

Anforderungen an eine modellbasierte Entwicklung sicherheitskritischer Software für Stellwerkstechnik

**Siemens
Transportation Systems
TS R A D E
Ackerstraße 22
D-38126 Braunschweig
Germany**

**Dipl.-Ing. Andreas Morawe
Andreas.Morawe@Siemens.com**

**Dr. Hans-Jürgen Nollau
Hans-Juergen.Nollau@Siemens.com**

**B.Sc. Murat Şahingöz
Murat.Sahingoez@TS.Siemens.de**

Übersicht

- Anforderungen
- Software-Entwicklungsprozess
- Modellbasierter Entwurf: Projektstand und -erfahrungen
- Anforderungen an modellbasierte Entwicklungsmethoden
- Arbeitsstand und Vorhaben

Anforderungen im Projekt: Aufgaben SIMIS® D

SIMIS® D für den Einsatz bei der Deutschen Bahn AG für komplexe und große Bahnhöfe mit hohen Anforderungen an Sicherheit und Verfügbarkeit und hohen betrieblichen Belastungen

Abgeschlossene Projekte Vorgängerbauform SIMIS® C:

- Hannover Hauptbahnhof
- Dresden Hauptbahnhof
- Knoten Magdeburg
- S-Bahn-Stammstrecke München (Fahrt im 120-Sekunden-Takt)

Laufendes Projekt SIMIS® C:

- Frankfurt/Main Hauptbahnhof

Anforderungen im Projekt: Einordnung der Stellwerkslogik

Leittechnik

Bedienung und Anzeige, Zuglenkung,
Zugnummernmeldung, Diagnose, ...

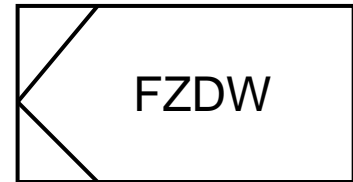
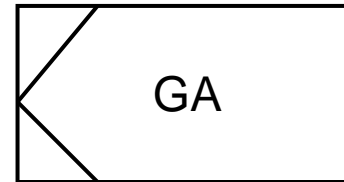
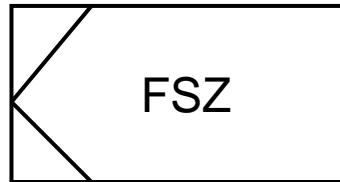
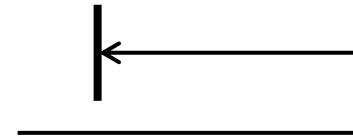
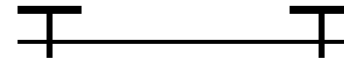
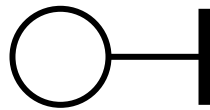
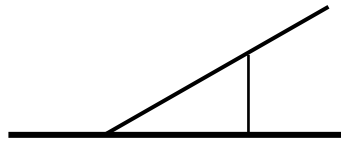
Stellwerkslogik

Gewährleisten der Signalabhängigkeit, Bilden der
Signalbegriffe, Steuern und Überwachen der Außen-
anlagen, Bilden und Auflösen der Fahrstraßen

Komponenten
der
Außenanlage

Weichen, Kreuzungen, Signale, Bahnübergänge,
Gleisfreimeldeabschnitte, Schnittstellen zu
Nachbarstellwerken, Blocktechnik, ...

Entwicklungsprozess: Definieren von Elementarten



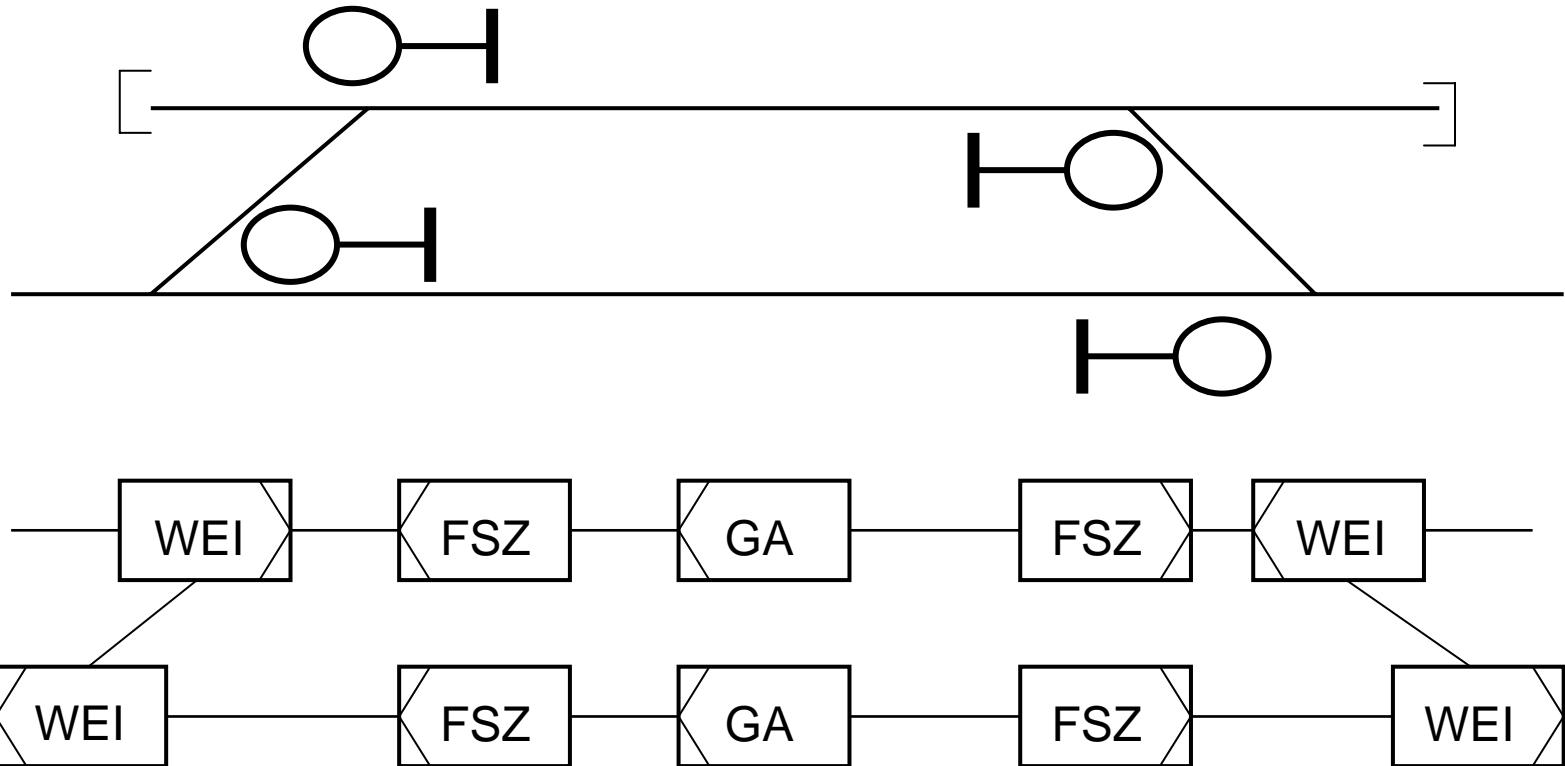
Einfache
Weiche

Fahrwegelement
Start/Ziel

Gleis-
abschnitt

Fahrwegelement
Ziel/Durchrutschweg

Entwicklungsprozess: Bilden von Objektinstanzen



Entwicklungsprozess: Umfang der Steuerungsaufgabe

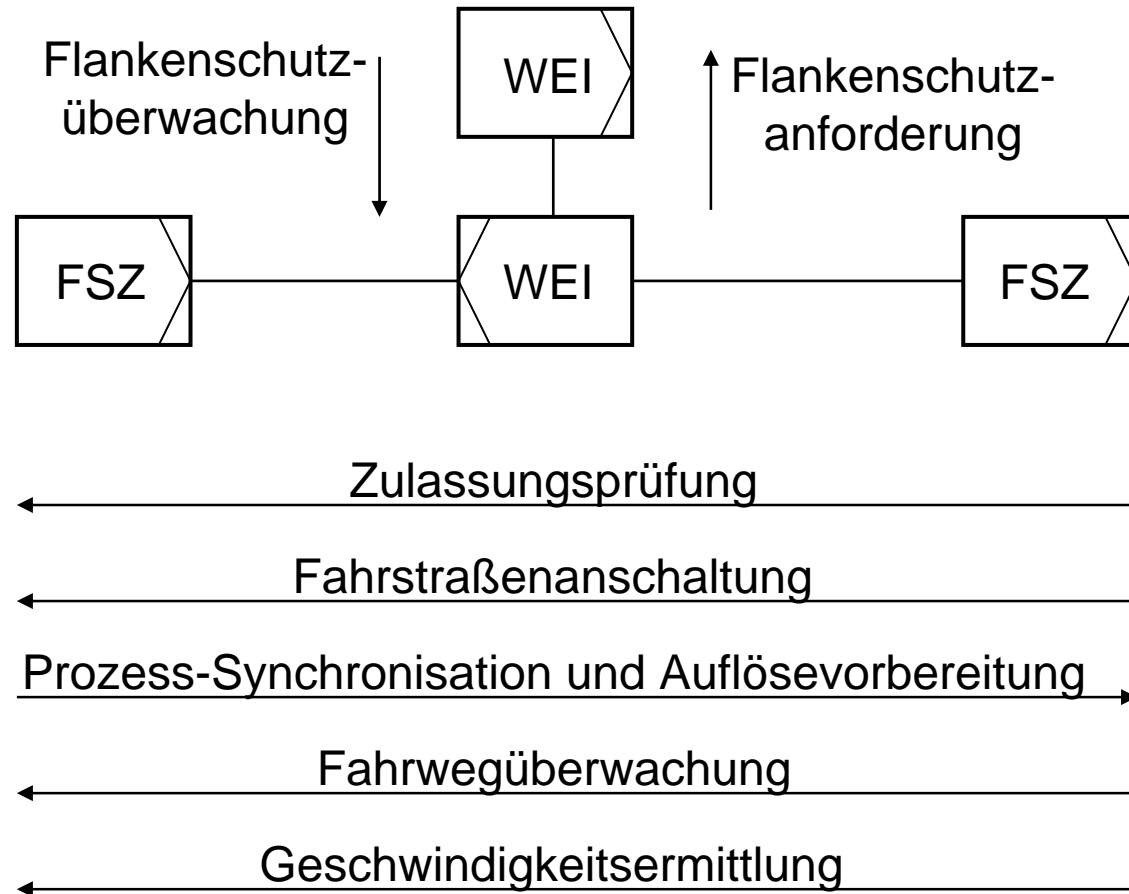
Die Komplexität der Steuerungsaufgabe wird weniger bestimmt durch folgende statistische Aussagen:

- Anzahl der Elementarten für Basislösung: 32
- Anzahl der Empfangsmethoden für Basislösung: 2300
- Anzahl der Telegrammarten für Basislösung: 450
- Anzahl der Stelleinheiten in Frankfurt/Main Hauptbahnhof: 1300

Die Komplexität der Steuerungsaufgabe wird vielmehr bestimmt durch die komplexe Kommunikation der Elemente.

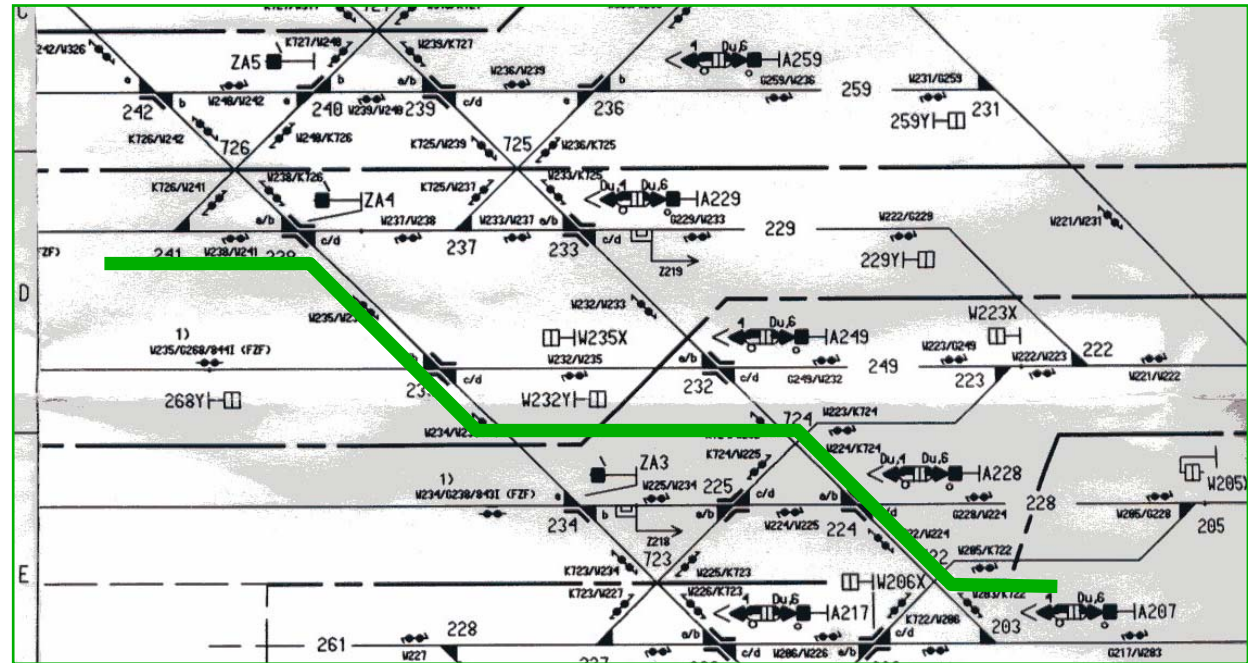
Entwicklungsprozess: Komplexität der Kommunikation (1)

Einfache Steuerungsaufgabe



Entwicklungsprozess: Komplexität der Kommunikation (2)

Reales Projekt



Projektstand und -erfahrungen (1)

Mit welchen Methoden und Werkzeugen versuchen wir, die Anforderungen an den Entwicklungsprozess zu erfüllen?

Projektstand und -erfahrungen (1)

Werkzeug
GRACE-FST

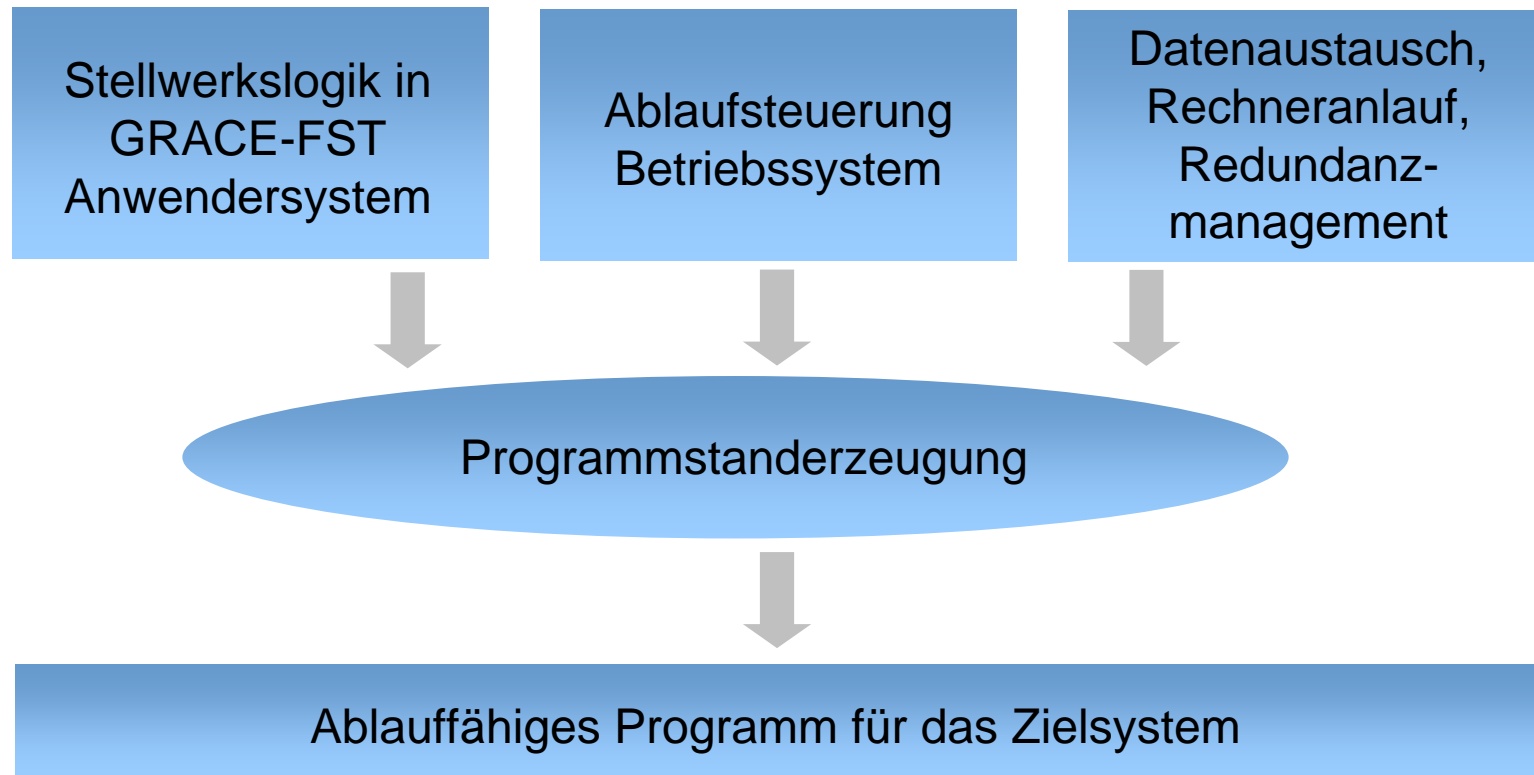
The screenshot displays two windows from the GRACE-FST software:

- Top Window: GRACE-FST Deklaration ESTWS_DB (read-only)**
 - Buttons: Betriebsordnung, Ansicht, Bearbeiten, Prüfen, Hilfe
 - Field: ESTWS_DB
 - Buttons: Zuweisen, Löschen, Öffnen
 - Field: K:\ACC\Anwender\Anwendung\...\A0000001.DOC
 - Field: Kommentar
 - Tree View (Right):
 - Betriebsordnung
 - Beschreibung
 - Telegrammanalysen
 - Telegrammketten
 - Telegramme
 - Parameter
 - Nutzerdatentypen
 - SubSEC-Schablonen
 - Funktions-Schablonen
 - Übergabevariablen
- Bottom Window: GRACE-FST Deklaration ESTWS_DB - WEI (read-only)**
 - Buttons: Elementtyp, Bearbeiten, Prüfen, Hilfe
 - Field: WEI
 - Buttons: Zuweisen, Löschen, Öffnen
 - Field: K:\ACC\Anwender\Anwendung\...\A4001001.doc
 - Field: Kommentar
 - Text Area:
 - Weichenelement
 - Dient zum Steuern und Überwachen von Weichen (einfache Weichen, DKW, EKW; nicht für Gleissperren) im Bahnhof.
 - WEI-Elemente sind Gegenstand der elementweisen Fahrstraßenhilfsauflösung oder elementweisen Fahrstraßenrücknahme sowie der Flankenschutzbearbeitung.
 - Tree View (Right):
 - Beschreibung
 - Telegrammports
 - Variablen
 - Konstanten
 - Projektierung
 - Triggervariablen
 - SubSEC
 - Funktionen
 - interne Telegramme
 - Telegrammpfade
 - SEC-Grafiken

Graphical Requirement Analysis
and design method in a CENELEC
based Engineering process –
Functional Specification Tool

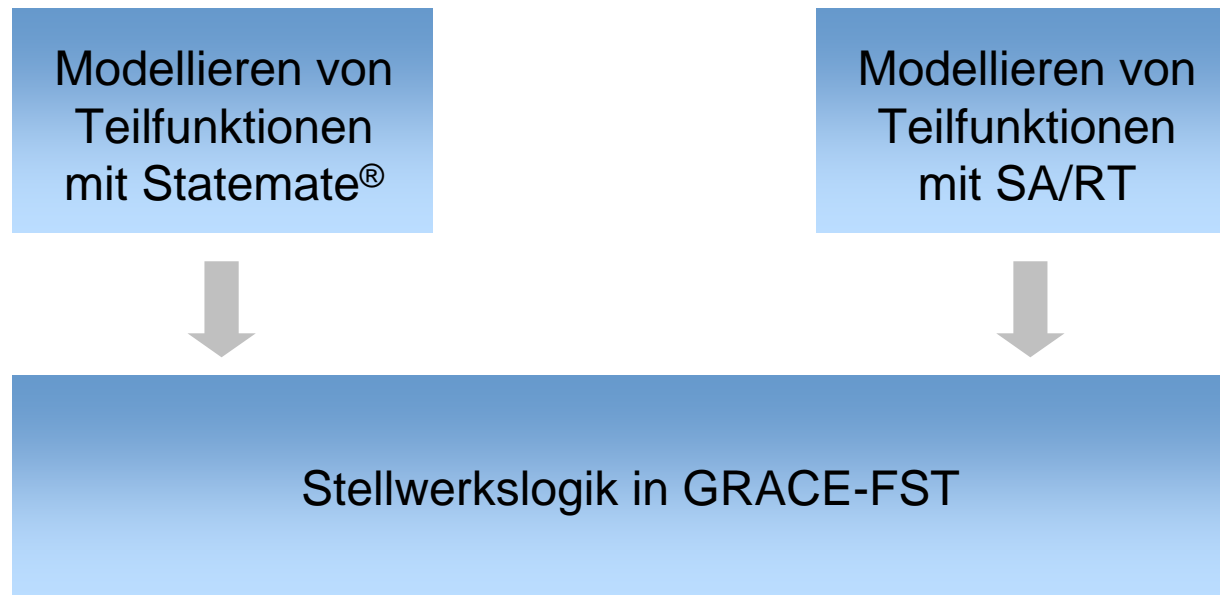
Projektstand und -erfahrungen (2)

Automatisiertes Überführen in das Zielsystem



Projektstand und -erfahrungen (3)

Abstraktion der Stellwerksfunktionen



SA/RT Structured Analysis with Realtime Extensions

Projektstand und -erfahrungen (4)

Einsatzmöglichkeiten modellbasierter Methoden im Projekt bei Design, Verifikation und Validierung

- Anfertigen verschiedener Sichten auf die Stellwerkslogik (Automat, Sequenzdiagramme, ...)
- Visualisieren der Funktionen verschiedener Lageplanfälle
- „Rapid Prototyping“ mit iterativer Entscheidungsfindung und Erweiterung bis zur zulassungsfähigen Lösung
- Generieren von Testfällen
- Diagnose bei Fehlfunktionen
- Unterstützen von Verfahren der formalen Verifikation

Projektstand und -erfahrungen (5)

Besondere Anforderungen generischer Systeme

Modell (Zustandsmodell, Sequenzdiagramm, ...)
des Lageplanfalls

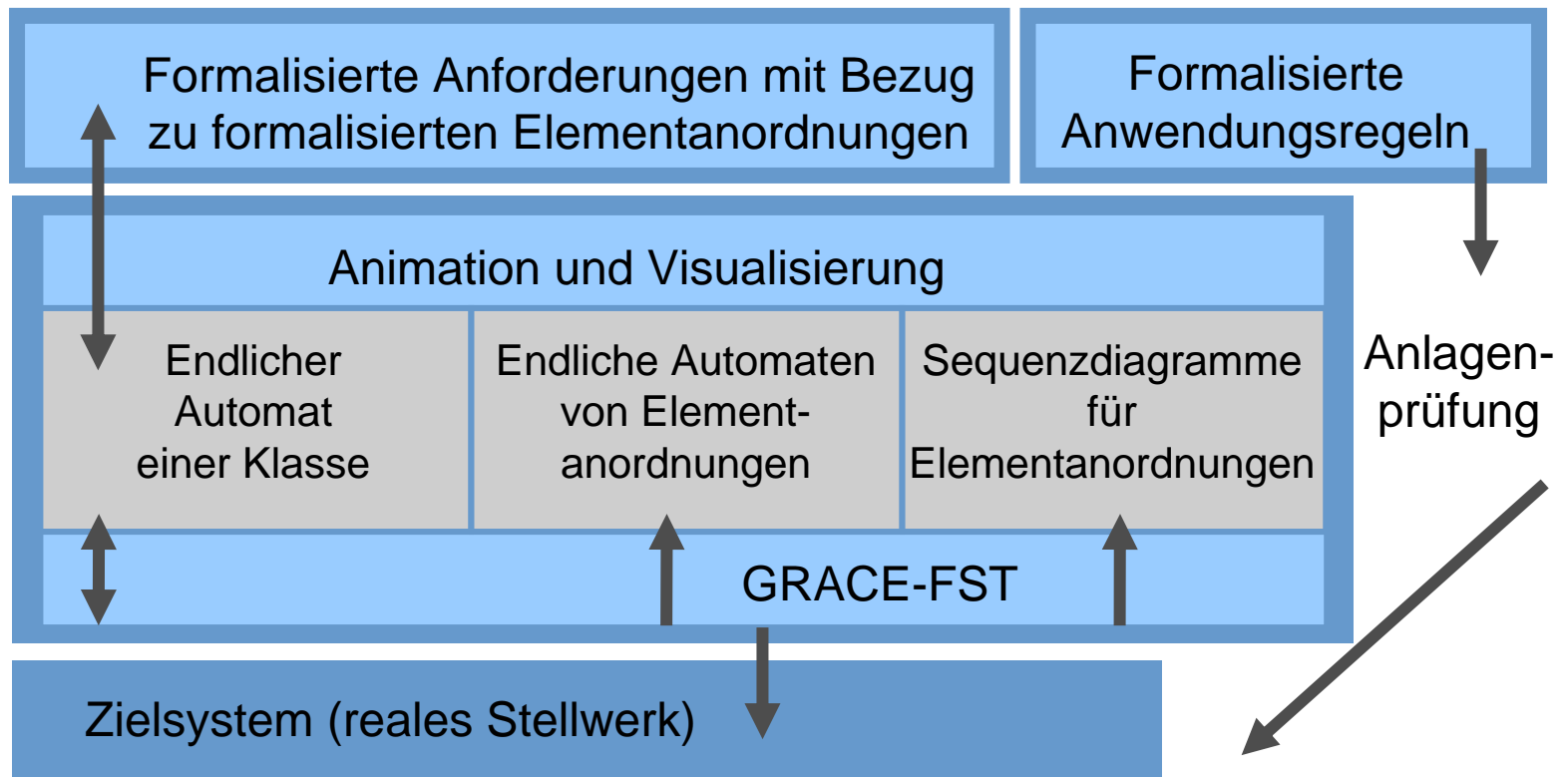
Lageplanfall

A diagram illustrating a layout plan case (Lageplanfall). It shows two parallel horizontal lines on the left that converge towards a central vertical line. From this central vertical line, a single horizontal line extends to the right. This represents a transition from two parallel paths to a single path.

Stellwerkslogik in GRACE-FST

Projektstand und -erfahrungen (6)

Vision für Werkzeugentwicklungen



Anforderungen an modellbasierte Entwicklungsmethoden (1)

Anforderungen aus technischer Sicht

- Kein substanzielles Verändern der domänenspezialisierten Werkzeuge (GRACE-FST)
- Abbilden komplexer System in verschiedenen Sichten (Automat, Sequenzdiagramm, ...) mit stabilen, funktionalen Werkzeugen
- Unterstützen von „Rapid Prototyping“ und iterativer Entwicklung

Anforderungen an modellbasierte Entwicklungsmethoden (2)

Weitere Anforderungen aus technischer Sicht

- Methodische Schnittstellen (temporale Logik, Prädikatenlogik u. ä. interessant, aber nicht vermittelbar)
- Unterstützen generischer Systeme (Automatenmodelle, Sequenzdiagramme u. ä. von Lageplanfällen)
- Schnittstellen zu einer methodischen Anforderungsbeschreibungssprache mit Möglichkeit der Testfallgenerierung

Anforderungen an modellbasierte Entwicklungsmethoden (3)

Anforderungen aus wirtschaftlicher Sicht

- Stabilität und Intuitivität der Werkzeuge
- Rückfluss von Investitionen in Methodenentwicklung und Werkzeugentwicklungen/-adaptionen innerhalb der üblichen Entwicklungszeiträume für Weiterentwicklungen der Stellwerkslogik (Erfahrungswert: drei Jahre)
- Kosten für Methodenentwicklung und Werkzeugentwicklungen/-adaptionen in begründbarem Verhältnis zu den übrigen Entwicklungsaufwendungen

Arbeitsstand und Vorhaben: Abgeschlossene Aktivitäten

- Hochstabiles Werkzeug GRACE-FST zum Design der Stellwerkslogik, automatisiertes Überführen der Design-Ergebnisse in das Zielsystem
- Leicht auswertbare Schnittstelle für diverse stabile Verifikationswerkzeuge
- Kern von Mitarbeitern zum Abdecken der gesamten Entwicklungskette
- Testwerkzeuge zum Absichern der vollständigen Regressionsfähigkeit von Black-Box- und Grey-Box-Tests
- Stabiler Entwicklungsprozess

Arbeitsstand und Vorhaben: Laufende Aktivitäten

- Weiterentwickeln von Werkzeugen zur Verifikation der Stellwerkslogik
- Einleiten erster Schritte in Richtung Änderungsauswirkungsanalyse
- Formales Beschreiben der Lageplanstrukturen
- Optimieren des Änderungsmanagements

Arbeitsstand und Vorhaben: Weiteres Vorgehen

- Herstellen von Schnittstellen zu abstrakteren Beschreibungsmitteln für Lageplanfälle
- Definieren von Funktionsanforderungen mit formalen Ansprüchen, um automatisch Testfälle und Testumgebungen zu generieren
- Rationalisieren der Anlagenprüfung

Literatur

- [1] DIN EN 50128: Bahnanwendungen – Telekommunikations-technik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme, 2001
- [2] B. Jung: Die Methode und Werkzeuge GRACE, Vortrag anlässlich der Tagung FORMS2000, Braunschweig 2000, http://www.ifra.ing.tu-bs.de/forms/aktuell/workshops/2000/forms_2000.html
- [3] C. Trog / L. Eriksson: Spezifikation von Stellwerkslogik mit formalen Methoden, SIGNAL+DRAHT, Heft 1+2/2004
- [4] A. Rech: Transformation von Stellwerkslogiken in die Eingabesprache eines Model Checkers, TU Braunschweig, 2004
- [5] M. Sahingöz: Analyse der Testmethodik für die Betriebsordnung von Stellwerken der Siemens, Siemens AG, 2004