9th UCAAT User Conference on Advanced Automated Testing

Holistic model-based approach for test generation from safety models

Philipp Dormeier

Stefan Rothbauer

SIEMENS

15/09/2022

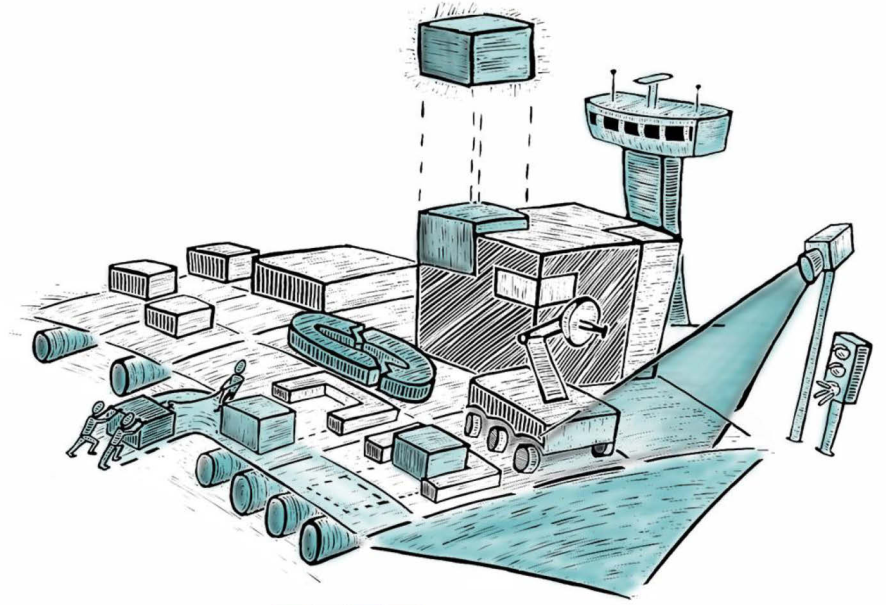
Siemens AG - Technology

Siemens Technology has a strong focus on model-based approaches to master the digital transformation at scale

Within Siemens T SSP (Software Systems and Processes) model-based approaches have been developed e.g., in the areas of:

- SW/System Architecture: DSL based approaches based on CoreDSL
- Safety: Model-based Reliability and Safety Engineering with mbrse
- Testing: Model-based Testing with tedeso

Siemens Technology SSP applies research results in the Siemens Businesses to help them master the challenges of digitalization in particular for highly critical and/or safety-relevant systems



mbrse

CoreDSL

Efficient Creation of
Domain Specific Languages

Problem Statement

Trends in Engineering

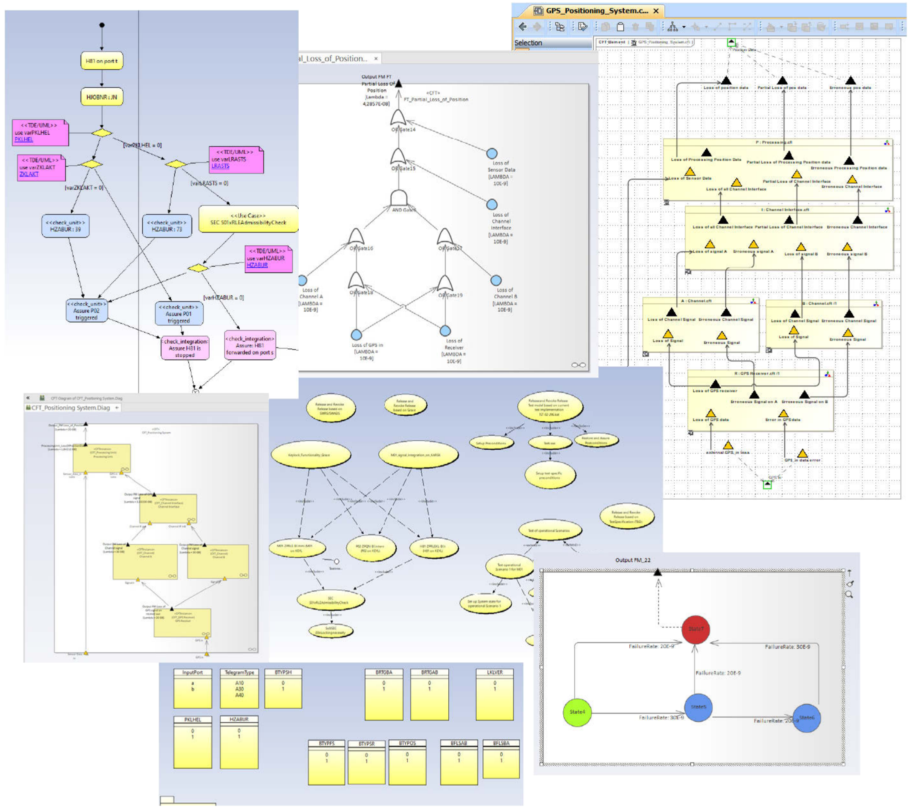
- Complexity of systems increases need for model-based engineering
- Model-based engineering methods support all engineering activities

State of practice

- Usually one model for each aspect under consideration
- Heterogenous, independent models coexisting with manual analyses
- No formal links to enable integration of models

Goal

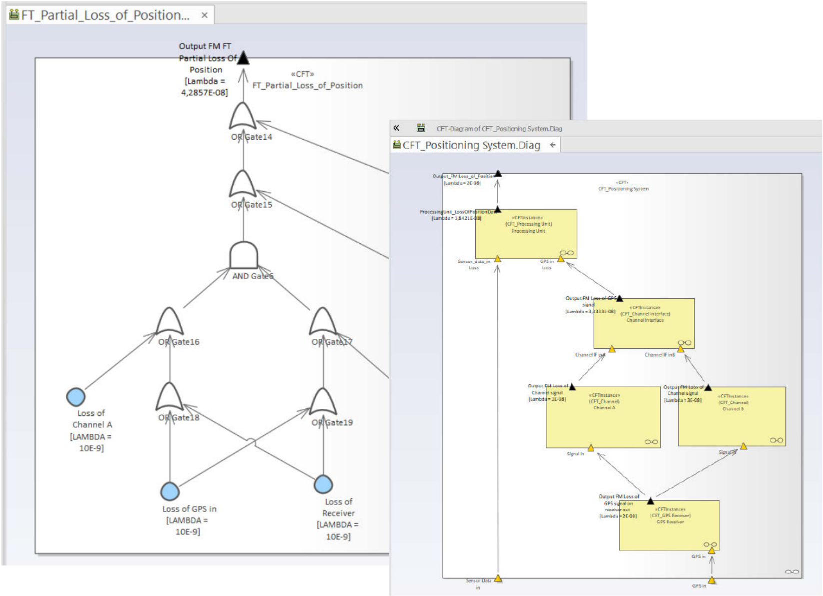
- Integrate models for consistency and efficiency in development
- Seamless integration of models for different aspects,
  e. g. system architecture, test, safety, qualities, …
- Leverage the power of automated analyses and information transfer across models



Solution Approach
Safety, architecture and test models

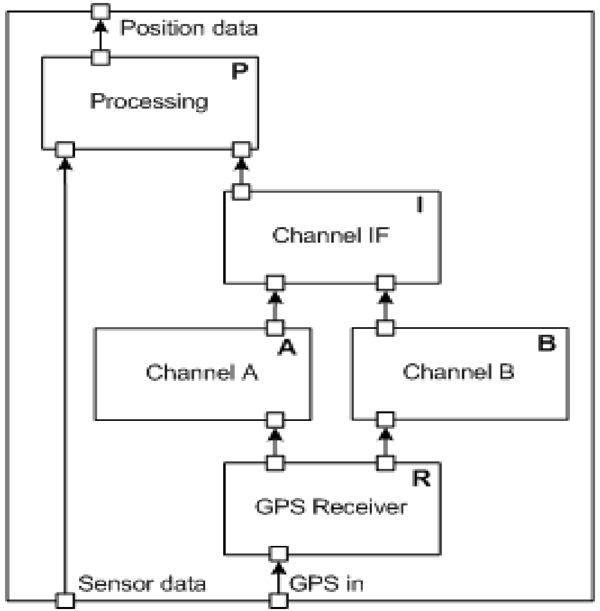
Safety Model

- focus on failure behavior in potentially critical (edge) cases
- cause-effect-relationships
- qualitative and quantitative evaluation for safety cases


FT_Partial_Loss_of_Position... ×
Output FM FT Partial Loss Of Position [Lambda = 4,2857E-08]
«CFT» FT_Partial_Loss_of_Position
OR Gate14
OR Gate15
AND Gate6
OR Gate16
OR Gate17
OR Gate18
OR Gate19
Loss of Channel A [LAMBDA = 10E-9]
Loss of GPS in [LAMBDA = 10E-9]
Loss of Receiver [LAMBDA = 10E-9]
CFT-Diagram of CFT_Positioning System.Diag
CFT_Positioning System.Diag
Output_FM Loss_of_Position [Lambda = 2E-08]
«CFT» CFT_Positioning System
ProcessingUnit_LossOfPositionData [Lambda = 1,8421E-08]
«CFTInstance» (CFT_Processing Unit) Processing Unit
Sensor_data_in Loss
GPS in Loss
Output FM Loss of GPS signal
«CFTInstance» (CFT_Channel Interface) Channel Interface
Channel IF in
Output FM Loss of Channel signal [Lambda = 3E-08]
«CFTInstance» (CFT_Channel) Channel A
«CFTInstance» (CFT_Channel) Channel B
Signal in
Output FM Loss of GPS signal on receiver out [Lambda = 2E-08]
«CFTInstance» (CFT_GPS Receiver) GPS Receiver
GPS in
Sensor Data in

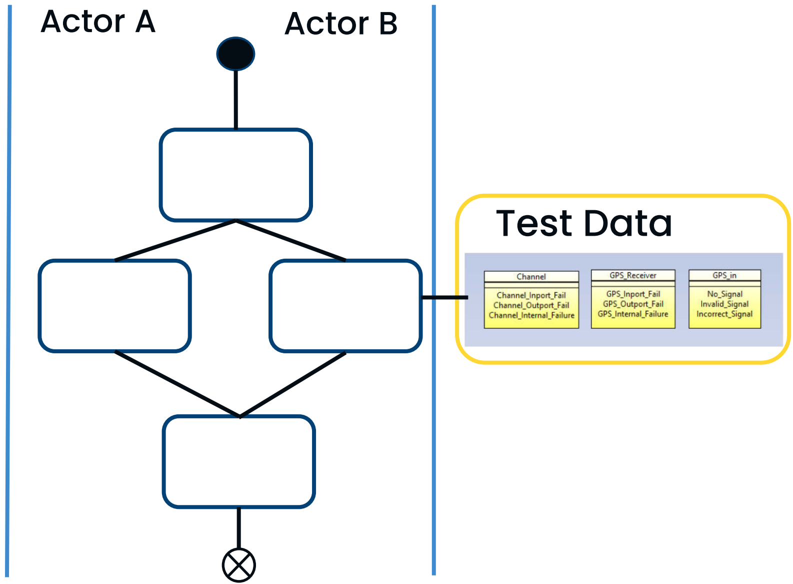
System Architecture Model

- focus on system structure and behavior
- hierarchically structured
- permits various views according to analysis goals



Test Model (tedeso)

- focus on test flow & data (stimuli and system responses)
- basis for test generation and test automation
- Allows to optimize test coverage and high efficiency



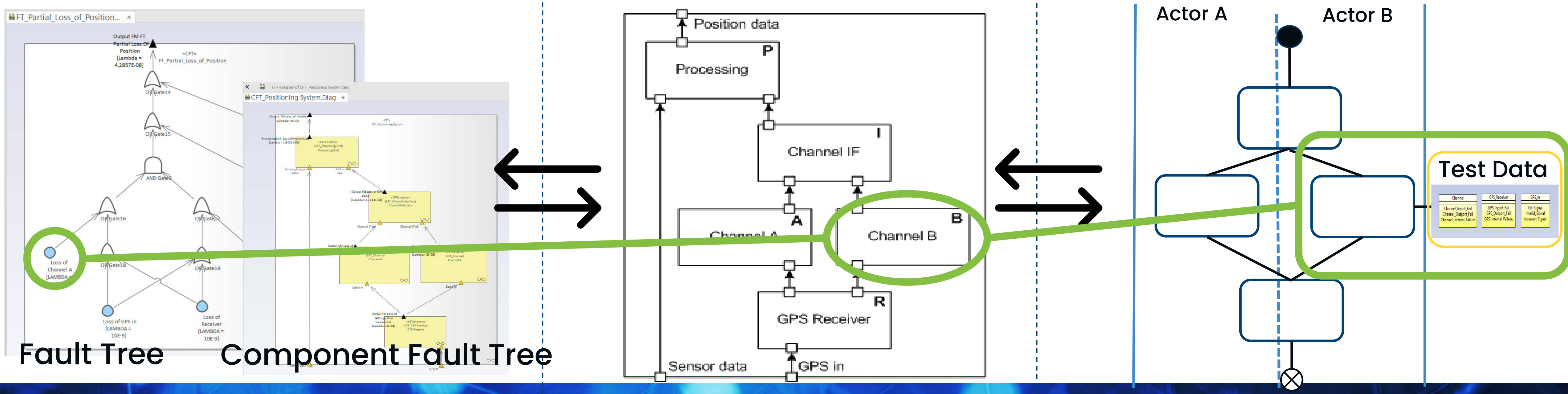
Solution Approach
Transfer of information between models

Safety Model(s)

System Architecture Model

Test Model (tedeso)

- Common data exchange format enables more robust and partly automated reasoning among the models
- Large number of artifacts!
  - Increases with links!

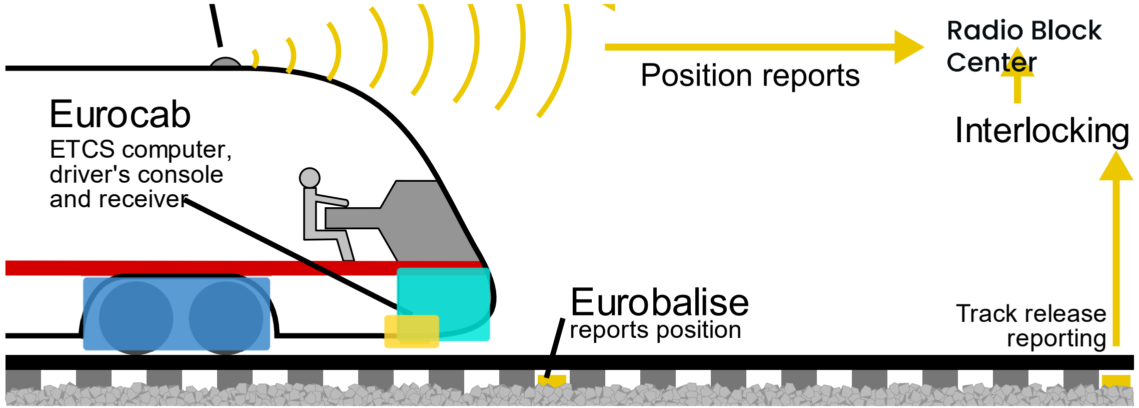


FT_Partial_Loss_of_Position...
Output FM FT Partial Loss Of Position [Lambda = 4,2857E-08]
«CFT» FT_Partial_Loss_of_Position
OR Gate14
OR Gate15
AND Gate6
OR Gate16
OR Gate17
OR Gate18
OR Gate19
Loss of Channel A [LAMBDA =
Loss of GPS in [LAMBDA = 10E-9]
Loss of Receiver [LAMBDA = 10E-9]
CFT-Diagram of CFT_Positioning System.Diag
CFT_Positioning System.Diag
Fault Tree
Component Fault Tree
Position data
Processing
P
Channel IF
I
Channel A
A
Channel B
B
GPS Receiver
R
Sensor data
GPS in
Actor A
Actor B
Test Data

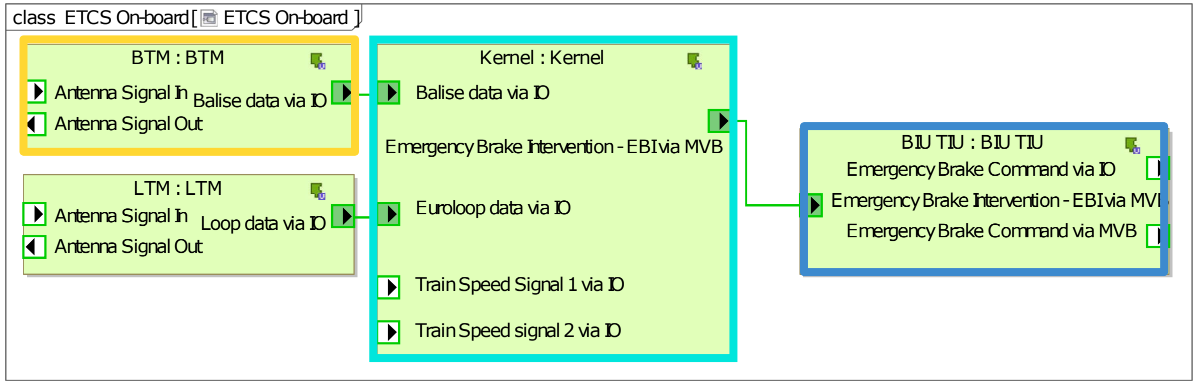
European Train Control System (ETCS) The problem domain and example project

European Train Control System

- Unified train protection system
- Replace national, partly incompatible train protection systems
- Defines trackside equipment and OnBoard systems
- Specified in *Subsets* of which one was chosen and adopted into an example project
  - ERTMS/ETCS Subset UNISIG-091 "Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2"

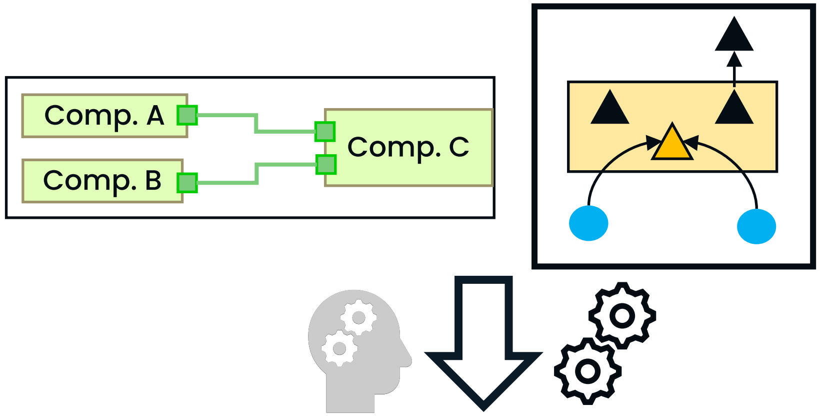


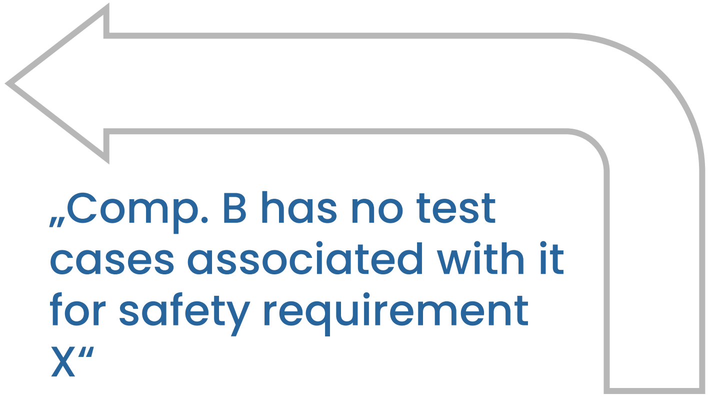
Source: https://de.wikipedia.org/wiki/European_Train_Control_System


class ETCS On-board [ETCS On-board]
BTM : BTM
Antenna Signal In
Balise data via IO
Antenna Signal Out
LTM : LTM
Antenna Signal In
Loop data via IO
Antenna Signal Out
Kernel : Kernel
Balise data via IO
Emergency Brake Intervention - EBI via MVB
Euroloop data via IO
Train Speed Signal 1 via IO
Train Speed signal 2 via IO
BIU TIU : BIU TIU
Emergency Brake Command via IO
Emergency Brake Intervention - EBI via MV
Emergency Brake Command via MVB

ETCS – Models, information transfer, generated parts…

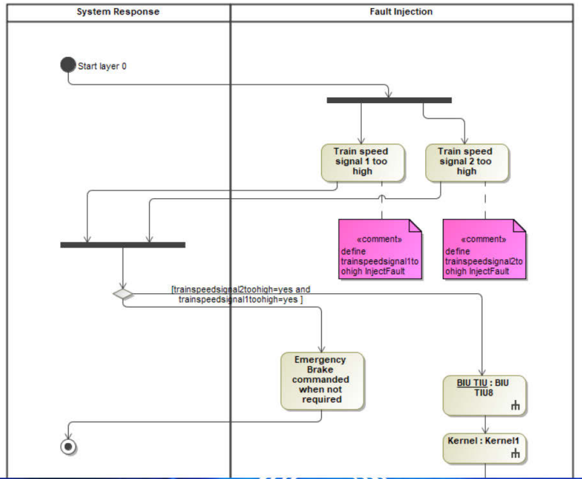
- *Example*: Service brake / emergency brake (EB) not commanded when required

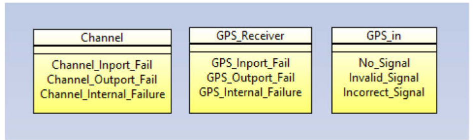




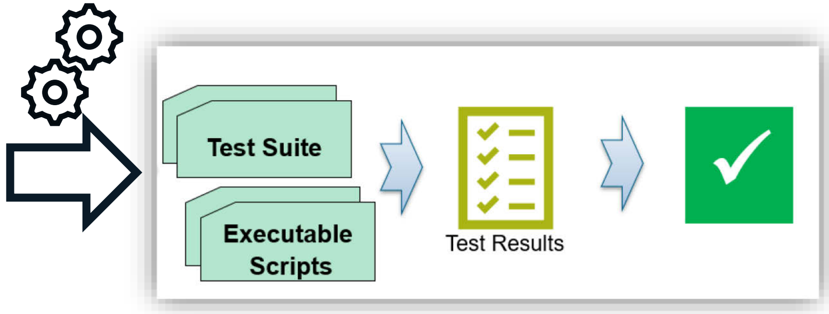
„Comp. B has no test cases associated with it for safety requirement X“

- Automated and well-defined information exchange via generated test models
  - System Response (“expected”)
  - Fault Injection
- Introduction of traceability approach


System Response
Fault Injection
Start layer 0
Train speed signal 1 too high
Train speed signal 2 too high
«comment» define trainspeedsignal1toohigh InjectFault
«comment» define trainspeedsignal2toohigh InjectFault
[trainspeedsignal2toohigh=yes and trainspeedsignal1toohigh=yes]
Emergency Brake commanded when not required
BIU TIU : BIU TIU8
Kernel : Kernel1



Channel	GPS_Receiver	GPS_in
Channel_Inport_Fail Channel_Outport_Fail Channel_Internal_Failure	GPS_Inport_Fail GPS_Outport_Fail GPS_Internal_Failure	No_Signal Invalid_Signal Incorrect_Signal



Example ETCS
…lead to

- Synchronized and consistent system models and artefacts regarding requirements, architecture, safety and test
- Bidirectional traceability of all artefacts involved
- Optimized test suites e. g. to support safety case
- Ability to collect, evaluate & interpret relevant metrics
- Highly automated

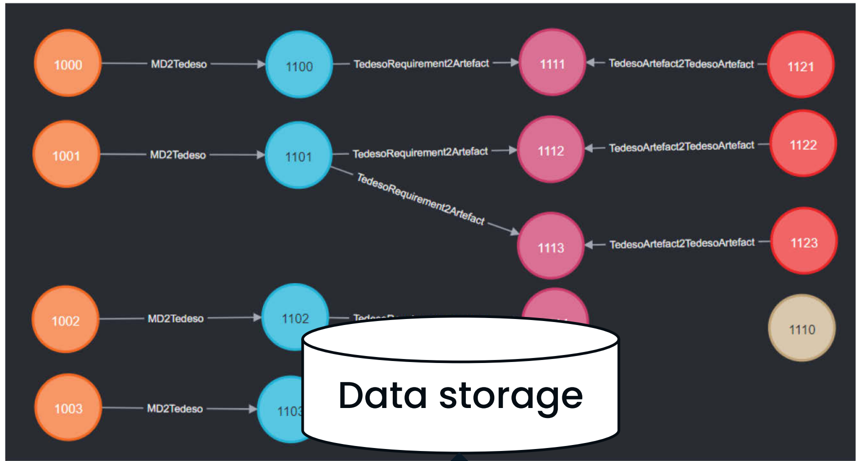
	EBCmdNotReq	EBNotOrTooLate		
	I - VIII	I-VI	VII	VIII
Komp. 1	67	33	x	67
Komp. 2	50	0	x	0
Komp. 3	0	100	x	100
Komp. 4	100	100	x	100
Komp. 5	100	100	x	100
Komp. 6	0	50	x	100
Komp. 7	0	50	x	100

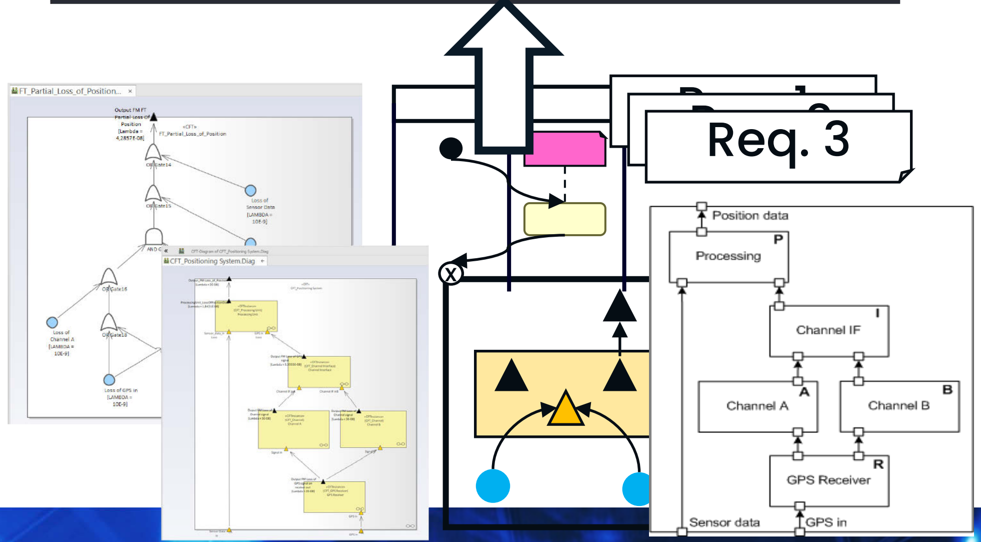
System Req.

Tedeso Req.

Test Model Element

Test Case


1000
MD2Tedeso
1100
TedesoRequirement2Artefact
1111
TedesoArtefact2TedesoArtefact
1121
1001
MD2Tedeso
1101
TedesoRequirement2Artefact
1112
TedesoArtefact2TedesoArtefact
1122
TedesoRequirement2Artefact
1113
TedesoArtefact2TedesoArtefact
1123
1002
MD2Tedeso
1102
1110
1003
MD2Tedeso
1103
Data storage



Benefits of holistic model-based approach integrating system, safety and test models

Consistent models

- Integration and synchronization of models and artefacts from various engineering perspectives
- Maintainable with less effort

Reduction of effort: more effective and efficient testing

- Generation of test models ensures consistency and bidirectional traceability between models for system architecture, safety, requirements and test
- Generation of executable test cases and test automation extends traceability to test results

Deeper level of insight

- Tracing information model enables optimizing test suites
  - E. g. regarding system or safety goals
  - Using domain and use case dependent specific coverage metrics
  - Extensible and inter-tool information flow can be used to adapt development and test

Summary, outlook and future work

Current status

- Implemented prototypical implementation of tooling to support methodology and approach integrating system, safety and test models for end-to-end tracing
- Shown feasibility and potential benefits on a realistic, but small scale, partly simplified example

Next steps

- Apply approach to an example from industrial practice to
  - proof scalability to larger and more complex projects
  - improve usability of tooling for domain experts
- Extend approach to further domains
  - investigate potentially needed adaptations
  - integration of different types of models

Any further questions?

Philipp Dormeier
philipp@dormeier.bayern

Stefan Rothbauer
Siemens AG, T SSP DAM-DE
stefan.rothbauer@siemens.com
+49 (152) 54690620