)
  - Collaboration tools (EGit, Teamwork)
- Cons
  - Currently limited support for floats and non-linear arithmetic
  - Not well-suited for algorithms (i.e., braking curves)

Conclusion

- **refinement-based** modeling approach
- **extensible** platform, many existing plug-ins
- **formal proof** automated provers, proof assistant

More Information

Event-B / Rodin Wiki Page

Rodin Information Flyer