Der Softwarebug von HH Altona

Berühmt-berüchtigte Softwarefehler

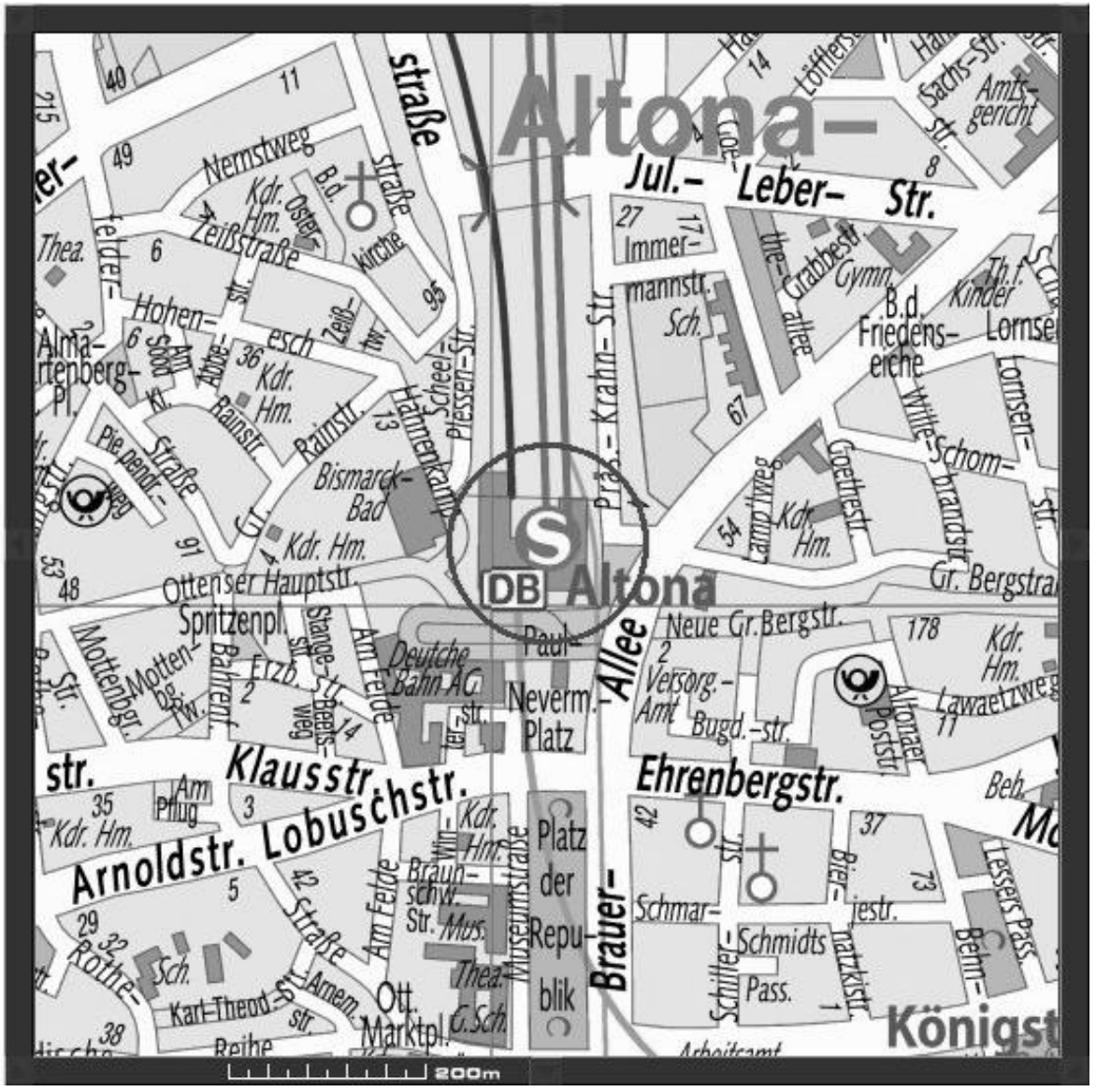
Matthias Bertram
berti@uni-koblenz.de

Universität Koblenz-Landau

Bahnhof Altona (1)

- jetzige Lage seit 1893
- mitten im Stadtgebiet
- historisch gewachsene Strukturen
- Kopfbahnhof
  - Züge können nur aus einer Richtung in den Bahnhof fahren

Bahnhof Altona (2)



Bahnhof Altona (3)

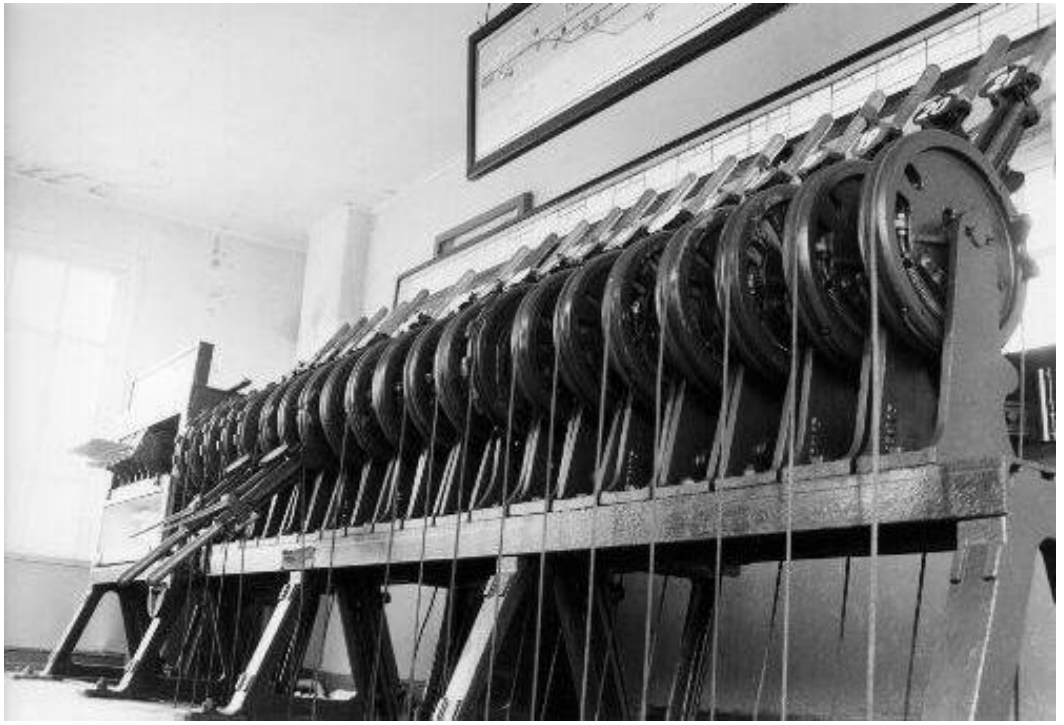
- Nähe Hamburger Hafen $\Rightarrow$ erhöter Güterverkehr
- nationaler und internationaler Verkehrsknotenpunkt
- ca. 900 Züge tgl.
- zw. 50000 und 100000 Passagieren
- enormes Rangieraufkommen und Betriebsbedingungen

Definition Stellwerk

Der Brockhaus definiert ein Stellwerk als:

> „... Teil der Eisenbahnsignalanlagen zum **Steuern und Sichern** des Zug- und Rangierbetriebs auf Betriebsstellen mit mehreren Gleisen, ... “

Hebelstellwerk (seit 1856)

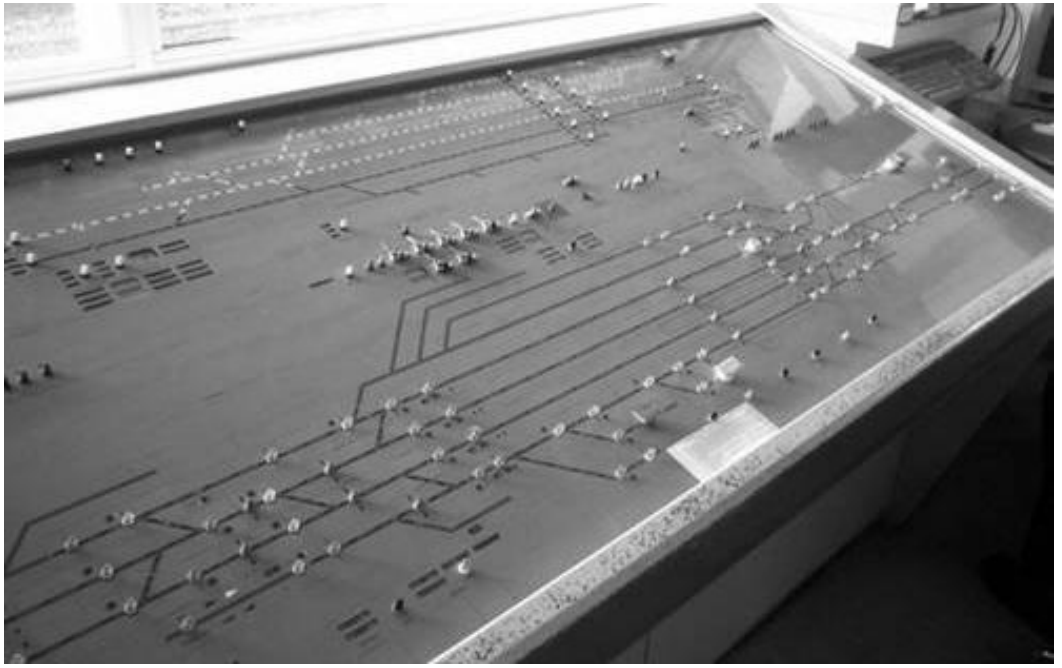


- Hebel stellen die Weichen und Signale z.B. über Seilzüge oder Gestänge
- einfache Fahrstrassensicherung durch Kaskadenstellwerken

elek.-mech. Stellwerk (seit 1896)

- Weichen und Signale werden über Motoren gestellt
- Vereinfachung der Bedienung
- Schalter statt Hebel

Gleisbildstellwerk (seit 1948)



- Gleisbildtisch bildet die Gleisanlagen nach
- Steuerung erfolgt über Relais
- aufwendige Mechanik fällt weg

Das alte System

- sieben alte Anlagen aus den Jahren 1911-1952
  - Hebelstellwerk
  - Gleisbilder, sollten die Arbeit erleichtern
- 50 Mitarbeiter waren mit der Steuerung beschäftigt
- dadurch nicht mehr zeitgemäß und rational

$\Rightarrow$ Umstellung auf elektronisches Stellwerksystem

Definition elektr. Stellwerk

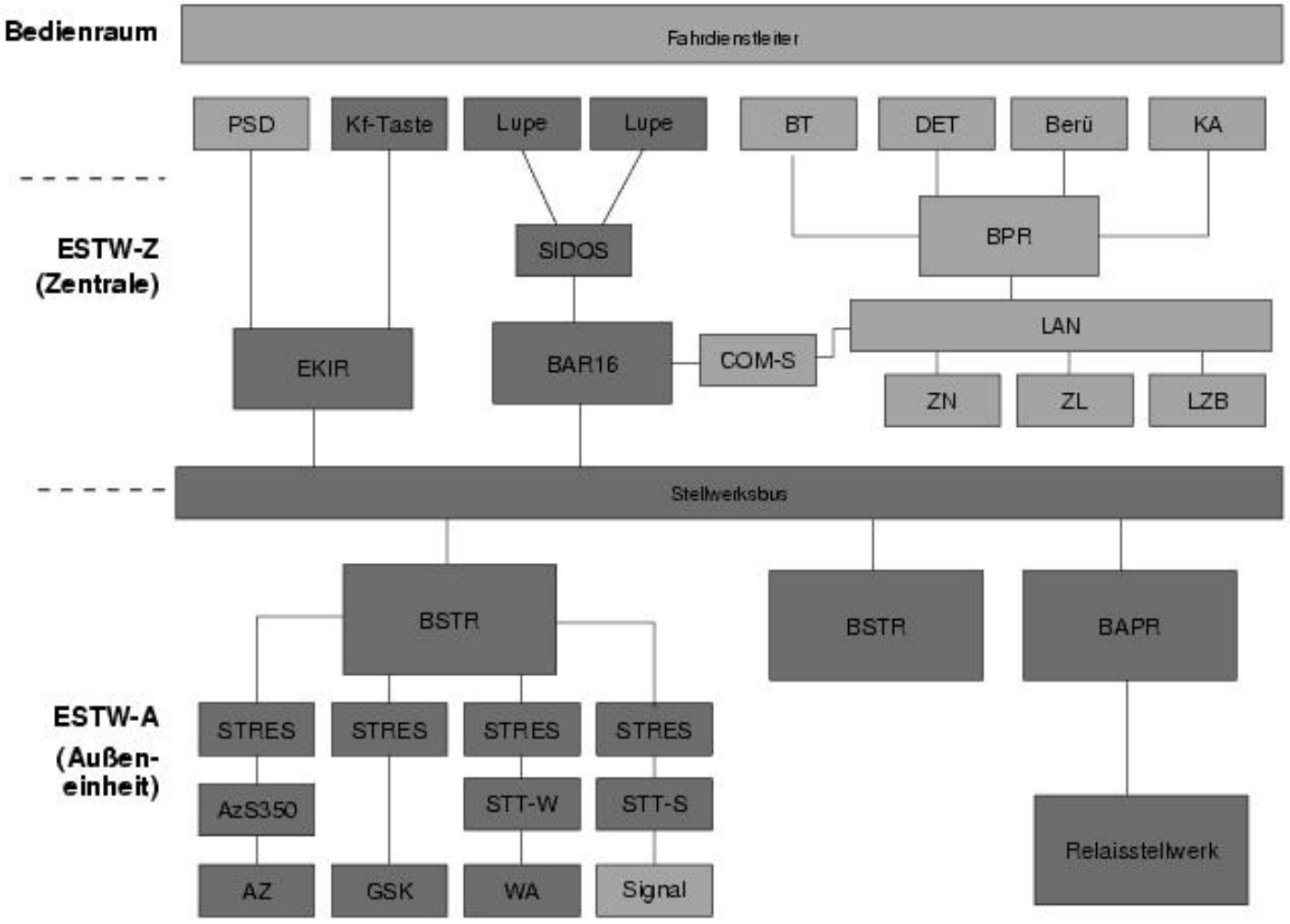
Ein elektronisches Stellwerk ist die Hard- und Software, die:

- die sicherungstechnischen Abhängigkeiten realisiert
- Schnittstellen für die zu steuernden Elemente und für Techniken, die das EStW beeinflussen oder von ihm beeinflusst werden, bereitstellt
- die unter den ersten beiden Punkten genannten Funktionen technisch verwaltet und sichert

Historie des EStW

- Entwicklung seit 1983
- erstes System 1986 in Murnau
- nach 2-jähriger Testphase wurde das EStW vom EBA abgenommen

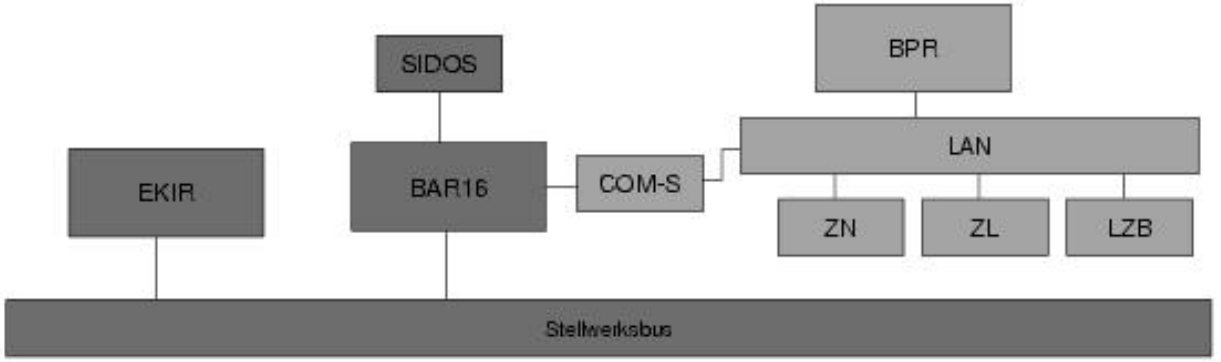
Das neue System



Bedienraum

- PSD : Protokoll- und Störungsdrucker
- Kf-Taste : zur Bestätigung kritischer Kommandos
- Lupe : zeigt Details eines Ausschnitts des Stellbereichs
- BT : Bedientablett
- KA : Kommunikationsanzeige
- BERÜ : Bereichsübersicht

Zentralrechnerraum



BPR:

- setzt den Befehlstext des Fahrdienstleiters zusammen
- schickt diesen über COM-Server an den BAR16

EKIR:

- Steuerung des PSD
- wieder in der Zukunft komplett durch BAR16 ersetzt

BAR16

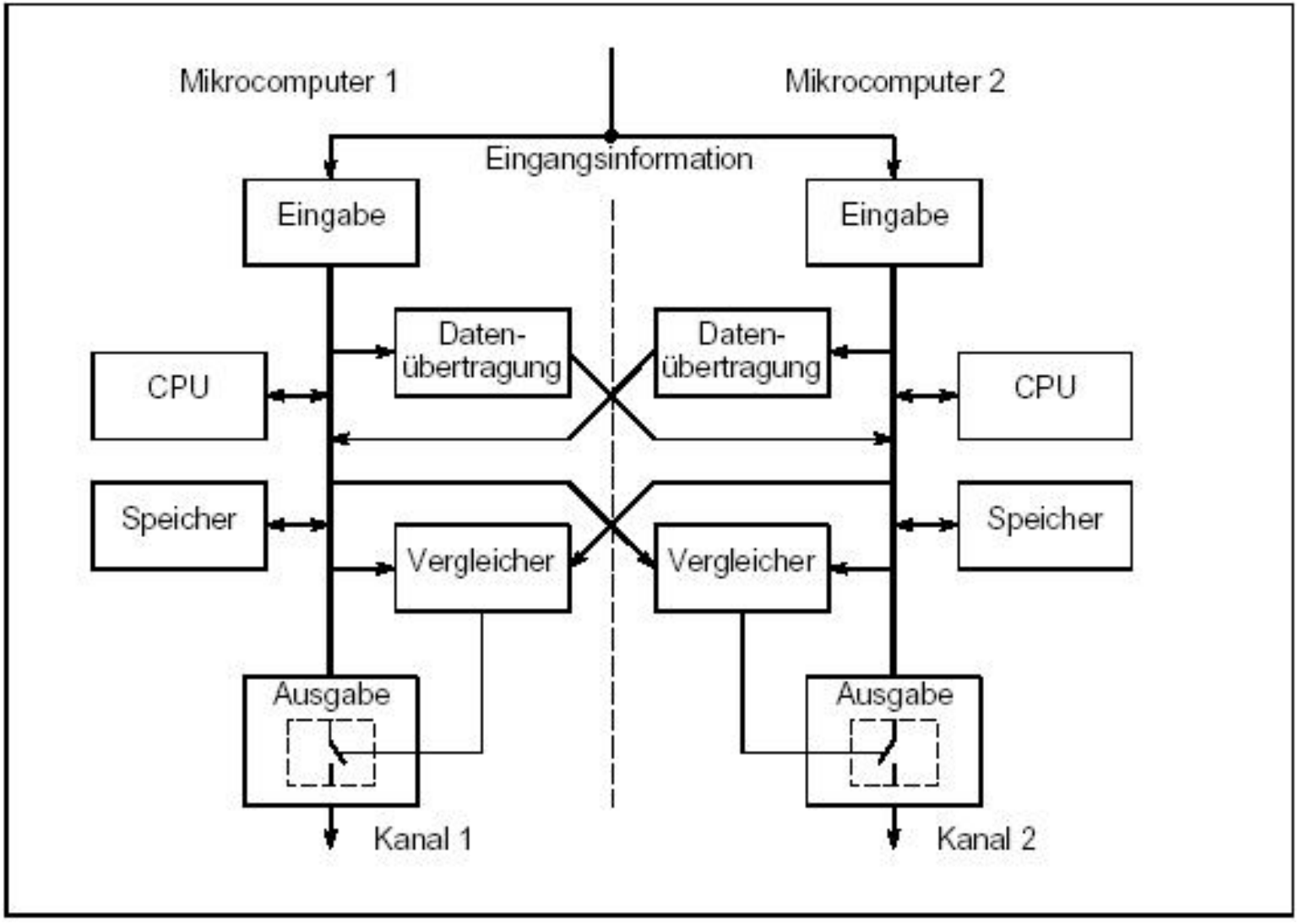
- der zentrale Rechner im ganzen System
- Aufbau nach SIMIS-Prinzip mit zwei INTEL-486/25 Rechnern
- Auswertung und Verarbeitung der vom BPR empfangenen Daten
- erzeugt Videosignale für Lupenbildschirme

Das SIMIS - Prinzip

Sicheres **Mi**crocomputersystem von **S**IEMENS:

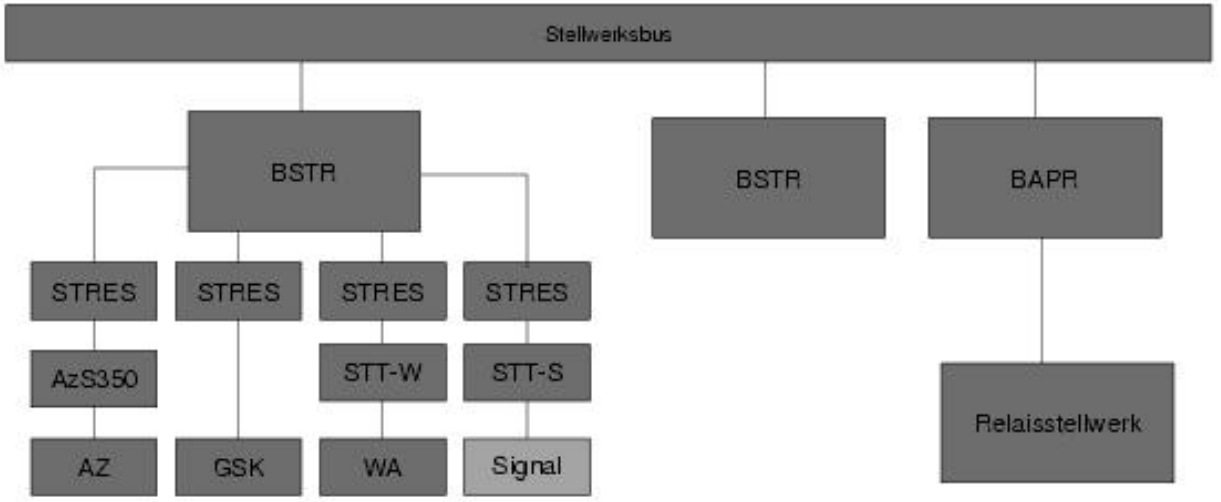
- zwei oder drei Rechner arbeiten parallel
- Ergebnisse werden hardwaremäßig verglichen
- nur bei gleichem Ergebnis beider Rechner werden erarbeitete Befehle ausgegeben

2v2-Konfiguration



Welche Probleme können hierbei auftreten?

Bereichsrechnerraum



BSTR:

- Bereichsrechner empfängt Kommandos von BAR16, setzt sich mit anderen Bereichsrechnern darüber auseinander und gibt Kommandos an Stellrechner
- Stellrechner steuert die entsprechenden Steuer-Relais an

Vorteile laut SIEMENS

- Technik ist anpassungsfähig, für kleine und grosse Bahnhöfe
- Technik ist erweiterungsfähig
- geringer Raum- und Personalbedarf
- schließt menschliche Fehlbedienung nahezu aus
- bietet ergonomisch gestalteten Arbeitsplatz

Kosten

- an dem EStW in Altona wurde über 1 Jahr gearbeitet
- insgesamt arbeiteten zeitweise 1000 Siemens und Bahnmitarbeiter an dem Projekt
- von den 62,5 Mio. DM Gesamtkosten gingen 2/3 an Siemens

Der Fehlertag

- Bahnhof zur Inbetriebnahme gesperrt
- nach der Inbetriebnahme kam es gegen 5:00 Uhr zu einer Sicherheitsabschaltung und alle Signale wurden auf Rot gestellt
- zwei weitere folgten
- Reboot dauerte jeweils 10 Minuten

Die Fehlersuche

- da es keine Möglichkeit zur manuellen Steuerung gab, wurde der Bahnhof, für den Personenverkehr zu sperren
- bis zur Reproduktion, im Siemens Testcenter in Braunschweig, dauerte es knapp einen Tag
- danach musste das EBA die Änderungen absegnen

Der Fehler

- BAR16 verfügte über einen STACK von max. 3,5 KB
- bereits bei normalem Berufsverkehr kam es zu einen Überlauf
- die falsch programmierte Fehlerroutine führte in Endlos-Schleife
- das führte dazu das sich das System, sicherheitshalber, abschaltete

Die Lösung

- der STACK wurde auf 4,0 KB erhöht
- die Fehlerroutine wurde überarbeitet
- 2 Tage nach erstem Auftritt konnte das, überarbeitete, System in Betrieb genommen werden

Auswirkungen

- Passagiere nach Altona musste mit der S-Bahn von Pinneberg und Harburg fahren
- Fernreiseverkehr wurde um Altona herumgelenkt
  - Verspätungen bis zu 40 min.
- jeder fünfte Fernreisezug in ganz Deutschland hatte zu dieser Zeit Verspätung

Fehler bei SIEMENS

- das System war zwar gegen alle möglichen Hardwareausfälle geschützt, jedoch wurden Maßnahmen bei Softwareproblemen vernachlässigt
- bei der Programmierung wurde teilweise nicht sorgfälltig vorgegangen
- es wurden nicht genügend Test gemacht, besonders beim BAR16 der komplette eine Neuentwicklung war

Fehler der Bahn

- generelle Probleme im Management
  - zu kurze Einführungsphase
  - keine Alternativen bei Problemen
  - übermäßiges Vertrauen in Computer
- die Mitarbeiter waren nicht ausreichend am neuen System ausgebildet, und in der ersten Woche nach dem Fehler kam es immer noch zu „Bedienfehlern“

Fazit

- immenser Imageverlust sowohl für SIEMENS als auch für die Bahn
- hohe Kosten durch Verspätungen und zusätzliche Arbeit
- laut Bahn waren zu keinem Zeitpunkt Personen gefährdet
- allerdings hat man nicht unbedingt daraus gelernt

Siemens Stellwerk in Berlin

- Ende Oktober 1996 traten erhebliche Probleme auf
- S-Bahnverkehr war für fast 4.5 Std. lahmgelegt
- Ursache: Zentralcomputer im neuen Stellwerk
  - Daten auf der Festplatte fehlten
  - alten System waren längst abgebaut

U-Bahn San Francisco

- seit Jahren taucht im Tunnelsystem ein Geisterzug auf
- man ist sich einig das der Zug nicht existiert
- Signale und Weichen müssen kontrolliert werden und von Hand gestellt werden
- Verspätung und Ärger bei den Fahrgästen

Jahr 2001 Problem

- am 31.12.00 konnte keiner von 29 Hochgeschwindigkeitszügen gestartet werden
- Software im Zugcomputer konnte das Datum nicht umstellen
- zurückdatiert auf 01.12.00 dadurch einen Monat für Fehlerkorrigtur

Abschlussbemerkung

- es gibt viele Sachen die bei Softwareentwicklung und - auslieferung beachtet werden müssen
  - Aufbau der Software selbst
  - komplette Auslieferung
  - sonstige Umstände (Datum,...)
- wichtig ist, dass die Einführungsphase falls möglich, nicht zu kurz gewählt wird und dass man eventuell auf Alternativen zurück greifen kann