Formale und anwenderfreundliche Verhaltensbeschreibung von reaktiven Systemen

Lars Ebrecht

Deutsches Zentrum
DLR für Luft- und Raumfahrt e.V.
in der Helmholtz-Gemeinschaft

Fragestellung

Wie kann / sollte / müsste das Verhalten von reaktiven Systemen beschrieben werden?

- formal
- anwenderfreundlich (intuitiv)

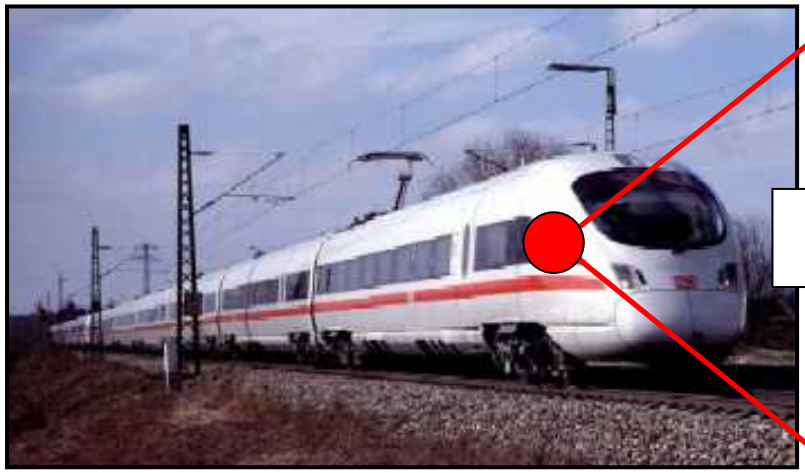
Was ist das Wesentliche bei reaktiven Systemen?

- Interaktion mit der Umwelt
  - anderen Komponenten/Systemen
  - dem Menschen
- Zustandsabhängiges Verhalten
- Zeitabhängiges Verhalten
  (zeitliche Bedingungen)
- Mehr oder weniger komplexe Funktionen
  - Ausgelöst durch Schnittstellenereignisse

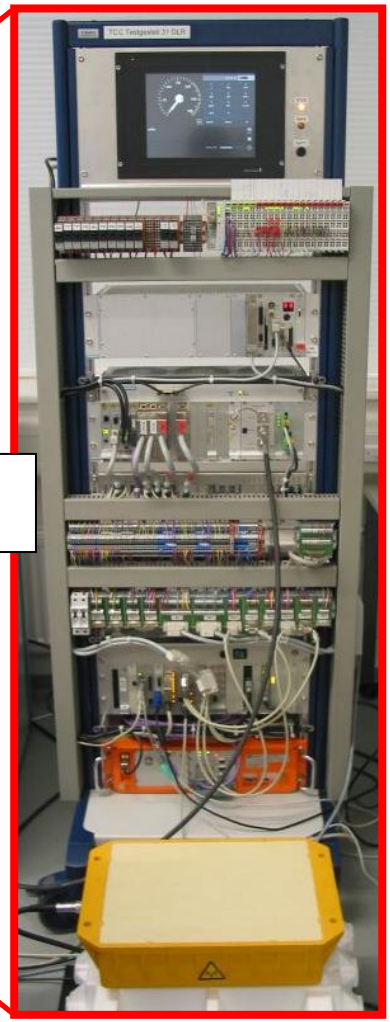
Was ist das Wesentliche bei reaktiven Systemen?

- Schnittstellenereignisse/-nachrichten
- Zustände
- Zeit
- Funktionen

Beispiel Steuer/-überwachungseinheit eines Zuges



ETCS EVC



ETCS – European Train Control System
EVC – European Vital Computer

Verhaltensbeschreibung von Reaktiven Systemen

Nur wie genau?

- Mit welcher Syntax?
- Nach welchen Regeln?
- Mit welcher Semantik?

Momentan tabellarische Darstellung (semi-formal) möglicher Startablauf eines EVC

ALCATEL * ALSTOM * ANSALDO SIGNAL * BOMBARDIER * INVENSYS RAIL * SIEMENS

SEQUENCE OF TEST										
Step	**Dist. (m)**	**Previous**		**Description of Events**	**I/O**	**Interface**	**Comments**	**Next**		**Test Result**
Feature 541: The ETCS on-board system is powered (Transition [4]) **Test Case 1:** Testing of mode transition from NP to SB										
1	0.00	L2	NP	The power of the on-board is switched on. The on-board equipment changes to SB mode.	-	-		L2	SB	
2	0.00	L2	SB	The new current mode SB is RECORDED on JRU	O	JRU		L2	SB	
Feature 522: Indication of Auto-tests results to the driver **Test Case 1:** Indication of Auto-tests results and SB mode to the driver										
5	0.00	L2	SB	Driver opens desk	I	TIU	Recording this TIU input is not mandatory (see SUBSET-27)	L2	SB	
6	0.00	L2	SB	The actual mode SB is DISPLAYED	O	DMI	The SB indication after opening the desk may not be recorded. Because the change of mode was already recorded while desk was closed (FT541)	L2	SB	
7	0.00	L2	SB	After finishing the tests (self test and test of external devices) the predefined text message 'TEST RESULTS ARE OK' (Or similar) is DISPLAYED.	O	DMI	With switch on of power the self test is initiated (automatically).	L2	SB	
8	0.00	L2	SB	The text message 'TEST RESULTS ARE OK' (Or similar) is RECORDED.	O	JRU		L2	SB	
Feature 523: Indication of Stand By mode to the driver **Test Case 1:** The on-board equipment is in Stand By mode. Then it has to be checked that the SB mode is permanently displayed to the driver.										
9	0.00	L2	SB	SB mode is permanently displayed to the driver when the on-board	O	DMI		L2	SB	

Grafische Darstellung mit UML

Zitat: „Wir haben von den Kunden gelernt, dass UML zu umfangreich ist und trotzdem manchmal nicht alle Anforderungen an ein System so abbilden kann, wie der Anwender es möchte“, Bastian Schönhage in Computer Zeitung Jg.38, Nr.5, 29. Januar

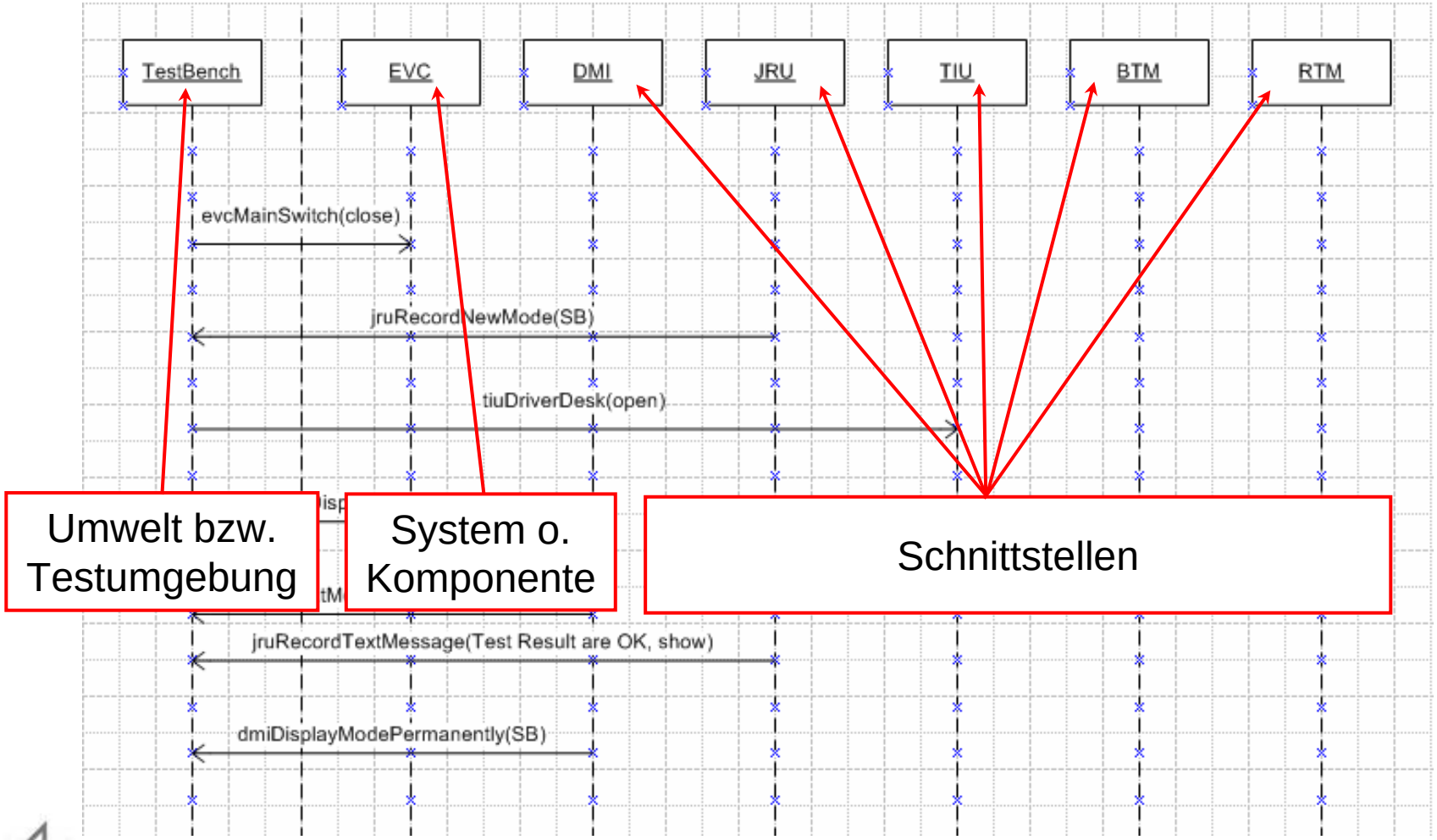
Grafische Darstellung mit UML
Problematik

- UML ist sehr generell, vielseitig und variabel
  - Vorteil und Nachteil zugleich!
  - Vorteil: weites Einsatzspektrum
  - Nachteil: ungenaue, unklare Anwendung im speziellen Kontext, d.h. welche(s) Diagramm(e) und Elemente, wie verwenden(?)

- These: Eine Systembeschreibung, 5 UML-Benutzer
  => 6 verschiedene Beschreibungsformen!?

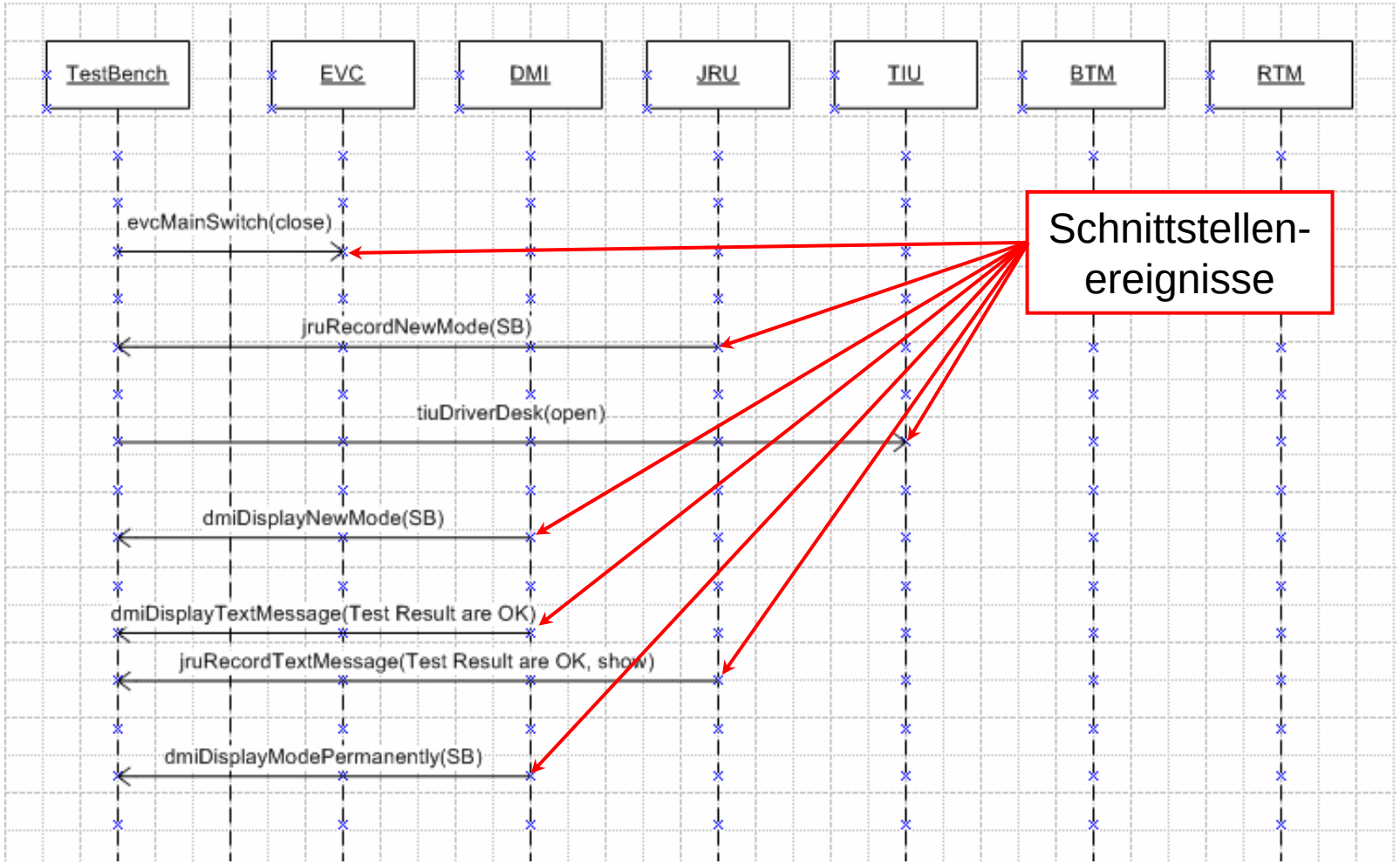
UML Sequenzdiagramm

Schnittstellenereignisse



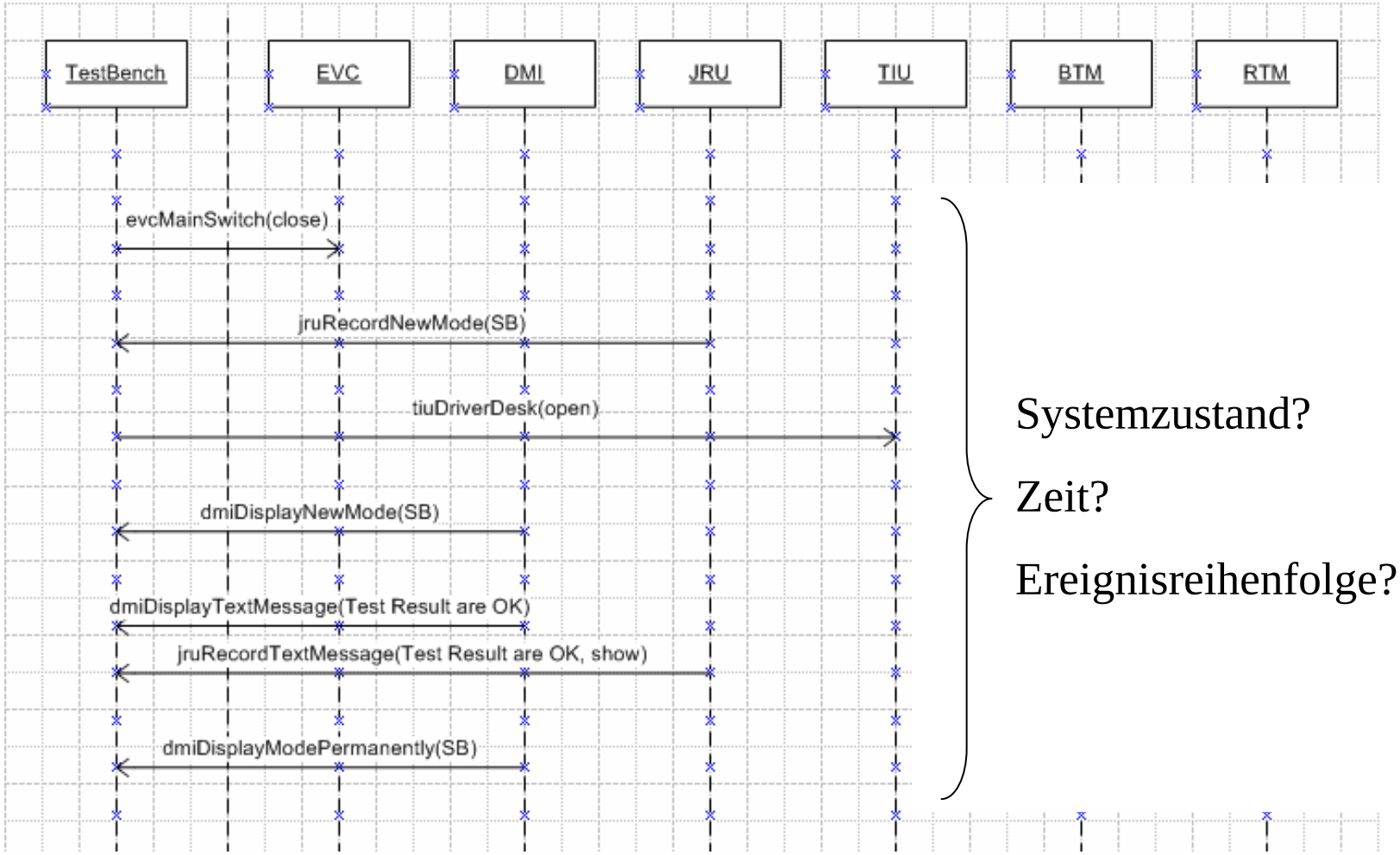
UML Sequenzdiagramm

Schnittstellenereignisse



UML Sequenzdiagramm

Schnittstellenereignisse



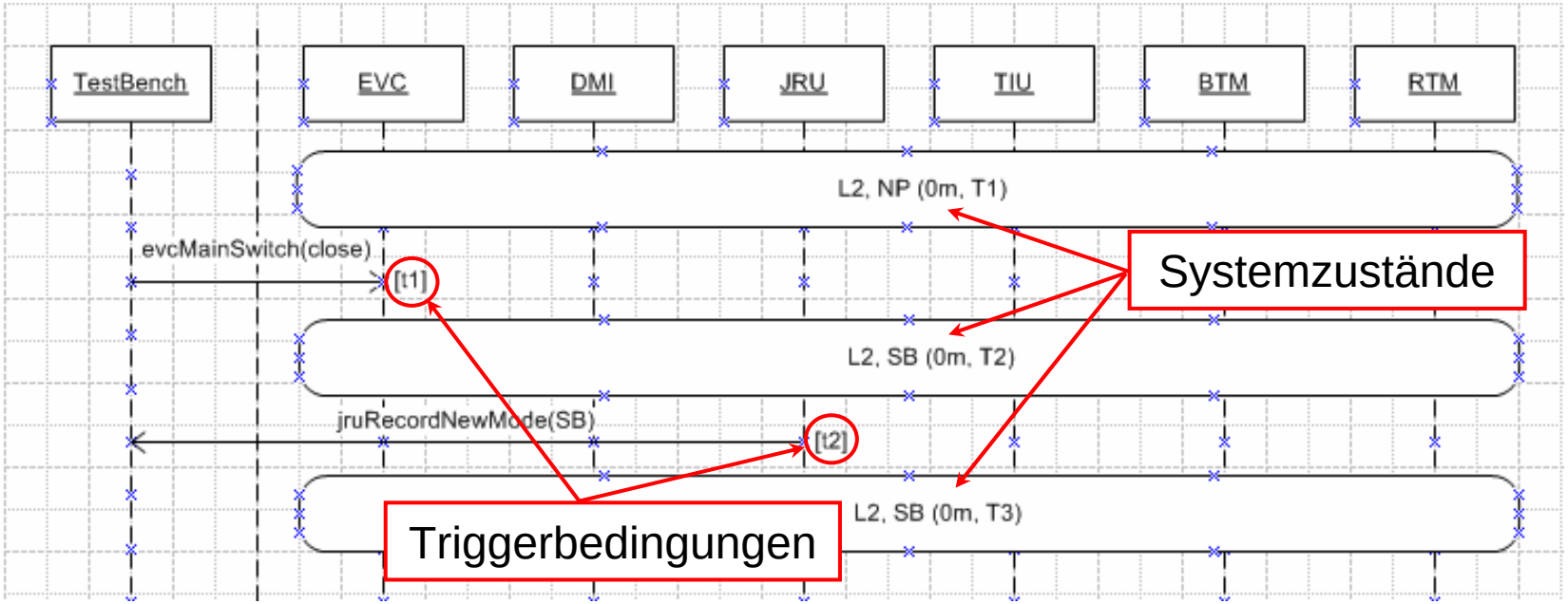
Systemzustand?

Zeit?

Ereignisreihenfolge?

Beschreibung eines Systemfunktionsaufruf

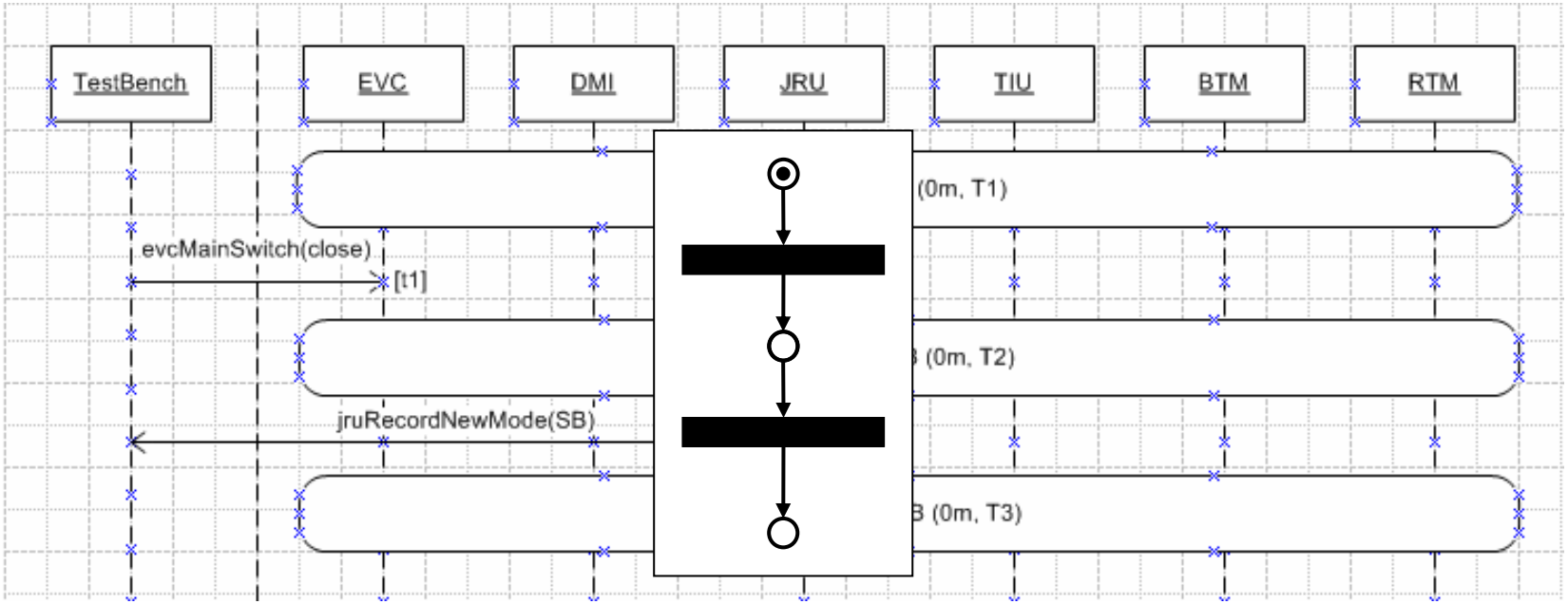
Schnittstellenereignisse, Zustände und Zeit



- Nicht-blockierende Funktionsaufruf
  - Startzustand, Stimulus, Zwischenzustand, Reaktion, Endzustand
  - Startzustand, Stimulus, Endzustand
- Zeit: T1, T2, T3; t1, t2

Beschreibung eines Systemfunktionsaufruf

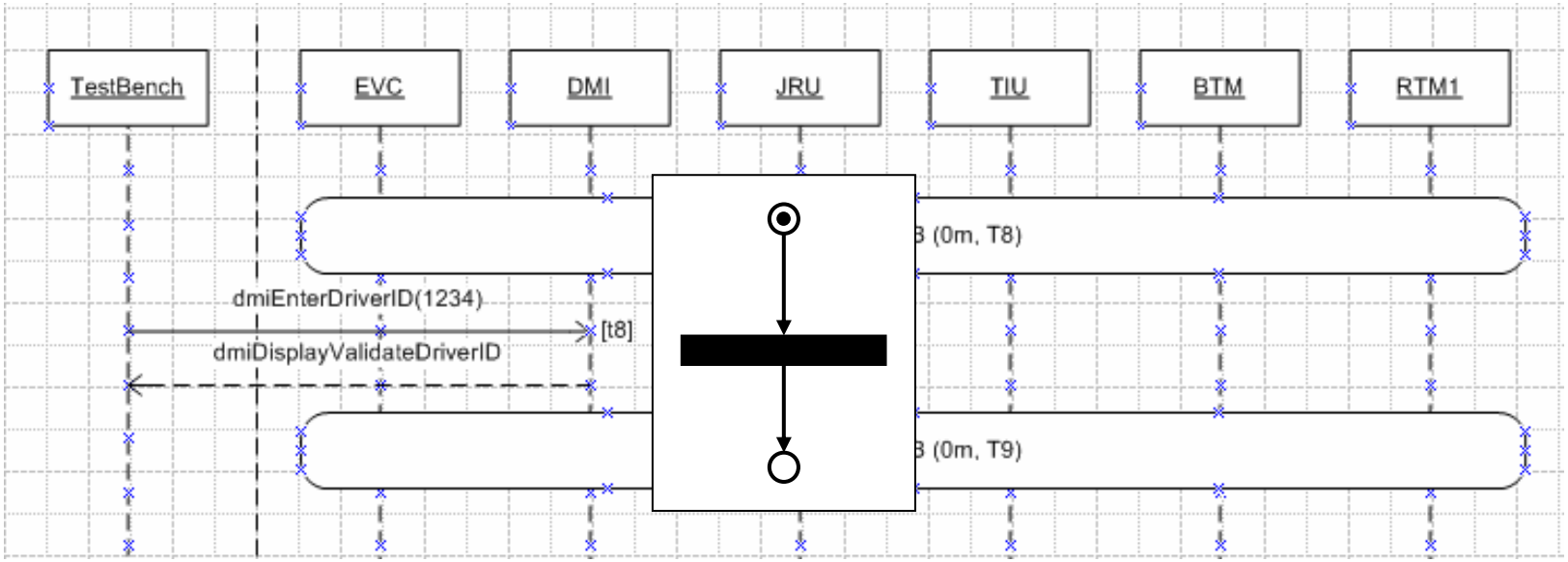
Petri Netz-Semantik der nicht-blockierenden Funktion



- Nicht-blockierende Funktionsaufruf
  - Startzustand, Stimulus, Zwischenzustand, Reaktion, Endzustand
  - Startzustand, Stimulus, Endzustand
- Zeit: T1, T2, T3; t1, t2

Beschreibung eines Systemfunktionsaufruf

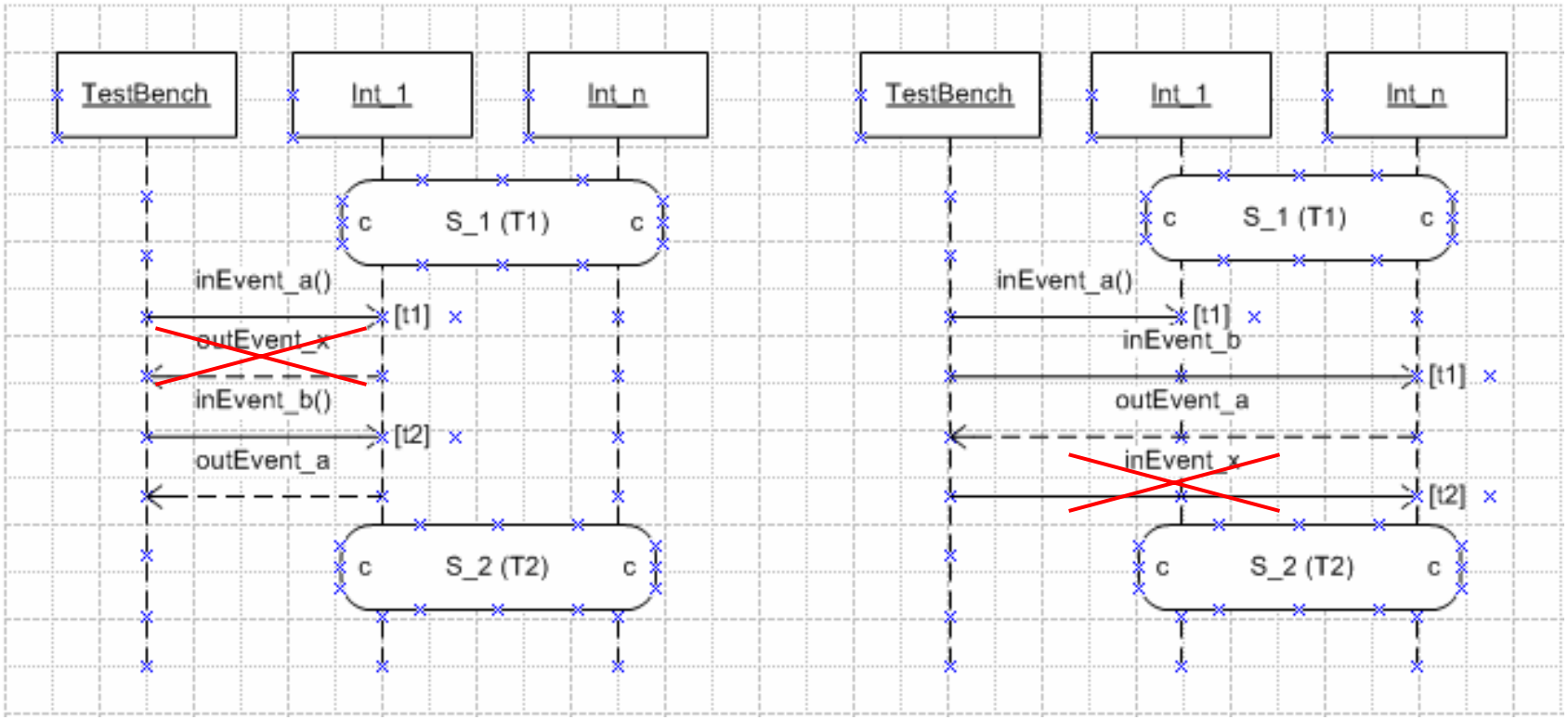
Petri Netz-Semantik der blockierenden Funktion



- Blockierender Funktionsaufruf
  - Startzustand, Stimulus, Reaktion, Endzustand
  - Stimulus und Reaktion sind geordnet (1. Stimulus, dann Reaktion)

Beschreibung eines Systemfunktionsaufruf

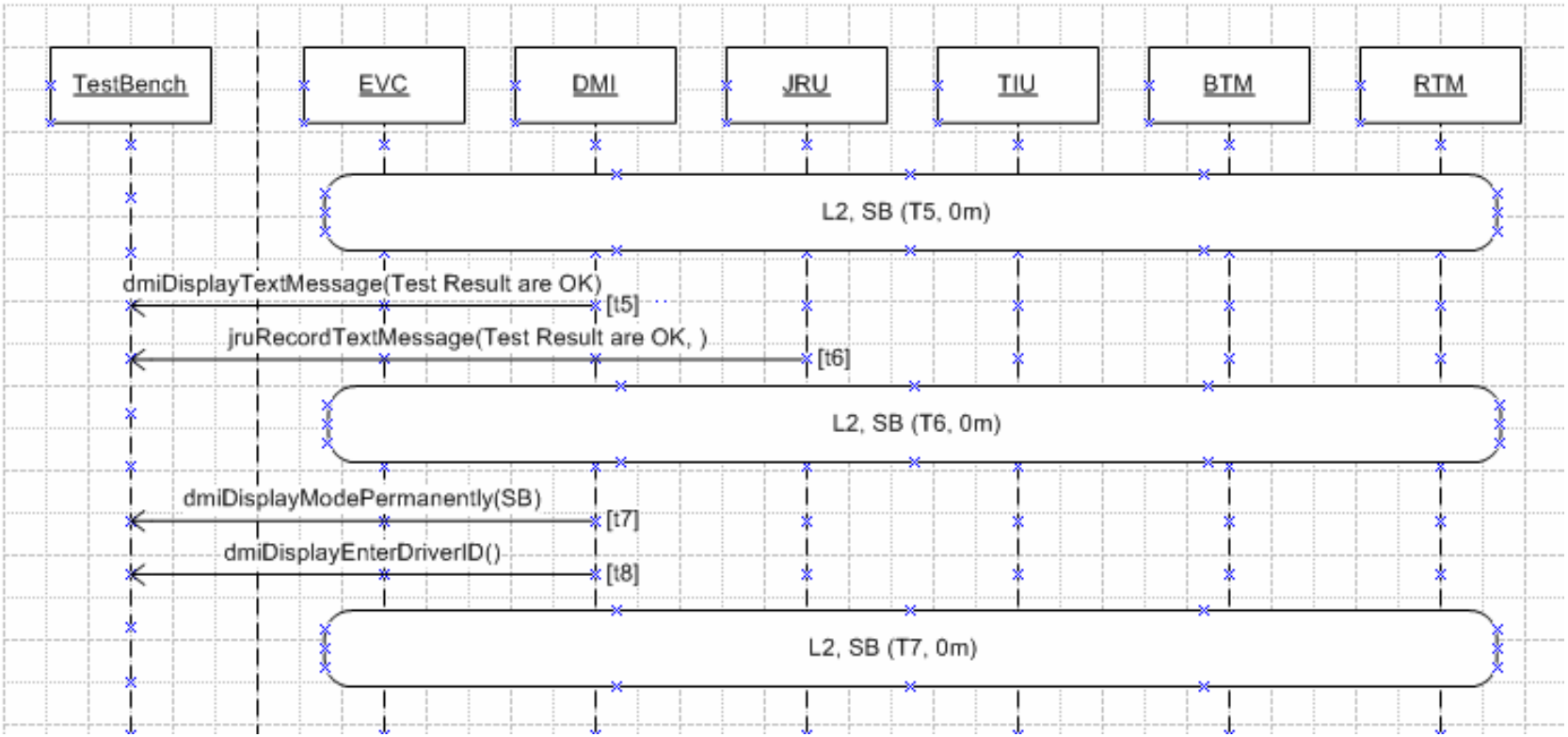
nicht-erlaubte Ereignisse



Bei parallelen Schnittstellen auch mehrere zusammenhängende ein- und/oder ausgehende Nachrichten möglich (inEvent_a, inEvent_b)!

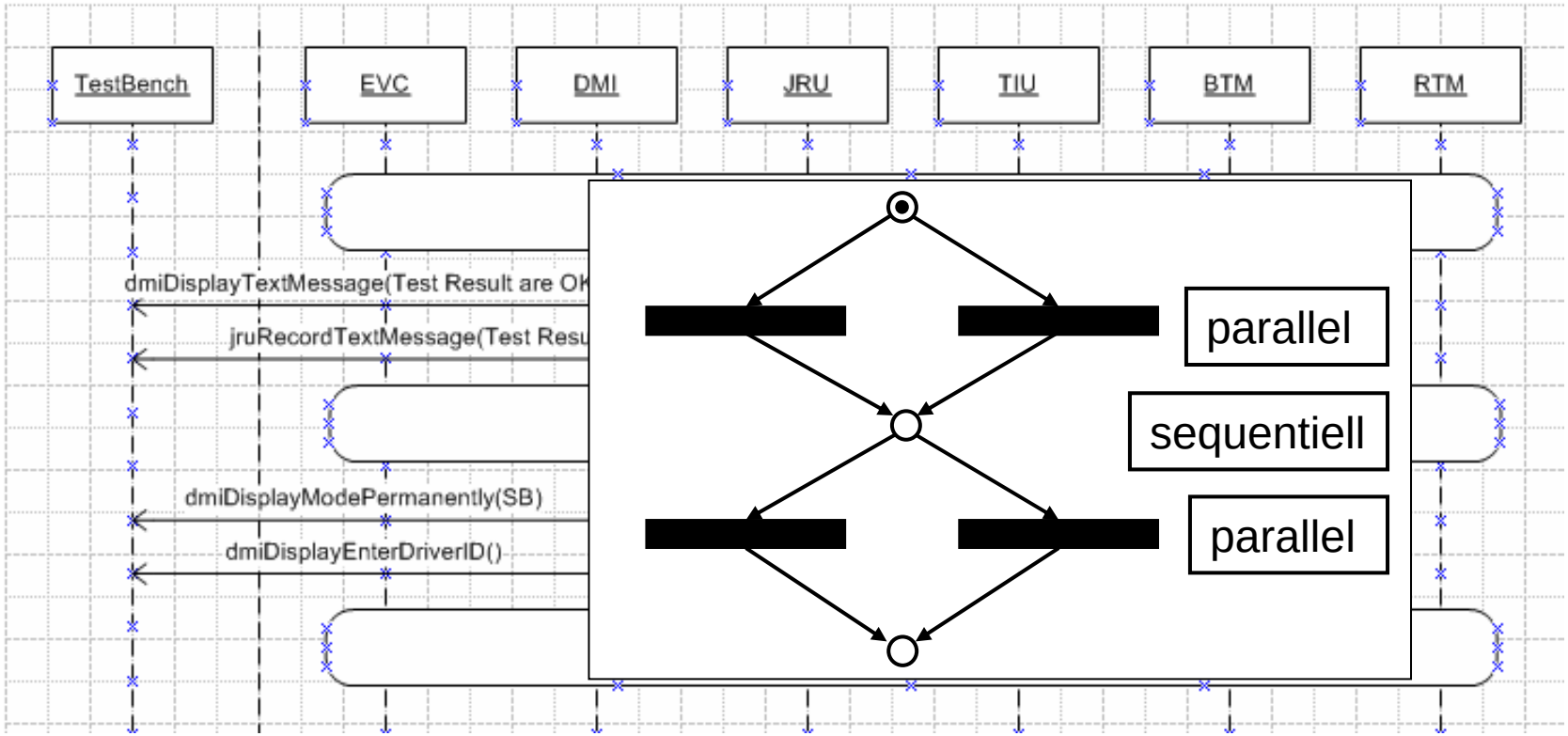
Sequentielle vs. parallele Schnittstellennachrichten

Nicht-/Deterministische Ereignisreihenfolge



Sequentielle vs. parallele Schnittstellennachrichten

Nicht-/Deterministische Ereignisreihenfolge



Vorteile der formalen Verhaltensbeschreibung

- Eindeutige Beschreibung des reaktiven Systemverhaltens
- Gewährleistung
  - einer ausführbaren Beschreibung
  - Berücksichtigung aller erforderlichen Eigenschaften und Parameter des reaktiven Systemverhaltens
- Verwendung für Testautomatisierung

Formale und anwenderfreundliche Verhaltensbeschreibung

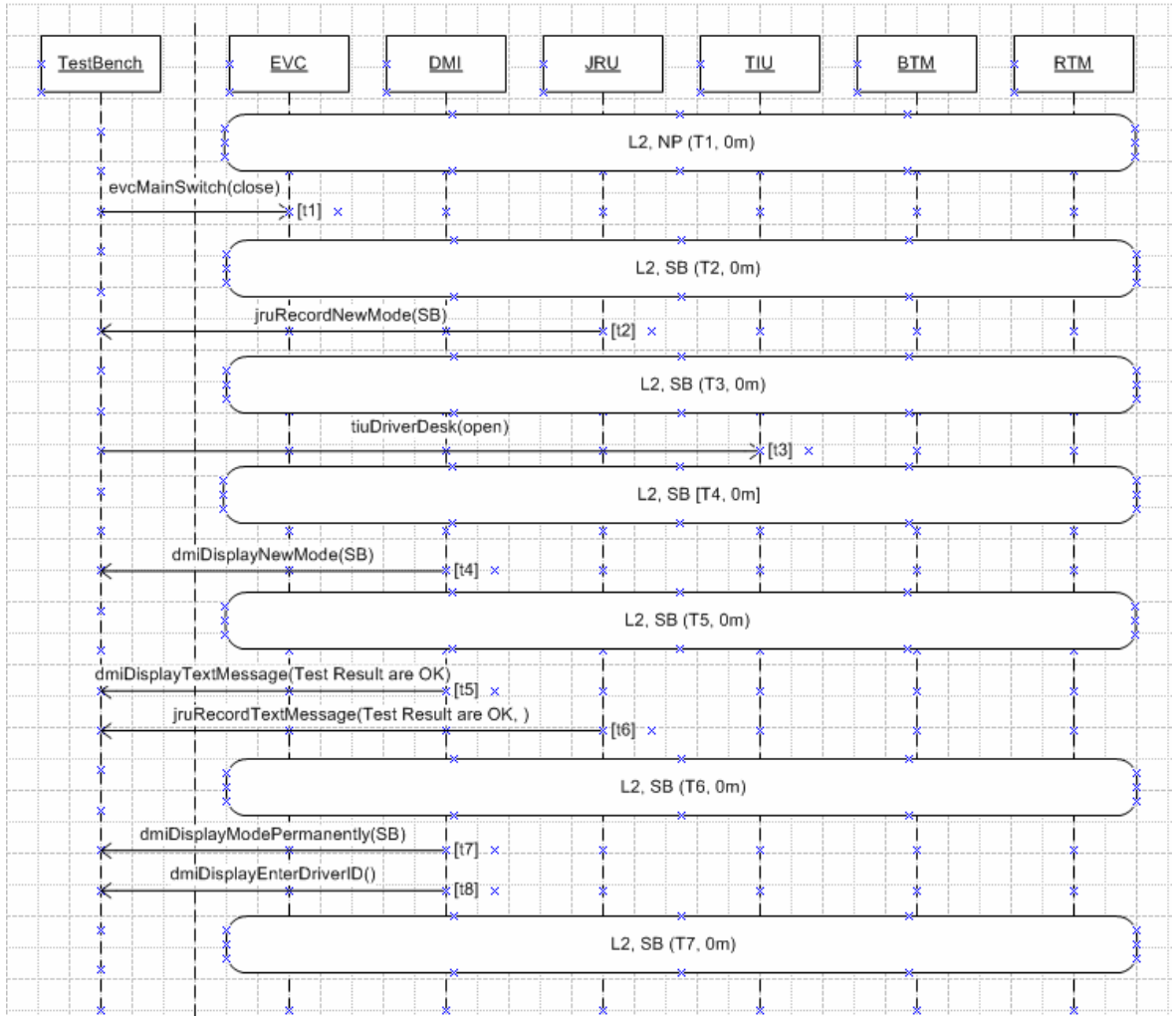
Tabellarisch oder grafisch?

Tabellarische Darstellung (formal)

ALCATEL * ALSTOM * ANSALDO SIGNAL * BOMBARDIER * INVENSYS RAIL * SIEMENS

SEQUENCE OF TEST										
Step	**Dist. (m)**	**Previous**		**Description of Events**	**I/O**	**Interface**	**Comments**	**Next**		**Test Result**
Feature 541: The ETCS on-board system is powered (Transition [4]) **Test Case 1:** Testing of mode transition from NP to SB										
1	0.00	L2	NP	The power of the on-board is switched on. The on-board equipment changes to SB mode.	-	-		L2	SB	
2	0.00	L2	SB	The new current mode SB is RECORDED on JRU	O	JRU		L2	SB	
Feature 522: Indication of Auto-tests results to the driver **Test Case 1:** Indication of Auto-tests results and SB mode to the driver										
5	0.00	L2	SB	Driver opens desk	I	TIU	Recording this TIU input is not mandatory (see SUBSET-27)	L2	SB	
6	0.00	L2	SB	The actual mode SB is DISPLAYED	O	DMI	The SB indication after opening the desk may not be recorded. Because the change of mode was already recorded while desk was closed (FT541)	L2	SB	
7	0.00	L2	SB	After finishing the tests (self test and test of external devices) the predefined text message 'TEST RESULTS ARE OK' (Or similar) is DISPLAYED.	O	DMI	With switch on of power the self test is initiated (automatically).	L2	SB	
8	0.00	L2	SB	The text message 'TEST RESULTS ARE OK' (Or similar) is RECORDED.	O	JRU		L2	SB	
Feature 523: Indication of Stand By mode to the driver **Test Case 1:** The on-board equipment is in Stand By mode. Then it has to be checked that the SB mode is permanently displayed to the driver.										
9	0.00	L2	SB	SB mode is permanently displayed to the driver when the on-board	O	DMI		L2	SB	

UML Sequenz-Diagramm Darstellung



Fragen, Anregungen, Meinungen sind herzlich willkommen

Kontakt: Lars.Ebrecht@dlr.de