ERTMS Solutions

ERTMSFormalSpecs (EFS)

A domain specific language to formalize ERTMS specifications for onboard unit development

Stanislas Pinte

Laurent Ferier

Svitlana Lukicheva

ERTMS SOLUTIONS

ERTMSFormalSpecs

ERTMS Specifications

100% ERTMS Business Logic
Formal Language

CASE tool

Simulink

Ada *B* *C*

SCADE SUITE

artisan
your model for success

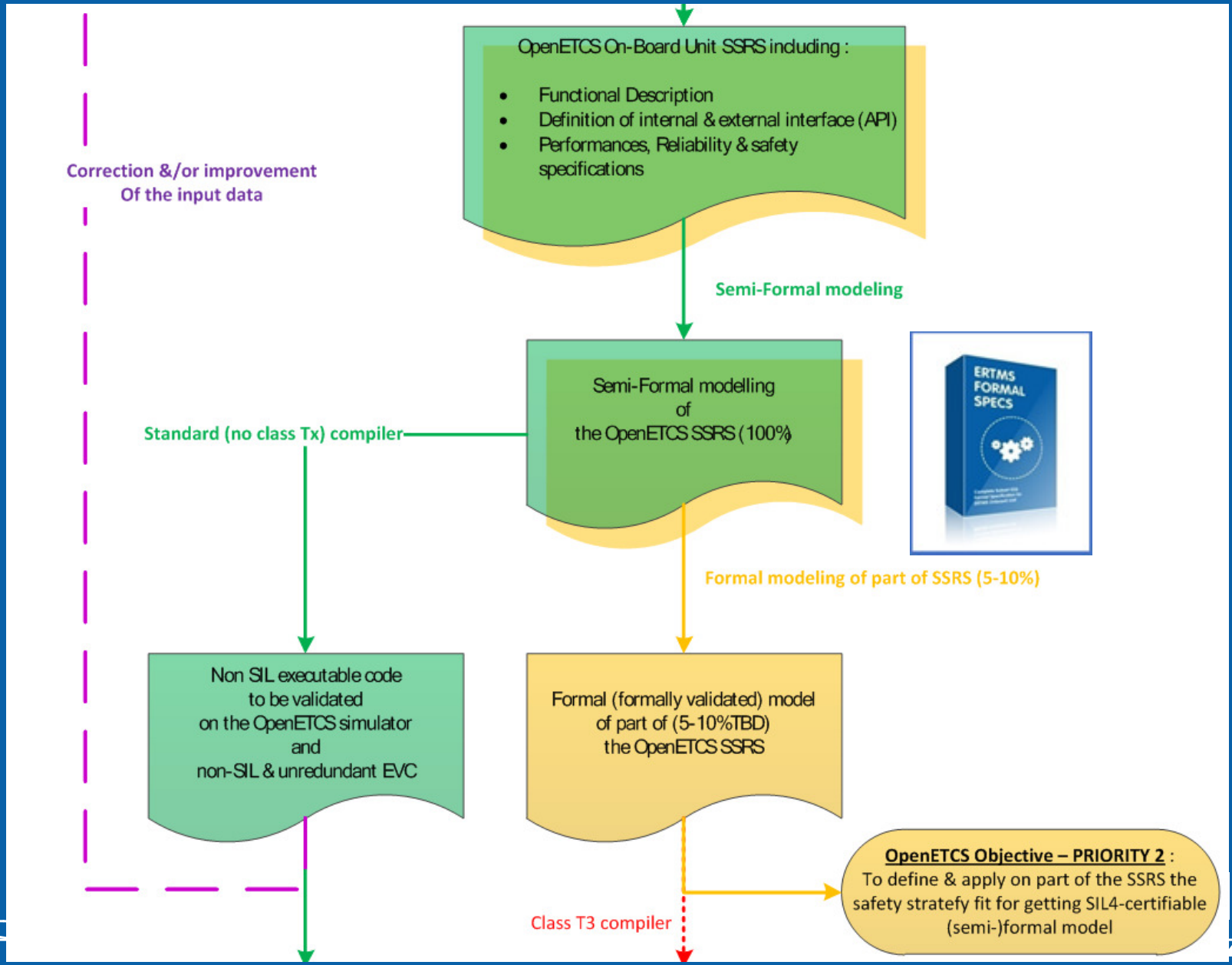
SILA Interpreter

Test tools

Target

ERTMS SOLUTIONS

Use in the OpenETCS process



Benchmark report

Paragraph id	Requirement	Implemented	Percentage	Total	Total percentage	Comment
§3.5.3	Establishing a communication session	11	21,4	26	0,78	
§3.13.4	Acceleration / Deceleration due to gradients	6	100	6	0,18	
§3.13.6.2	Emergency brake and more particularly	23	100	23	0,69	
§3.13.6.2.1.3	Calculation of A_safe	1	100	1	0,03	
§3.13.7	Determination of Most Restrictive Speed Profile	2	100	2	0,06	
§3.13.8.3	Emergency Brake Deceleration curves	3	100	3	0,09	
§3.13.9.3.3.9	Computation of d_FLOI	1	100	1	0,03	
§3.13.9.4	Release speed supervision limits and more particularly	13	92,9	14	0,42	*Not implemented: recalculation of t*
§3.13.9.4.7	Computation of different release speed supervision limits	1	100	1	0,03	
§3.13.9.4.8	Computation of the most restrictive value amongst several EBI	5	83,33	6	0,18	*Not implemented: recalculation of t*
§3.13.9.4.8.2	Iterative computation of the release speed	1	50	1	0,03	*Not implemented: recalculation of t*
§3.13.9.4.9	Using the most restrictive MRSP value instead of the release sp	1	100	1	0,03	
§3.13.10.4.2	Calculation of the MRDT	1	50	2	0,06	*Not implemented: calculations depe*
§4.6.2 & §4.6.3	from SB to SH	3	100	3	0,09	
	from SB to FS	1	100	1	0,03	
	from SB to IS	1	100	1	0,03	
§5.9	Procedure On-Sight	26	100	26	0,78	
§3.6.3.2	Location, Continuous Profile Data and Non-Continuous Profile	0	0	8	0,24	*All the implemented profile data pr*
§3.8.3	Structure of Movement Authority	12	92,3	13	0,39	*Not implemented: not handling of t*
§3.8.5	Update of Movement Authority	10	100	10	0,3	
§3.11.3	Static Speed Profile	10	100	10	0,3	
§3.11.12	Gradients	6	100	6	0,18	
§4.8.3.2	From National System X (through STM interface)	0	0	2	0,06	
§8.7.2	Movement Authority message	1	100	1	0,03	*All the messages and packets are in*
		139	76,53	168	5,04	

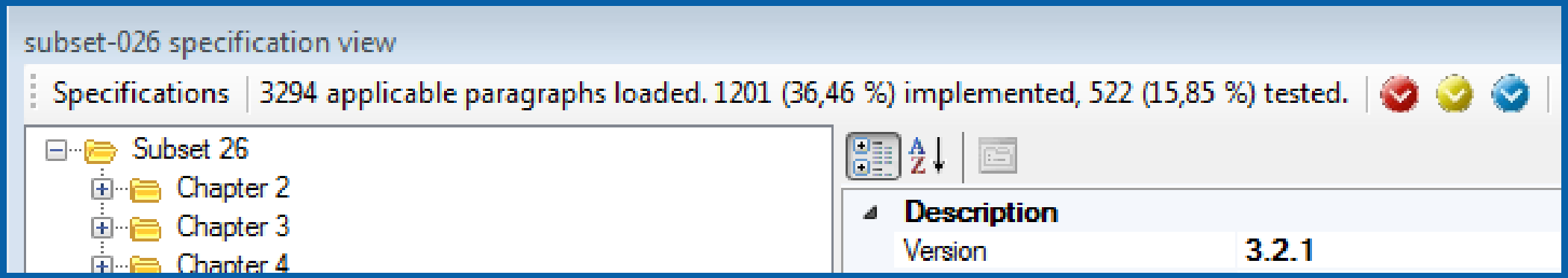
Benchmark report

Benchmark

5,04%

ERTMSFormalSpecs

36,46%



ERTMS SOLUTIONS

Benchmark report

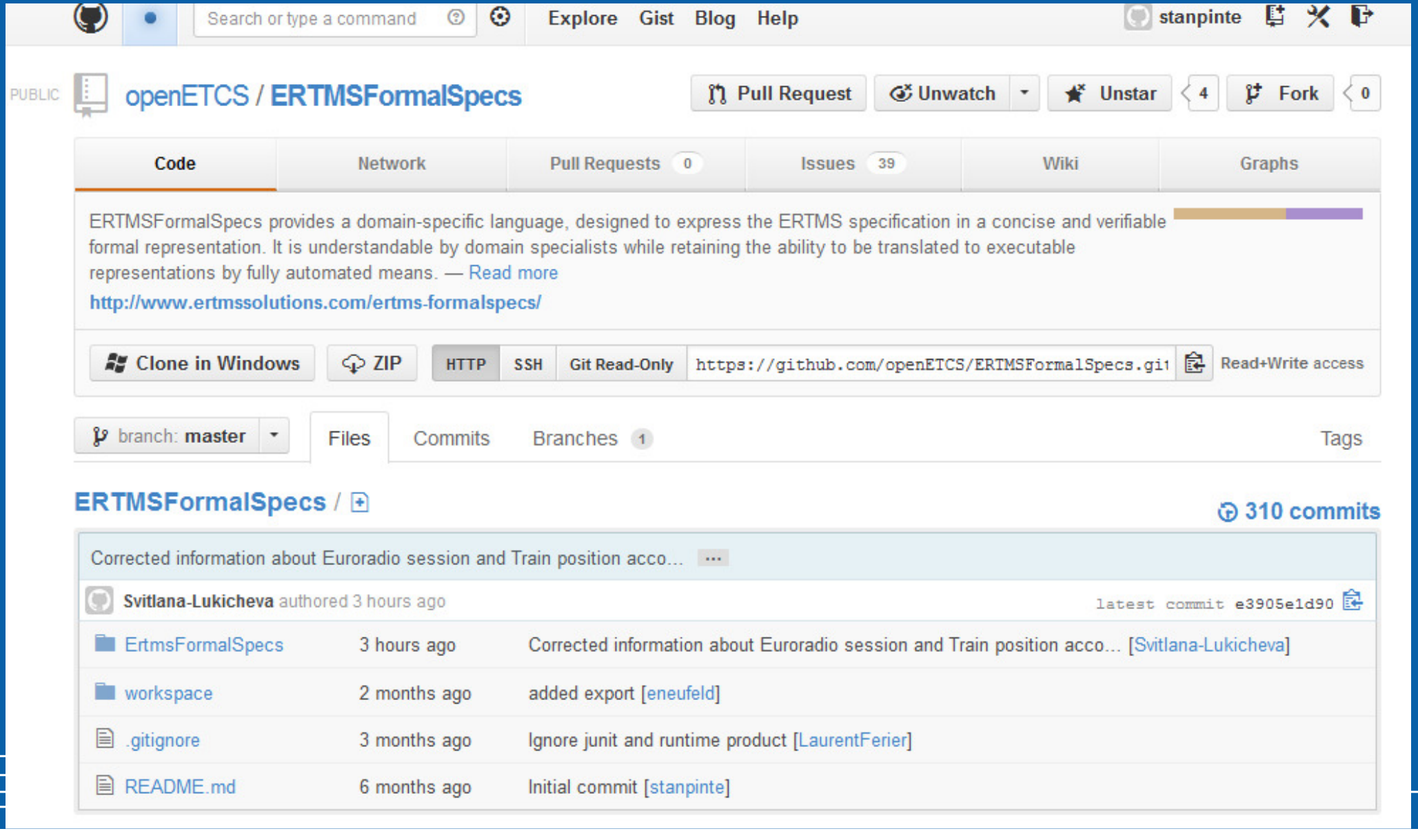
	Author	A
Consistency to SSRS (D.2.6-X-12.2)	☑	
Coverage of SSRS (D.2.6-X-12.2.1)	☑	
Traceability to SSRS (D.2.6-X-12.3)	☑	
Simulation or animation (D.2.6-X-13 partial)	☑	
Execution (D.2.6-X-13 partial)	☑	
Extensible to strictly formal model (D.2.6-X-14.3)	☑	
Easy to refine towards strictly formal model (D.2.6-X-14.4)	☑	
Extensible and modular design (D.2.6-X-15)	☑	
Extensible to software design (???)	☑	

Means / language

Does the language allow to formalize (D.2.6-X-29):

	Author	Assessor 1	Assessor 2	Total
State machines	☑			
Time-outs	☑			
Truth tables	☑			
Arithmetic	☑			
Braking curves	☑			
Logical statements	☑			
Message and fields	☑			

ERTMSFormalSpecs is open source

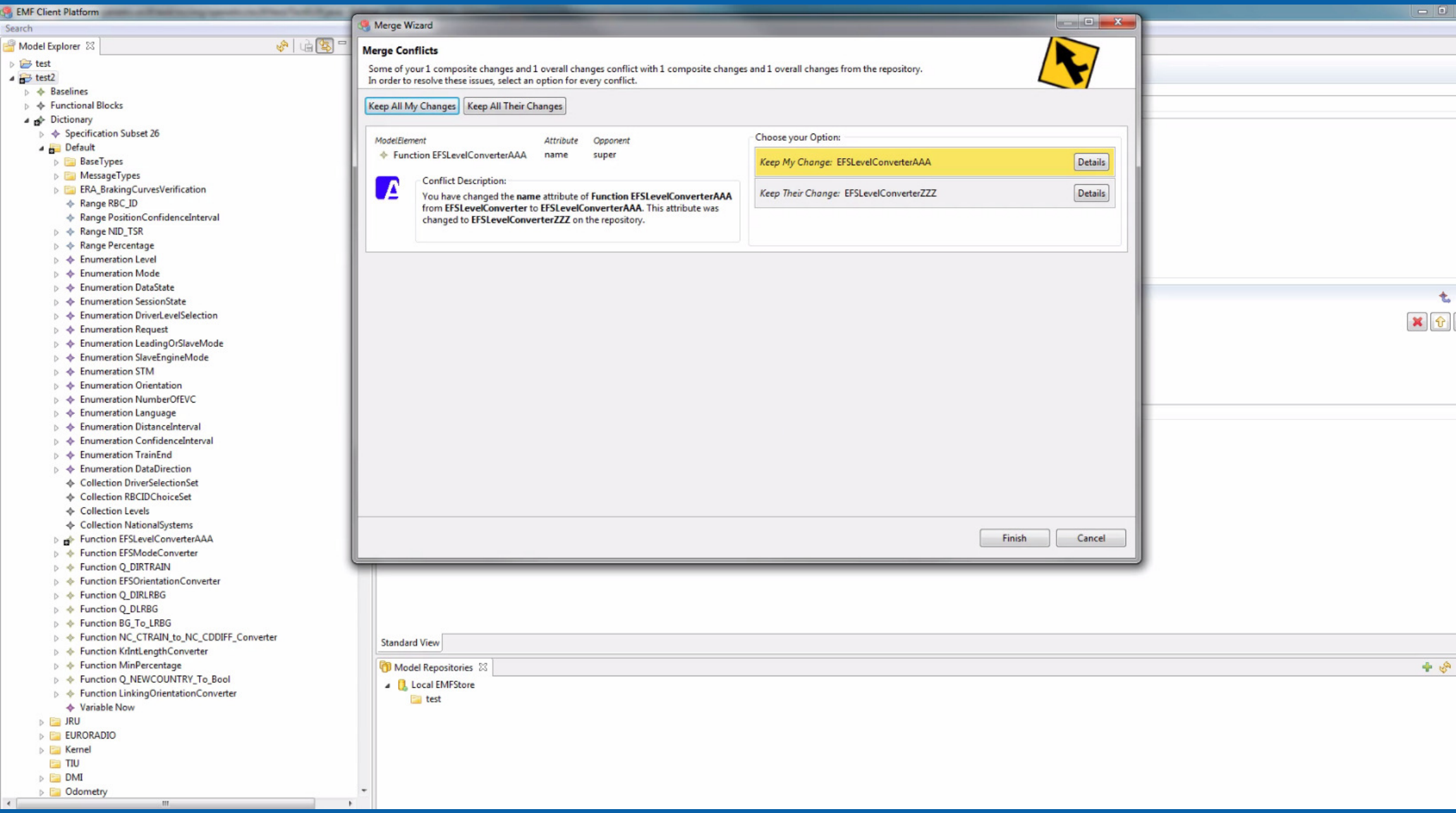


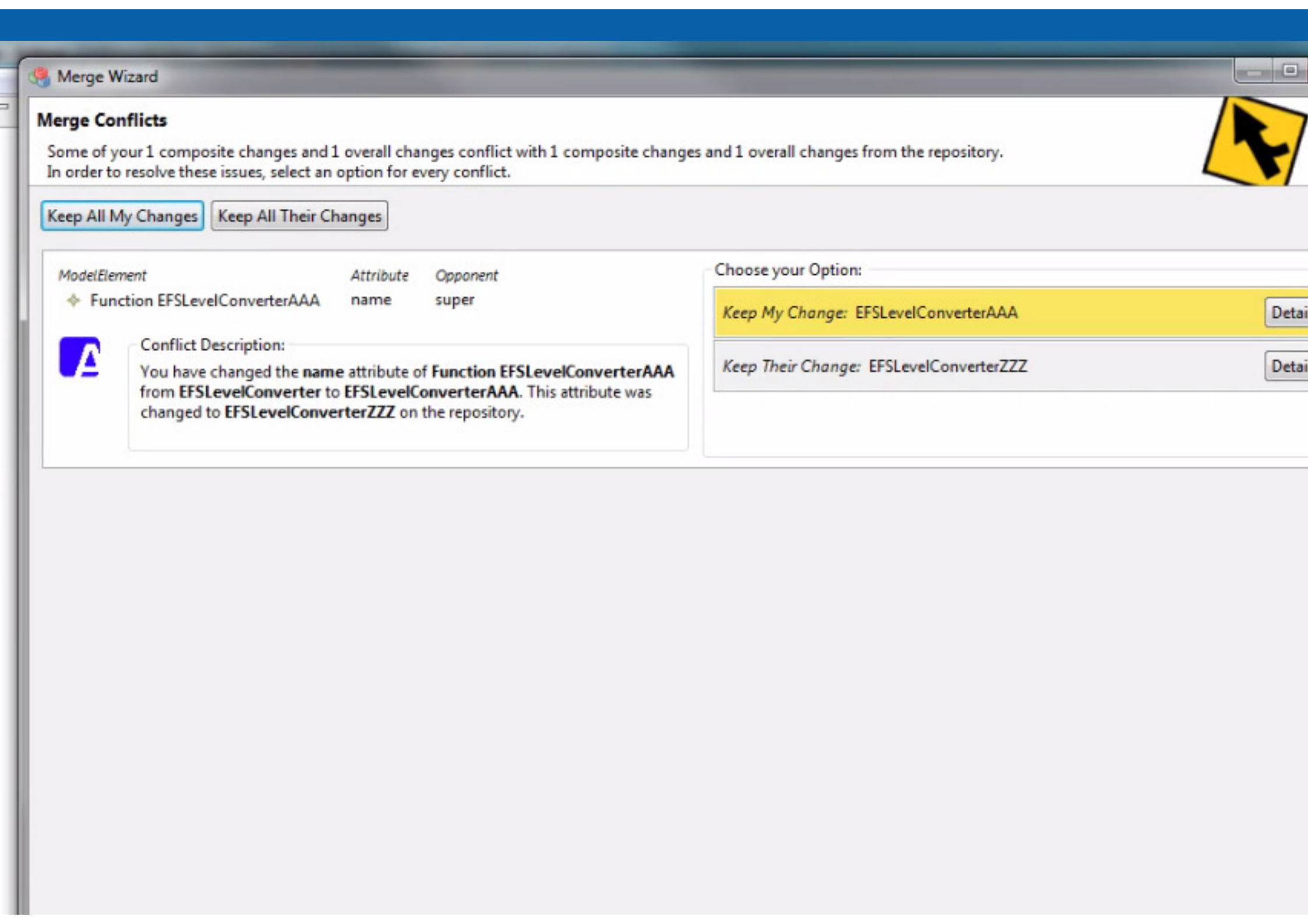
ERTMSFormalSpecs tools

- ERTMSFormalSpecs workbench usable today to model Subset-026
  - Requirements Traceability
  - Complete language
  - Testing environment (15,85% tested as of today)
  - Including Subset-076
- https://github.com/openETCS/ERTMSFormalSpecs/blob/master/ErtmsFormalSpecs/doc/EFSW_User_Guide.doc

Missing features?

- Eclipse version
- File-based version control -> model-based
- *Already available in ERTMSFormalSpecs Eclipse toolchain today:*
  - *ERTMSFormalSpecs EMF model interface*
  - *EMFStore repository for distributed model version control*
- *Ongoing: full ERTMSFormalSpecs Eclispe toolchain, target september 2013*


EMF Client Platform
Search
Model Explorer
test
test2
Baselines
Functional Blocks
Dictionary
Specification Subset 26
Default
BaseTypes
MessageTypes
ERA_BrakingCurvesVerification
Range RBC_ID
Range PositionConfidenceInterval
Range NID_TSR
Range Percentage
Enumeration Level
Enumeration Mode
Enumeration DataState
Enumeration SessionState
Enumeration DriverLevelSelection
Enumeration Request
Enumeration LeadingOrSlaveMode
Enumeration SlaveEngineMode
Enumeration STM
Enumeration Orientation
Enumeration NumberOfEVC
Enumeration Language
Enumeration DistanceInterval
Enumeration ConfidenceInterval
Enumeration TrainEnd
Enumeration DataDirection
Collection DriverSelectionSet
Collection RBCIDChoiceSet
Collection Levels
Collection NationalSystems
Function EFSLevelConverterAAA
Function EFSModeConverter
Function Q_DIRTRAIN
Function EFSOrientationConverter
Function Q_DIRLRBG
Function Q_DLRBG
Function BG_To_LRBG
Function NC_CTRAIN_to_NC_CDDIFF_Converter
Function KrIntLengthConverter
Function MinPercentage
Function Q_NEWCOUNTRY_To_Bool
Function LinkingOrientationConverter
Variable Now
JRU
EURORADIO
Kernel
TIU
DMI
Odometry
Merge Wizard
Merge Conflicts
Some of your 1 composite changes and 1 overall changes conflict with 1 composite changes and 1 overall changes from the repository.
In order to resolve these issues, select an option for every conflict.
Keep All My Changes
Keep All Their Changes
ModelElement
Attribute
Opponent
Function EFSLevelConverterAAA
name
super
Choose your Option:
Keep My Change: EFSLevelConverterAAA
Details
Keep Their Change: EFSLevelConverterZZZ
Details
Conflict Description:
You have changed the name attribute of Function EFSLevelConverterAAA from EFSLevelConverter to EFSLevelConverterAAA. This attribute was changed to EFSLevelConverterZZZ on the repository.
Finish
Cancel
Standard View
Model Repositories
Local EMFStore
test


Merge Wizard
Merge Conflicts
Some of your 1 composite changes and 1 overall changes conflict with 1 composite changes and 1 overall changes from the repository.
In order to resolve these issues, select an option for every conflict.
Keep All My Changes
Keep All Their Changes
ModelElement
Attribute
Opponent
Function EFSLevelConverterAAA
name
super
Conflict Description:
You have changed the name attribute of Function EFSLevelConverterAAA from EFSLevelConverter to EFSLevelConverterAAA. This attribute was changed to EFSLevelConverterZZZ on the repository.
Choose your Option:
Keep My Change: EFSLevelConverterAAA
Detai
Keep Their Change: EFSLevelConverterZZZ
Detai

Summary

- ERTMSFormalSpecs can cover 100% of SSRS (S026 as of today)
- ERTMSFormalSpecs can finish on time
  - Semi-formal model effort: 32 person / month
  - *WP3 T3.5 and T3.6: 194 person / month*
- EUPL toolchain available today
- Eclipse-based toolchain 0.3 available today
  - EMF-based ERTMSFormalSpecs model
  - EMFStore

Any questions?