Domänenmodellierung und MDSE im Entwurf elektronischer Stellwerke:

Wer stellt die Weichen - und wenn ja, wieviele?

Wilhelm Hasselbring

AG Software Engineering, Institut für Informatik, Universität Kiel

Wolfgang Goerigk

b+m Informatik AG, Melsdorf

SEACON 2010

Agenda

- **Projektkontext**
  - KoSSE, MENGES
- **Fachliche Domäne**
  - Ein Beispiel:
    Die Weiche im Lichte einer Fahrstraße
- **Simulation, Monitoring und Profiling**
  - Kieker-Framework (Siehe auch SEACON 2009)
- **Domänenspezifische Modellierung**
  - MENGES DSL-Partitionslandkarte
  - Ontologie, Topologie, Projektierung
  - Stellwerksarchitektur, Modellgetriebene Entwicklung, MDSE
- **Pragmatik bei der Modellierung**
  - Kieler-Framework
- **Ausblick**

Fotos / Abbildungen: © Funkwerk IT, Markus-Steur.de

Der Kontext: KoSSE-Projekt MENGES

Kompetenzverbund Software Systems Engineering

Verbundprojekte im Themenbereich des Software System Engineering der Universitäten Kiel und Lübeck mit zahlreichen Unternehmen aus Schleswig-Holstein

http://www.kosse-sh.de/

ZUKUNFTSprogramm Schleswig-Holstein
Investition in Ihre Zukunft

MENGES
KoSSE

Modellbasierte Entwurfsmethoden für eine neue Generation elektronischer Stellwerke

AG Software Engineering, Universität Kiel
Wilhelm Hasselbring, Reiner Jung

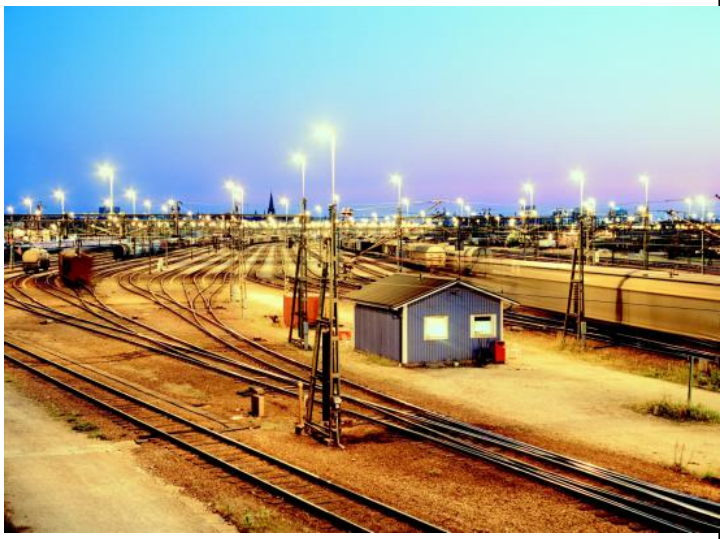
AG Echtzeitsysteme und Eingebettete Systeme, Universität Kiel
Reinhard von Hanxleden, Christian Motika, Christian Schneider

Funkwerk Information Technologies GmbH, Kiel
Holger Neustock, Elferik Schultz

b+m Informatik AG, Melsdorf
Wolfgang Goerigk, Thomas Stahl, Stefan Zeug

MENGES: Motivation und Fachliche Domäne

Sicherer Bahnbetrieb



Elektronische Stellwerke, Gleise, Weichen, Signale, Fahrwege, …

Hohe Sicherheitsanforderungen, technische Sicherheit, Verfahrenssicherheit, Betriebssicherheit, technisch verfahrensgesicherter Bedienplatz

Zertifizierung nach CENELEC, höchster Standard SIL-4 sehr hohe Zertifizierungsaufwände

Wirtschaftlicher Bahnbetrieb

Verlagerung von Personen- und Güterverkehr auf die Schiene, Zukunftssicherung bei gleichzeitiger Aufwands- und Kostenreduktion

Hoher Modernisierungsbedarf bei der Bahn, Pilotprojekt ESTW-R Lindaunis durch Funkwerk IT, Kompetenzbündelung im Kieler Raum

Der modellgetriebene, generative Ansatz (MDSD) bietet einen schlanken Entwicklungsprozess, erhöht die Entwicklungseffizienz, senkt damit die Entwicklungskosten und erhöht die Qualität der entstehenden Anwendungen

MENGES: Zielplattform

Speicherprogrammierbare Steuerungen (SPS)

Hohe Sicherheit und Kostenreduktion in der Entwicklung und im Betrieb durch Einsatz von kompakten Standardlösungen (Speicherprogrammierbare Steuerungen SPS)

Die DB will Kosten sparen → COTS-Produkte, ausfallsichere und hochverfügbare SPSen mit langen Lebenszyklen, gleichzeitig Gewährleistung sicheren Betriebs

Offener Ansatz, generisch, lässt sich aus der ESTW-R-Domäne auf andere Domänen auch im Schienenverkehr übertragen, SPS sind Standardkomponenten in der Industrieautomatisierung

Softwareentwicklung für SPS

SPS sind verschleißfrei, flexibel einsetzbar, relativ klein und kostengünstig, echtzeitfähig, zertifiziert, zuverlässig, schnelle Fehleranalyse, geringerer Stromverbrauch

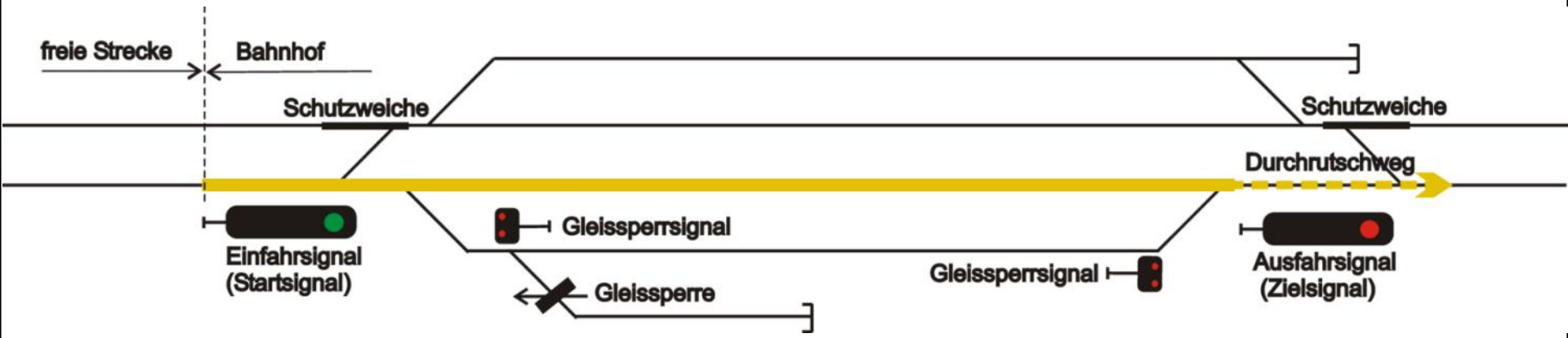
SPS bieten Funktionsblöcke einfacher Art, als eingebettete Systeme einen begrenzten Speicher, spezifische Beschränkungen in der Programmierung für einen zertifizierten Entwicklungsprozess

Ein Beispiel:
Die Weiche im Lichte einer Fahrstraße

Als **Fahrstraße** bezeichnet man im Eisenbahnwesen die Verknüpfung von

Kreuzungen, Weichen, Signalen, …

in passender Stellung zu einem *signaltechnisch gesicherten Fahrweg* für Fahrten durch einen Bahnhof oder über die freie Strecke.



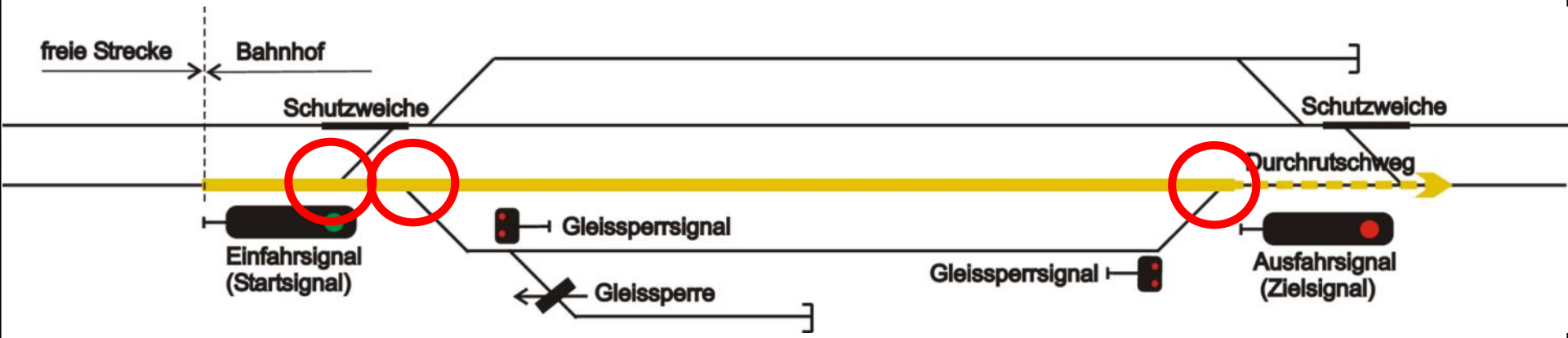
Zeichnung aus Wikipedia

Die Weiche im Lichte einer Fahrstraße

Weichen,

- werden beansprucht

  im Fahrweg einer Fahrstraße

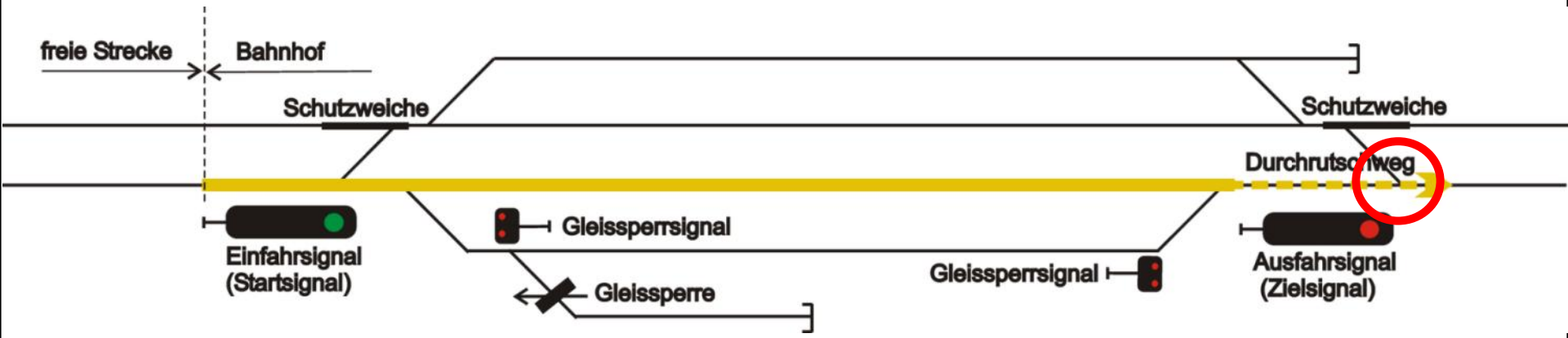


Die Weiche im Lichte einer Fahrstraße

Weichen,

- werden beansprucht

  im Durchrutschweg einer Fahrstraße

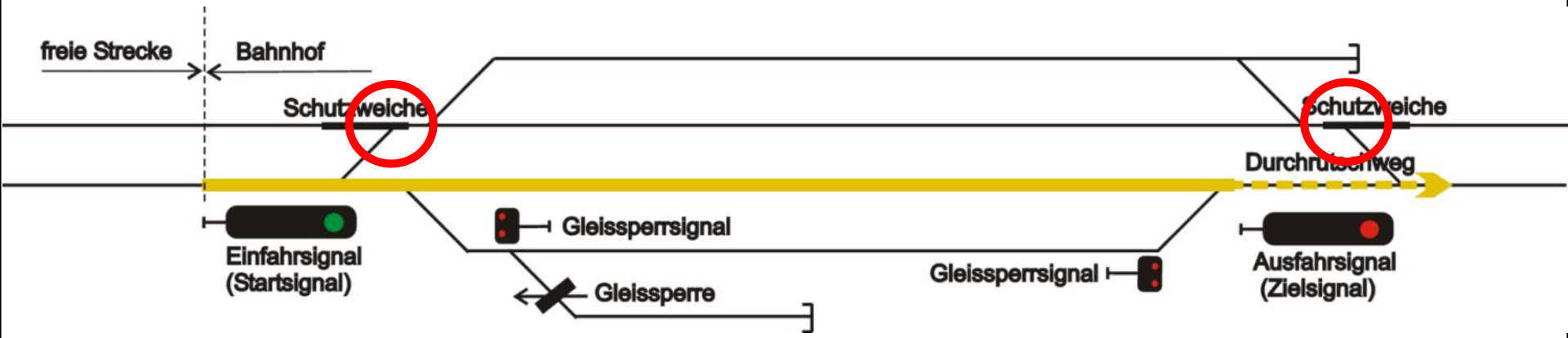


Die Weiche im Lichte einer Fahrstraße

Weichen,

- werden beansprucht

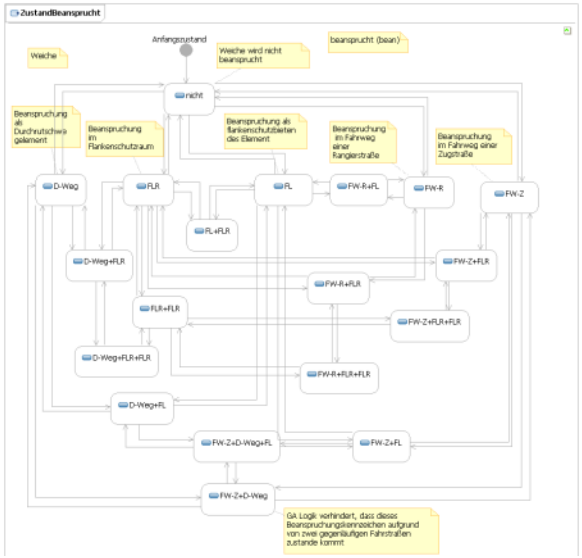
  als flankenschutzbietendes Element
  einer Fahrstraße

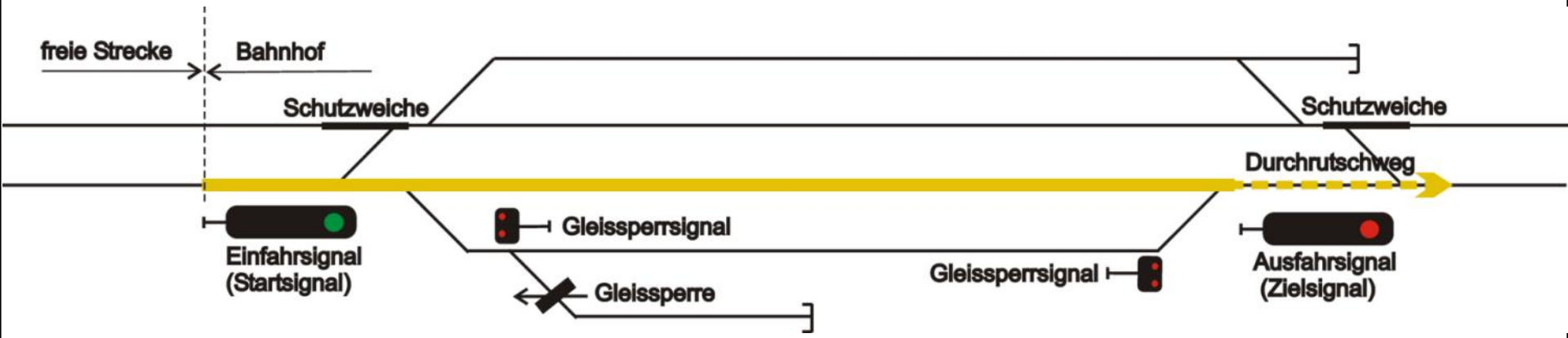


Die Weiche im Lichte einer Fahrstraße

Weichen,

- Die Zustandsvariable „*Beanspruchung*“ hat **19** mögliche Zustände

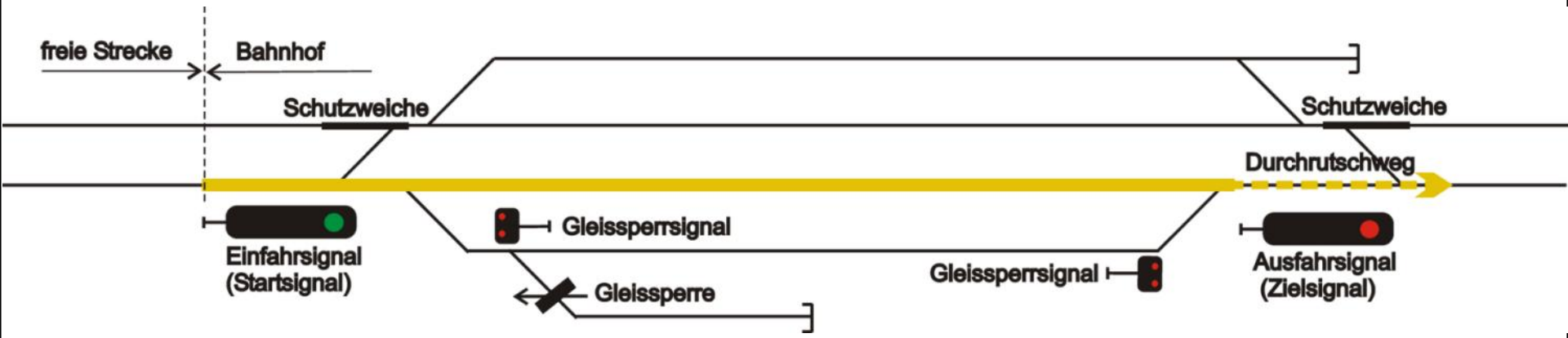




Die Weiche im Lichte einer Fahrstraße

Weichen,

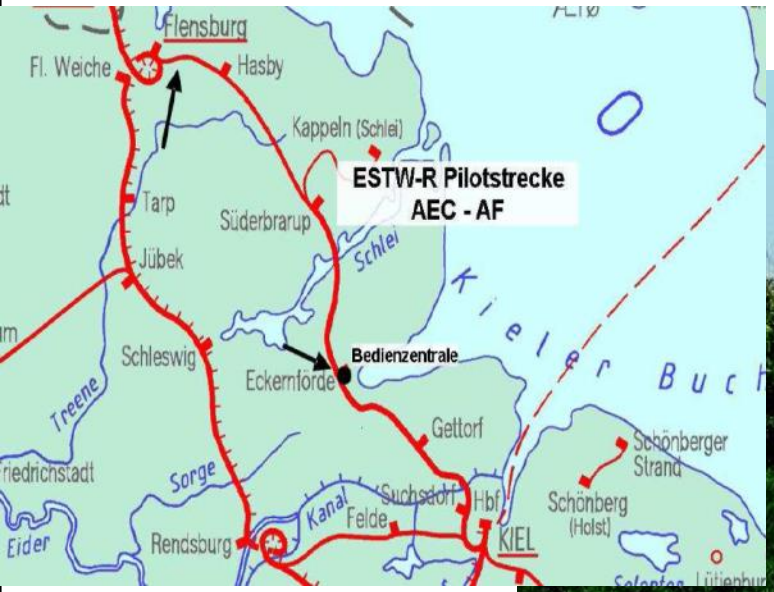
- weitere Zustandsvariablen: Beanspruchung, Befahrbarkeitssperre, Endlageüberwachung, Flankenschutzsicherung, Folgeabhängigkeit, Freimeldung, Profilraumfreimeldung, Reservierung, Solllage, Sperre Weichenlaufkette, Umstellsperre, Verschluss, Weichenauffahrung, Weichenlage, ZustandsdatenVorhanden
- Insgesamt: **466.944** Zustände (allein für die Weiche)



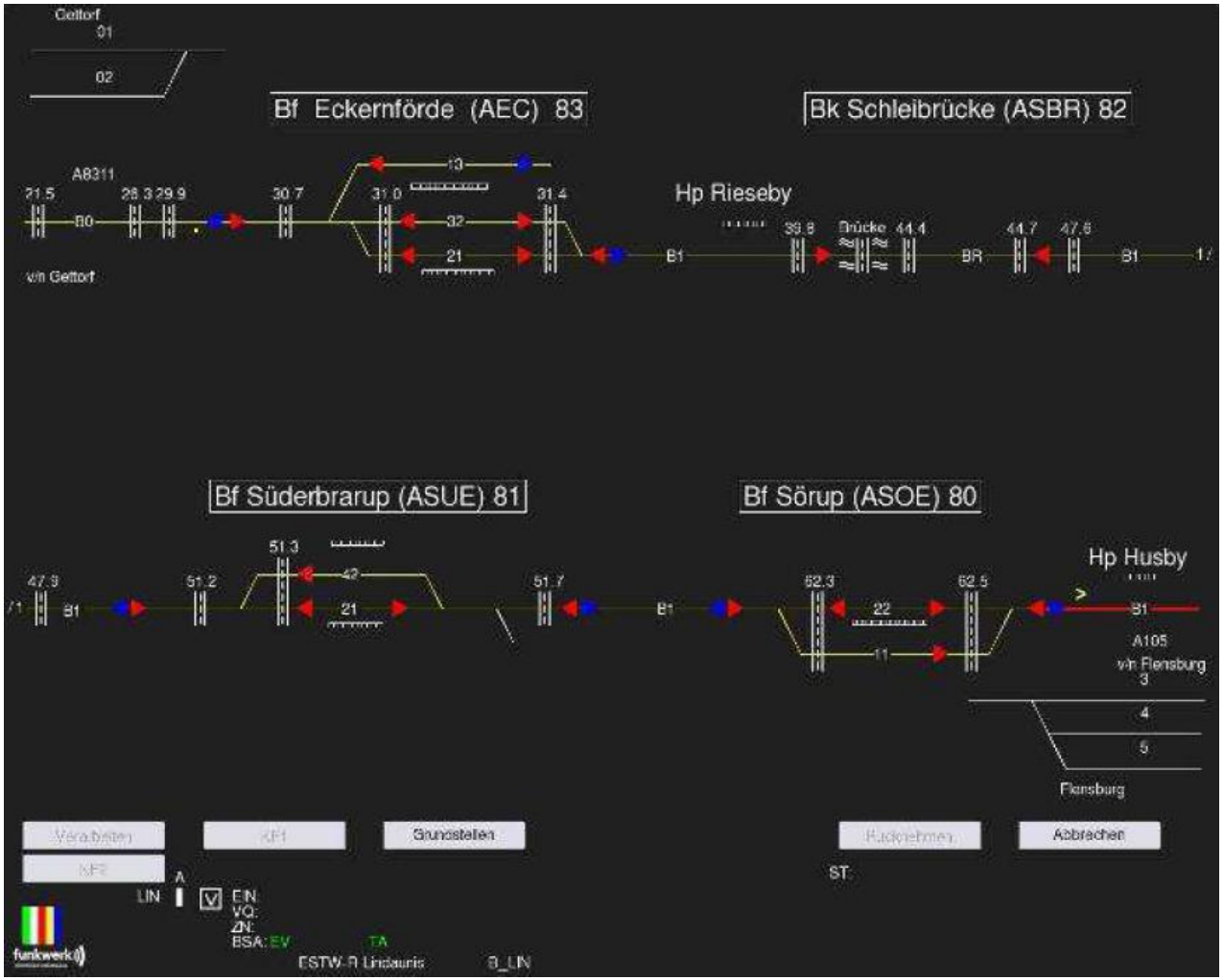
Regionalstrecken

Neben **Weichen** gibt es allein in Regionalstellwerken

- knapp 20 Feldelemente: Vorsignale, Hauptsignale, Gleisabschnitte, Gleissperren, Achszähler, Bahnübergänge und sogar
- eine Klappbrücke über die Schlei, die gleichzeitig dem Straßenverkehr und dem Schienenverkehr dient: Eisenbahn- und Straßenbrücke Lindaunis



Regionalstellwerk ESTW-R Lindaunis



Ein Schaltkasten für die Ansteuerung eines Signals

Steuerungen und IO-Module im Labor-Testfeld

Simulation

Modelle und Szenarien

- **Stellwerksmodell** Beschreibung der Feldelemente
- **Stellwerkslogik** modelliert die Regeln für Fahrstraßen und Bedienhandlungen
- **Umweltmodell** beschreibt äußere Einflüsse, wetterbedingte Störungen, technische Defekte u.ä.
- **Nutzungsszenario** beschreibt die Steuerung von Zugläufen, Rangierfahrten etc.

Teilsimulatoren

- **Steuerungslogik** Ereignisgesteuerte Simulation von Automaten
- **Stellwerkssimulation** Simulation der Gleisanlagen, Signale etc.
- **Umweltsimulation** Aktionen der Züge, Erzeugung von Defekten im Stellwerk und den Zügen, Aktionen des Fahrdienstleiters.

Monitoring und Profiling

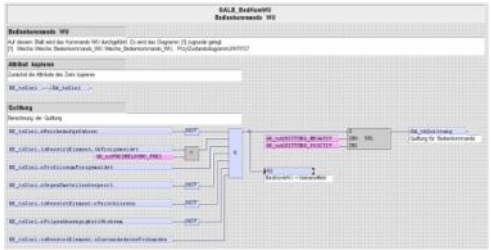
- **Monitoring und Profiling**
  - Die in der Simulation gewonnen Daten werden mit Hilfe des Kieker-Frameworks zur Laufzeit in die Online-Visualisierung eingespeist und in eine Datenbank abgelegt, um sie für eine anschließende Offline-Analyse nutzen zu können.
  - http://kieker.sourceforge.net/

- **Siehe auch Vortrag auf der SEACON 2009**

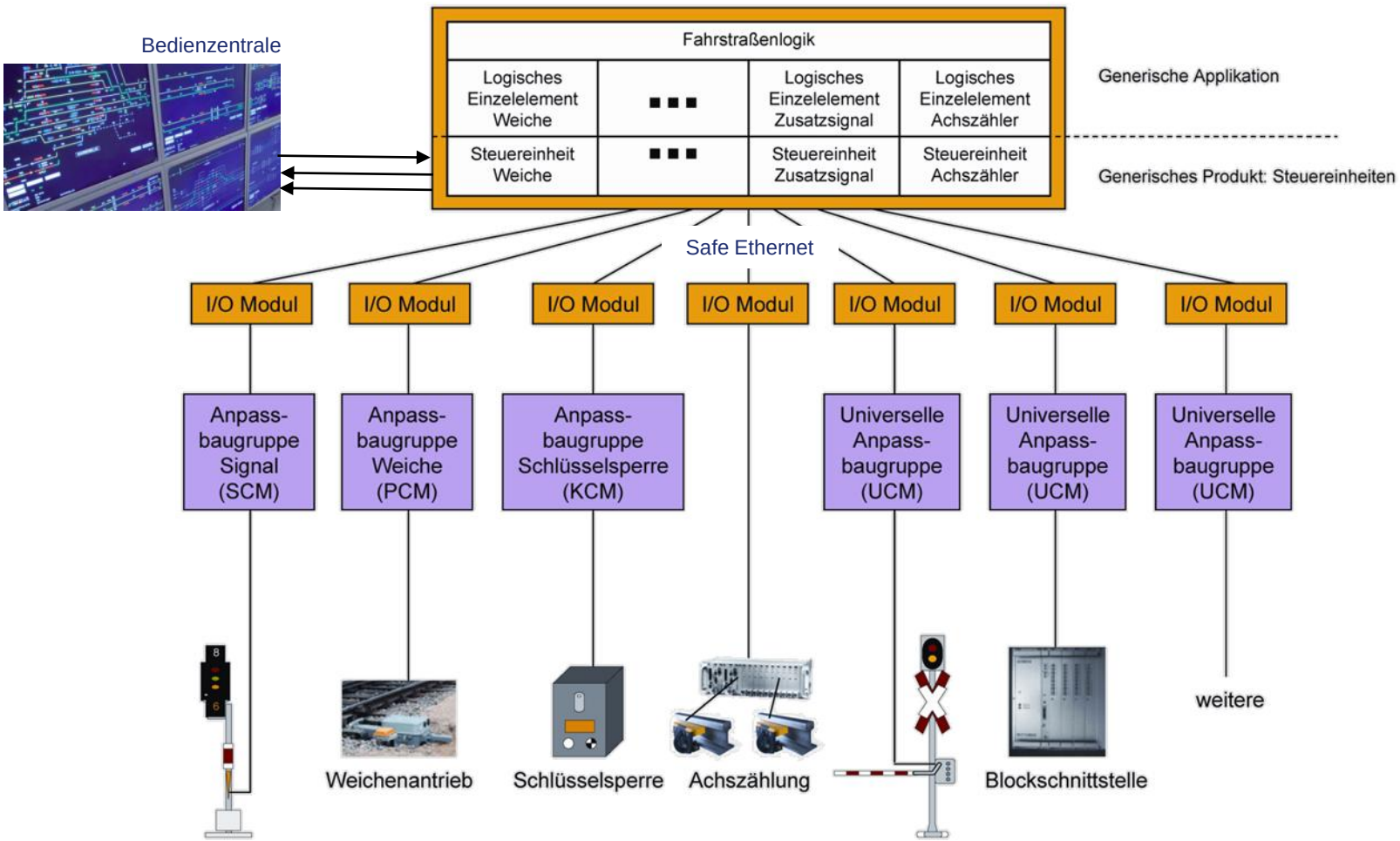
Entwicklung für Speicherprogrammierbare Steuerungen

- **Verschiedene Programmiermöglichkeiten:**
  - Grafisch: Kontaktplan, Funktionsbausteinsprache (FUP), Ablaufsprache
  - Textuell: Anweisungslisten, Strukturierter Text

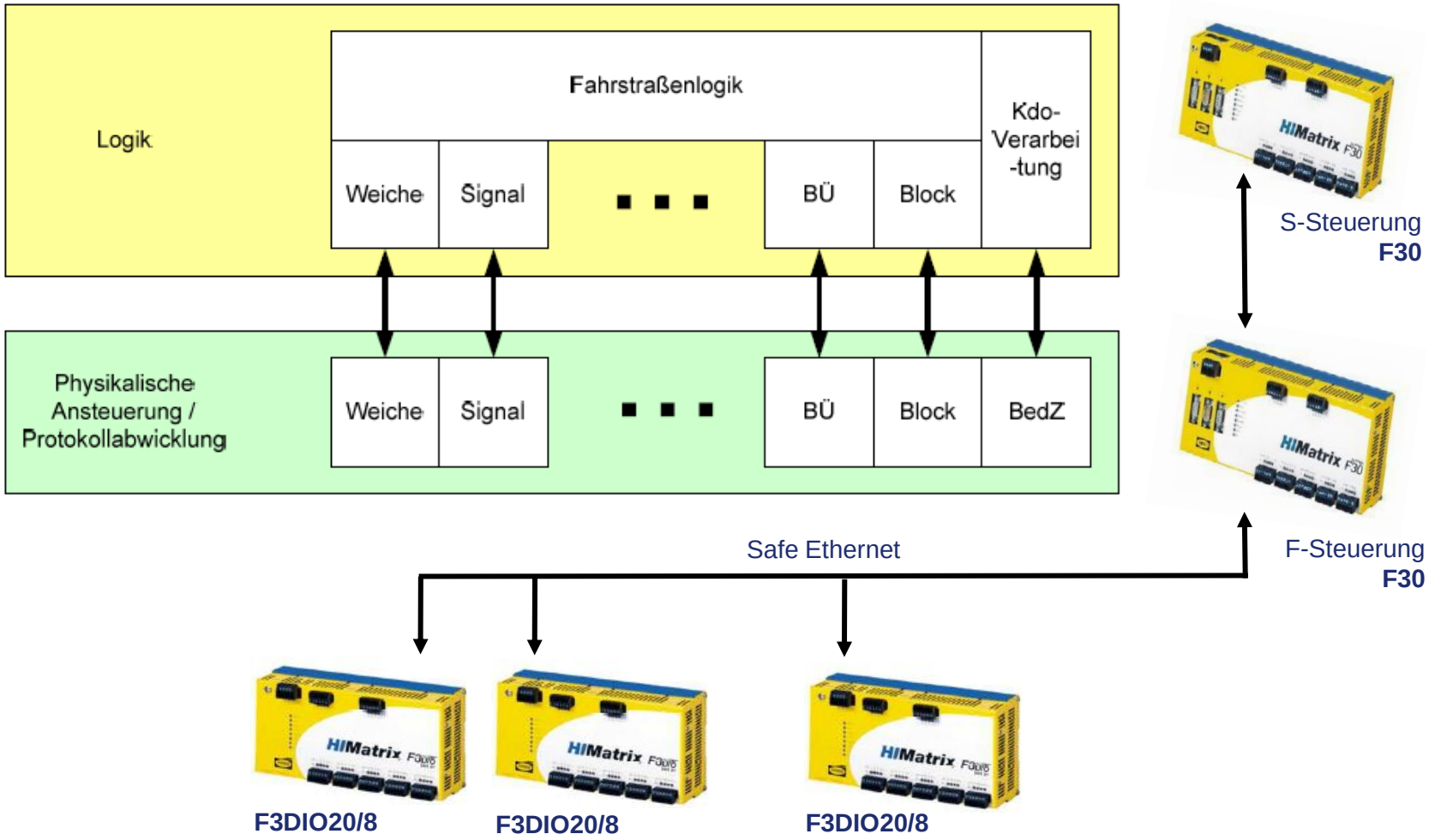
- **Eigenschaften von SPSen:**
  - Zyklische Verarbeitung: Eingabe, Verarbeitung, Ausgabe
  - Deutlich eingeschränkter Sprachumfang gegenüber herkömmlichen Programmiersprachen
  - Proprietäre Toolunterstützung



Stellwerksarchitektur

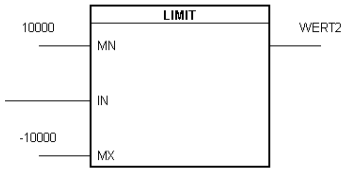


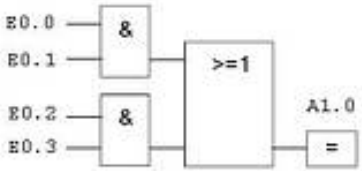
Generische Komponenten und Deployment

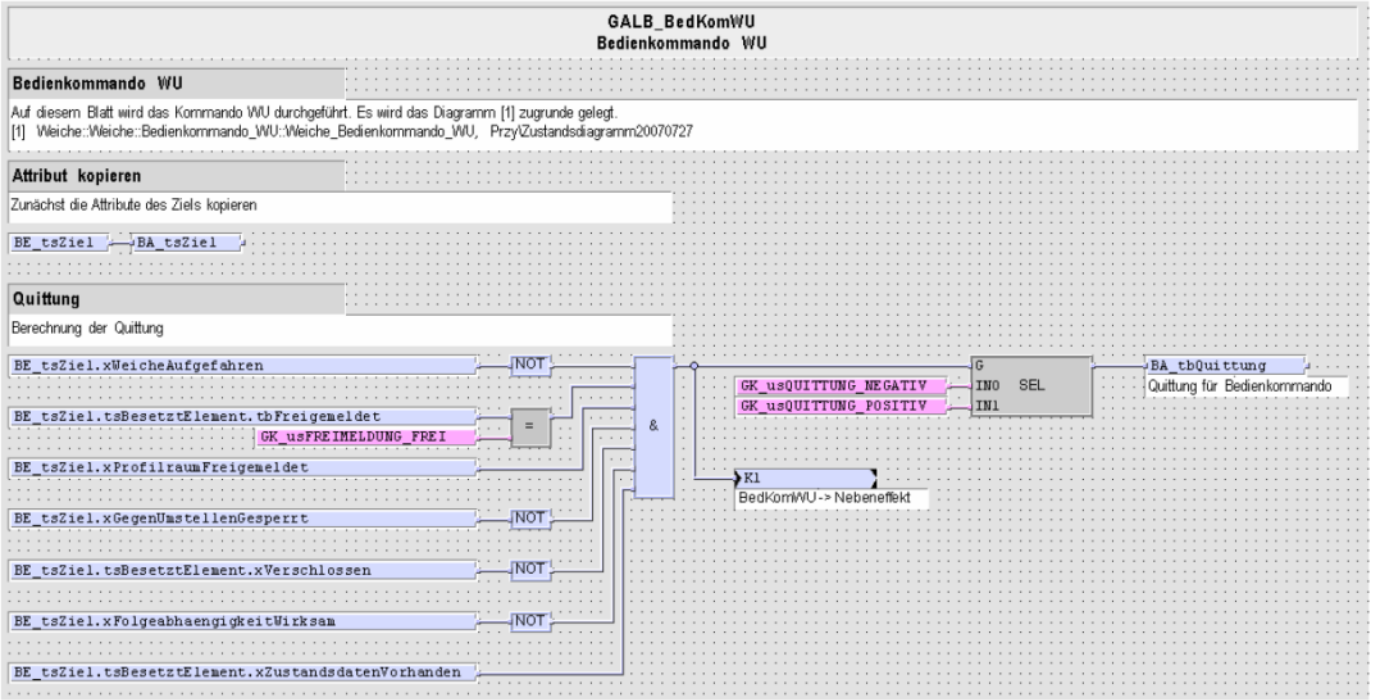


Stellwerksentwicklung (Beispiel)

Funktionsplan (FUP) am Beispiel des Werkzeugs ELOP II
graphische Vernetzung von Funktionsblöcken







Tool-Chain (Kompilation von ELOP II auf HiMatrix SPS) ist für den Bahnbereich zertifiziert und darf nicht aufgebrochen werden.

Modularisierung wird großgeschrieben

Generische Plattform (GP DE)

- Plattform für das ESTW-R in Deutschland, bestehend aus drei Komponenten:
  - Stellwerksplattform
  - Anpassbaugruppen
  - Treiber für die Anpassbaugruppen und die Bedienzentrale

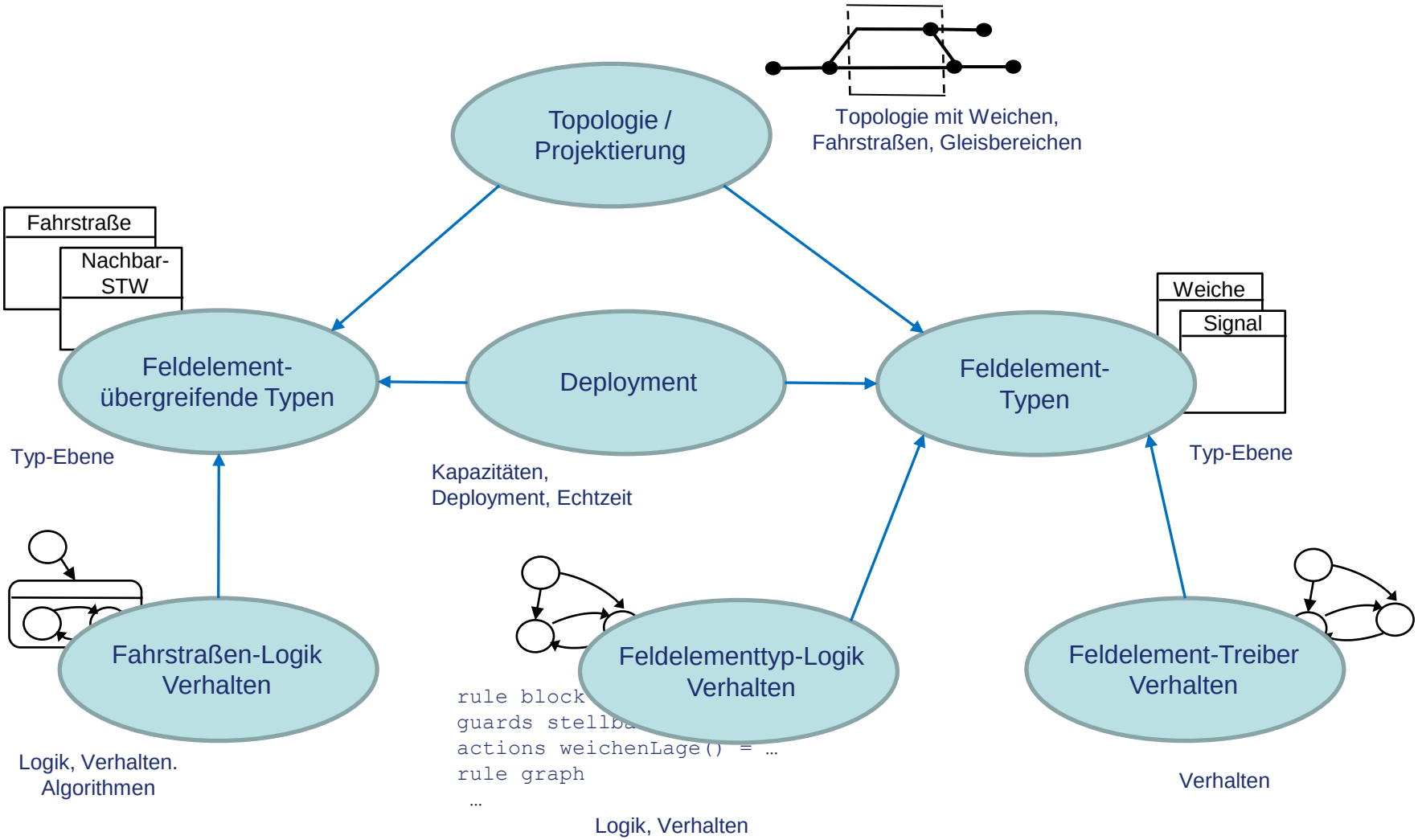
Generische Applikation ESTW-R Logik (GA-Logik)

- Funktionalität eines ESTW-R aus rein logischer Sicht

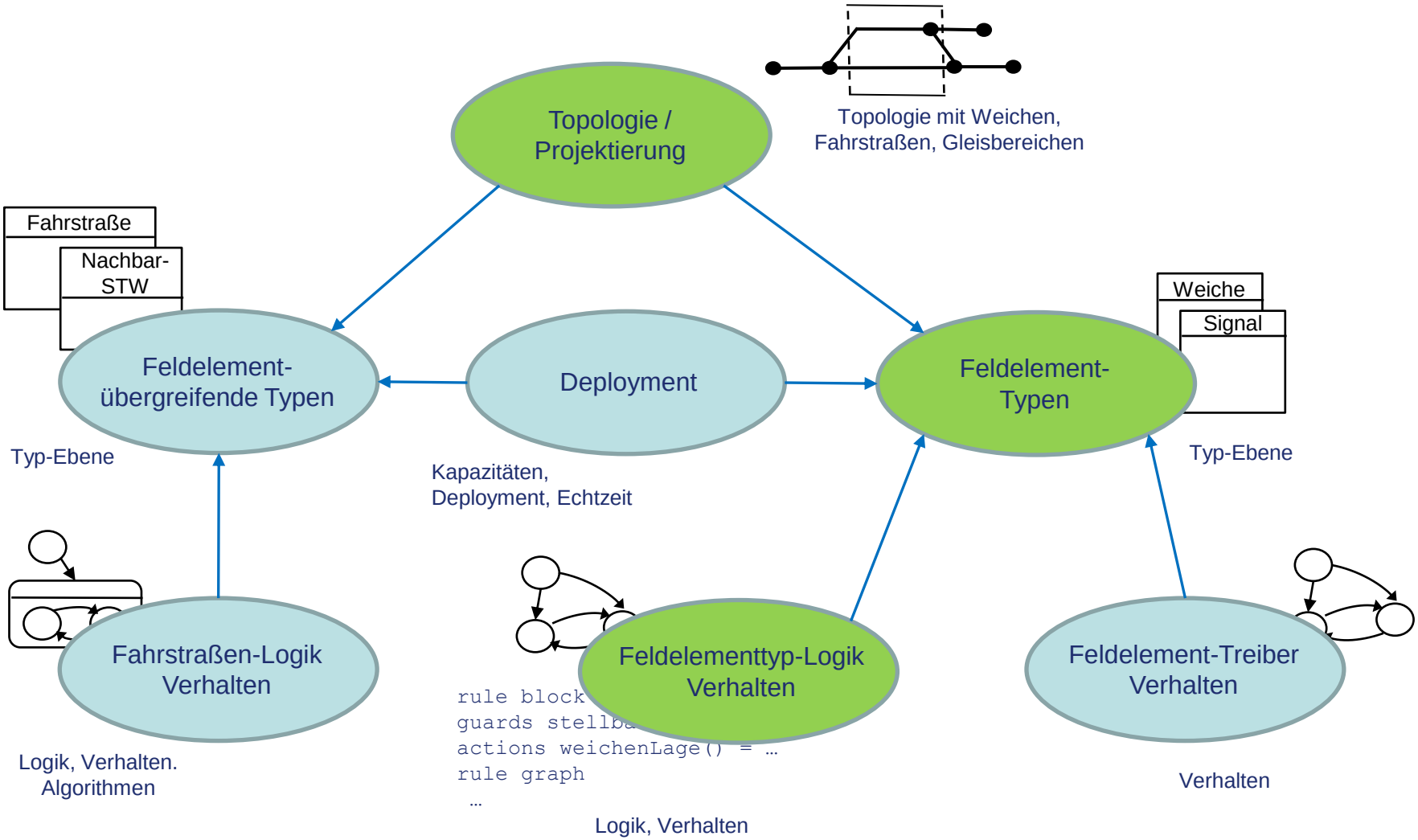
Spezifische Applikation (SA)

- Projektierung / Topologie / Fahrstraßen (konkret)

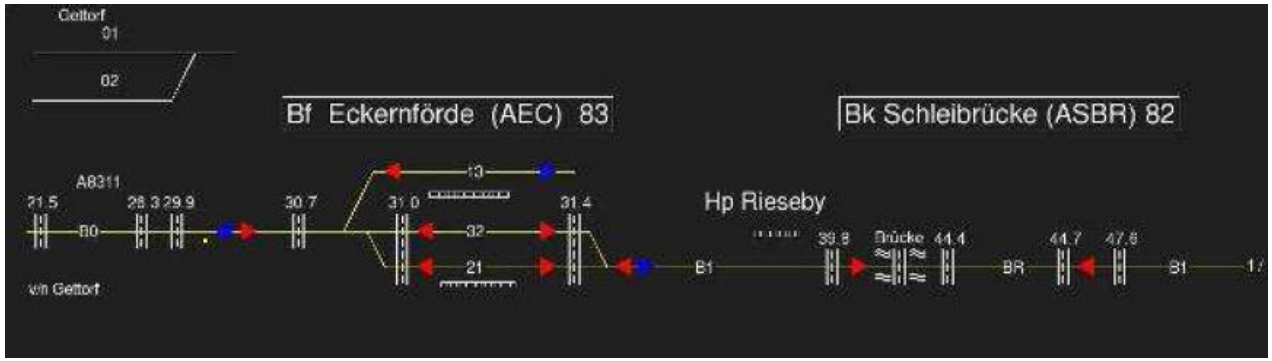
MENGES: DSL-Partitionslandkarte

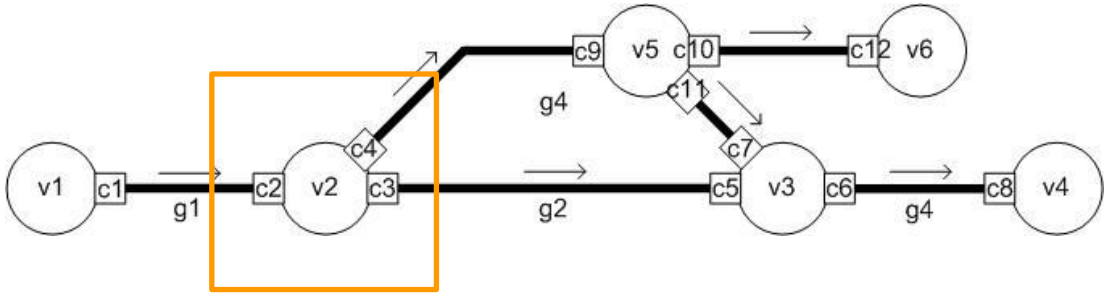


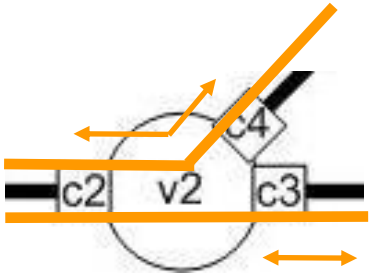
MENGES: DSL-Partitionslandkarte



Topologie / Projektierung







Feldelement-Typen

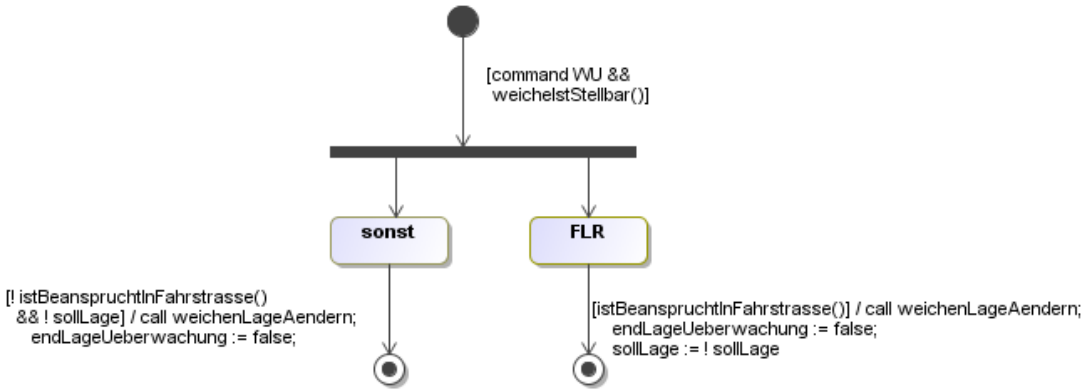
```
abstract FE Beanspruchbar {

        statevars
            beanspruchtr: (
                    nicht,          // nicht beanspruchtr
                    DWeg,           // beanspruchtr als Durchrutschweg-Element
                    FLR,            // beanspruchtr im Flankenschutzraumn
                    FWR,            // beanspruchtr im Fahrweg einer Rangierstrasse
                    FWZ,            // beanspruchtr im Fahrweg einer Zugstrasse
                    DWeg_FLR, FLR_FLR, FWR_FLR, FWZ_FLR,
                    DWeg_FLR_FLR, FWR_FLR_FLR, FWZ_FLR_FLR,
                    FWZ_DWeg
            );

        attributes
                    befahrbarkeitsSperre        : boolean;
                    reserviert                  : boolean;
                    freiMeldung                 : boolean;
                    verschluss                  : boolean;
                    zustandsDatenVorhanden      : boolean;

        predicates
                    istBeanspruchtInFahrstrasse() =
                            ((beanspruchtr != nicht && beanspruchtr != FLR)
                             && beanspruchtr != FLR_FLR);
}
```

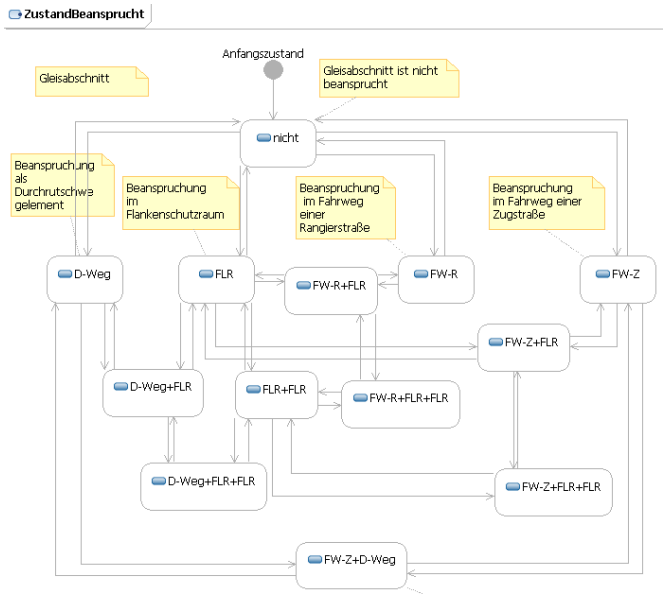
Eclipse EMF, Xtext

Verhalten (GA-Logik)

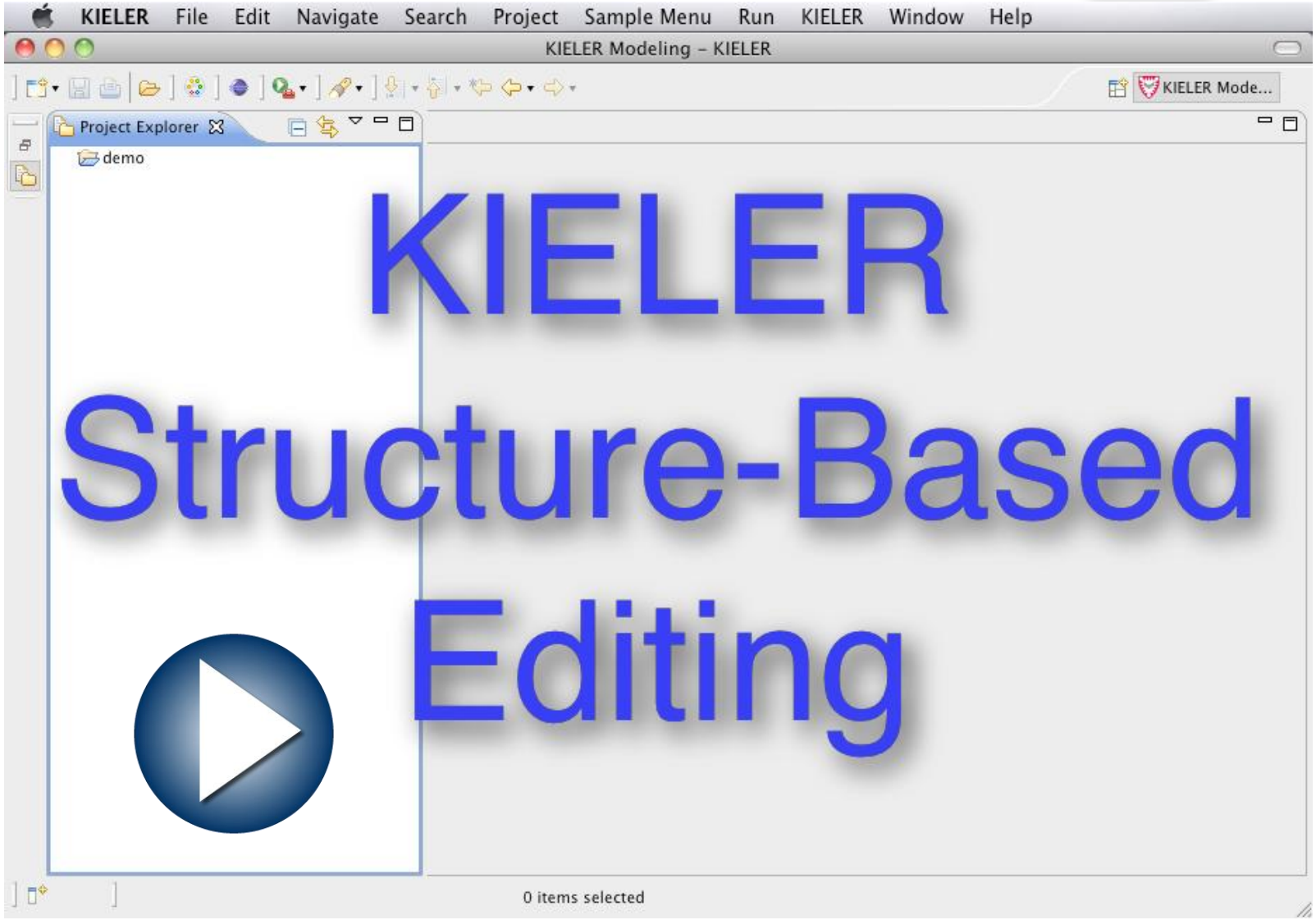
Eclipse EMF, Xtext

```
state machine Beansprucht_SM {
    references beansprucht in Beanspruchbar;
    transitions
        nicht           --> DWeg, FLR, FWR, FWZ;
        DWeg            --> nicht, DWeg_FLR, FWZ_DWeg;
        FLR             --> nicht, DWeg_FLR, FWR_FLR, FLR_FLR, FWZ_FLR;
        FWR             --> nicht, FWR_FLR;
        FWZ             --> nicht, FWZ_FLR, FWZ_DWeg;
        FLR_FLR         --> FLR, DWeg_FLR_FLR, FWZ_FLR_FLR, FWR_FLR_FLR;
        FWR_FLR         --> FLR, FWR, FWR_FLR_FLR;
        FWZ_FLR         --> FWZ, FLR, FWZ_FLR_FLR;
        DWeg_FLR        --> DWeg, FLR, DWeg_FLR_FLR;
        FWZ_DWeg        --> FWZ, DWeg;
        DWeg_FLR_FLR    --> DWeg_FLR, FLR_FLR;
        FWR_FLR_FLR     --> FWR_FLR, FLR_FLR;
        FWZ_FLR_FLR     --> FWZ_FLR, FLR_FLR;
}
```





Pragmatik: Strukturbasiertes Editieren



Ausblick

Fokus zunächst auf Domänenmodellierung

Nächste Schritte

- Codegenerierung für SPS und Simulator-Plattform
- Simulation, Profiling, Analyse, Validierung
- Tooling (Eclipse EMF, EMP; Kieker, Kieler, Netzplaneditor, …)
- Model Checking

MENGES: Projektlaufzeit von Januar 2010 bis Dezember 2012

KoSSE:

- Der Kompetenzverbund Software Systems Engineering soll nachhaltig als Informatiktransfereinrichtung etabliert werden
- KoSSE ist offen für weitere Partner und Transferprojekte