Vorwort

„Die Produktivkräfte und die Reichtümer der Nation werden durch ein vollkommenes Transportsystem in außerordentlicher und mannigfaltiger Weise vermehrt werden."

Friedrich List (1789-1846)

Als Friedrich List zu Beginn des vorigen Jahrhunderts diesen Satz formulierte, ahnte er sicherlich nicht, welche Leistungsfähigkeit das von ihm propagierte Transportmittel einmal bekommen sollte. Doch mit Sicherheit wußte er auch nichts von der starken Konkurrenz, die das einstige Monopol der Bahn längst gebrochen hat.

Einen großen Beitrag, um dem drohenden Verkehrsinfarkt der Industrienationen zu entgehen, kann die Bahn leisten. Dafür jedoch muß sie konkurrenzfähig bleiben oder wieder werden. Um das zu erreichen, sind innovative Konzepte gefragt, die die ohne Zweifel vorhandenen Rationalisierungspotentiale ausschöpfen. Einen wesentlichen Beitrag dazu leisten Elektronische Stellwerke, die sich – aus verschiedenen Gründen – später als andere elektronische Steuerungen durchsetzten, heute aber weltweit Verwendung finden.

Ebenso, wie es unterschiedliche Spurweiten oder Stromsysteme bei verschiedenen Bahnverwaltungen gibt, haben sich auch unterschiedliche Sicherheitsphilosophien entwickelt, aus denen die verschiedensten Stellwerksbauformen – auch elektronische – hervorgingen. Ähnlich wie die Engländer, die im vorigen Jahrhundert ihre Spurweite in die ganze Welt „exportierten", versuchen heute die großen Signalbaufirmen, ihre elektronischen Stellwerke (ESTW) und damit die Sicherungsphilosophie der Bahnverwaltung, für die das jeweilige ESTW zuerst entwickelt wurde, in aller Welt zu verkaufen.

Wie sind diese Systeme nun aufgebaut, und was leisten sie? Welche Philosophien stecken dahinter, was unterscheidet sie von deutschen Ansichten? Diese Fragen zu beantworten, soll Gegenstand der vorliegenden Untersuchung sein. Darin werden im ersten Teil Grundlagen für die einheitliche Beschreibung der ESTW gelegt. Im zweiten Teil, der den wesentlichen Anteil der Arbeit darstellt, werden die einzelnen Systeme vorgestellt. Ein Vergleich ausgewählter Eigenschaften sowie die Einteilung der ESTW in drei Kategorien fassen die wesenlichen Ergebnisse der Arbeit im dritten Teil zusammen.

Für die Unterstützung und die Hinweise bei der Anfertigung der Arbeit danke ich Herrn Dr.-Ing. P. Naumann (TU Dresden), Herrn Prof. Dr.-Ing. habil. W. Fenner und Herrn Dipl.-Ing. H.-J. Petersen (SIEMENS AG, Bereich Verkehrstechnik, Braunschweig).

Teil I:

Konzeptionelle Grundlagen und ausgewählte Sicherheitsaspekte

1 Begriffsabgrenzungen

1.1 Elektronisches Stellwerk

Zunächst soll für den Begriff des „Stellwerks“ eine auf die elektronische Technik abgestimmte Definition gefunden werden. Hier besteht Klärungsbedarf, da der Begriff des Stellwerks bei ESTW unterschiedlich gehandhabt wird.

Was ist ein Stellwerk? Für den Außenstehenden ist ein Stellwerk der Hochbau mit seinen Inneneinrichtungen, von dem aus ein Bediener Signale und Weichen stellt. Für den Sicherungstechniker ist es weit mehr als das. In herkömmlichen Fachlexika wird das Stellwerk als eine Betriebsstelle beschrieben, die

a) die sicherungstechnischen Abhängigkeiten realisiert und

b) die Bedienungseinrichtungen aller sicherungstechnisch relevanten Elemente zusammenfaßt [20].

Die Ansicht des Außenstehenden ist dann richtig, wenn es sich um ein mechanisches oder elektromechanisches Stellwerk handelt, da die Abhängigkeiten hier größtenteils direkt an der Bedieneinrichtung realisiert werden. Bei einem Relaisstellwerk wird im Bedienraum nur die Forderung b) erfüllt. Erst im Relaisraum, der sich in einem separaten Gebäude oder zumindest in einem anderen Raum befindet, wird der Forderung a) entsprochen. In elektronischen Stellwerken verschärft sich die funktionelle und räumliche Trennung nach Erfüllung der beiden Forderungen noch mehr, da die Realisierung der sicherungstechnischen Abhängigkeiten wesentlich weiter entfernt von der Bedieneinrichtung geschehen kann.

In bisherigen ESTW, die weitgehend autark arbeiteten, fiel es leicht, den Bedienplatz dem ESTW zuzuordnen. Mitunter handelt es sich dabei noch um einen herkömmlichen Stelltisch, der zwangsläufig starr mit dem Stellwerk verbunden sein muß. Mit der Einführung von Betriebszentralen und anderen intelligenten Techniken (z. B. Zuglenkung) verliert der Bedienplatz den Anspruch auf alleinige Einflußnahme auf das ESTW (Abbildung 1). Darüber hinaus wird es zukünftig auch möglich sein, Bedienplätze nicht nur innerhalb eines Stellwerks freizügig zu verwenden, sondern von einem Bedienplatz auf verschiedene ESTW einzuwirken. Dieser Trend ist nicht nur bei der DB AG, sondern auch bei anderen Bahnverwaltungen zu erkennen.

Im Hinblick auf die Bildung von Betriebszentralen verliert die bisherige Vorstellung, die entlang der Strecke aufgestellten Stellwerke seien die untere Kommandoebene des Eisenbahnbetriebes, zunehmend an Bedeutung. In Zukunft wird es die Betriebszentrale sein; das Stellwerk – ob elektronisch oder relaisgesteuert – ist dann „nur“ noch ein zwar sicherungstechnisch unverzichtbares aber betrieblich untergeordnetes Instrument (Abbildung 2). Diese These wird durch folgende Aussage unterstützt:

„Aus zukünftiger … betrieblicher Sicht muß ein ‚Stellwerk' in seiner Eigenschaft als Komponente eines allgemeinen Leitsystems für den Bahnbetrieb betrachtet werden, wodurch sein Stellenwert relativiert wird und gegebenenfalls seine Bedeutung verringert wird."[4]

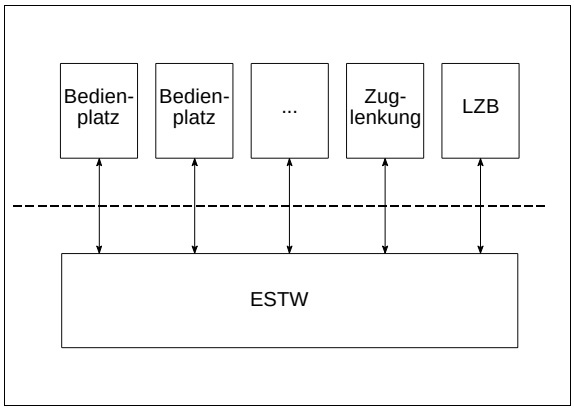


Abbildung 1: Einordnung des ESTW aus sicherungstechnischer Sicht

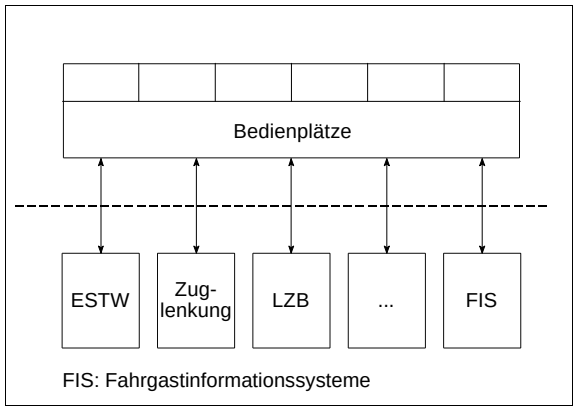


Abbildung 2: Einordnung des ESTW aus betrieblicher Sicht

Die bisher verwendete Definition, die für herkömmliche Stellwerke ausreichend war, kann zwar auf ein ESTW angewendet werden und entspricht auch der allgemeinen Auffassung; in neuerer Literatur wird jedoch die Bedienungseinrichtung mitunter getrennt vom ESTW betrachtet. Auch in den Systemstrukturen der meisten ESTW-Bauformen läßt sich eine konsequente Trennung der sicherungstechnischen Datenverarbeitung von der Einflußnahme auf das Stellwerk (Bedienung und Anzeige) erkennen. Für die vorliegende Arbeit hat sich eine Definition, die die konsequente Abtrennung der Bedienungsfunktionen vom ESTW vornimmt, als günstiger erwiesen.

Aufgrund der geschilderten Sachverhalte wird innerhalb der Diplomarbeit ein elektronisches Stellwerk (ESTW) folgendermaßen definiert:

Das ESTW ist die Hard- und Software, die

a) die sicherungstechnischen Abhängigkeiten realisiert,
b) Schnittstellen für die zu steuernden Elemente und für Techniken, die das ESTW beeinflussen oder von ihm beeinflußt werden, bereitstellt und
c) die unter a) und b) genannten Funktionen technisch verwaltet und sichert.

1.2 Elemente

Für die Bezeichnung der Elemente, die die Schnittstellen zwischen ESTW und Transportprozeß bilden, werden in der Literatur und seitens der Hersteller verschiedene Begriffe verwendet. Deshalb soll für diese Arbeit eine Abgrenzung und Unterteilung des Begriffs „Elemente" erfolgen.

SIEMENS unterteilt den Begriff „Elemente" folgendermaßen: **Aktive Elemente** sind solche, die bedienbar sind oder eine Anzeige nach sich ziehen. Im Gegensatz dazu stehen die **passiven**

Elemente wie z. B. BÜ-Anrückmelder oder Durchrutschwegelemente. Passive Elemente sollen in dieser Arbeit nicht weiter betrachtet werden, da sie sehr speziell sind.

Für die aktiven Elemente wird im folgenden der Begriff **Feldelemente** gebraucht. Diese lassen sich weiter unterteilen in **Stellelemente**, die bedienbar sind (z. B. Weichen einschließlich Antrieb, Lichtsignal einschließlich Leuchtmittel) und **Meldeelemente**, die nicht bedienbar sind, aber eine Anzeige nach sich ziehen (Gleisfreimeldeanlagen). Achszählanlagen lassen sich zwar bedienen (Grundstellung); da das aber keine Regelbedienung ist, sollen sie trotzdem den Meldeelementen zugeordnet werden. Der oft verwendete Begriff „Stelleinheit“ ist inhaltlich identisch mit dem Begriff „Stellelement“.

2 Vorgehensweise bei der Strukturbeschreibung

2.1 Das Drei-Ebenen-Modell

Für die Struktur der einzelnen ESTW gibt es erwartungsgemäß kein einheitliches Design. Jedoch sind Aufgabenschwerpunkte zu erkennen, die sich bei allen Stellwerken wiederholen: **Bedienungsverarbeitung – Sicherungstechnische Verknüpfung – Ansteuerung der Feldelemente**. Diese Einteilung wird nachfolgend das „Drei-Ebenen-Modell“ genannt und soll bei der Beschreibung und Systematisierung der Stellwerkssysteme behilflich sein.

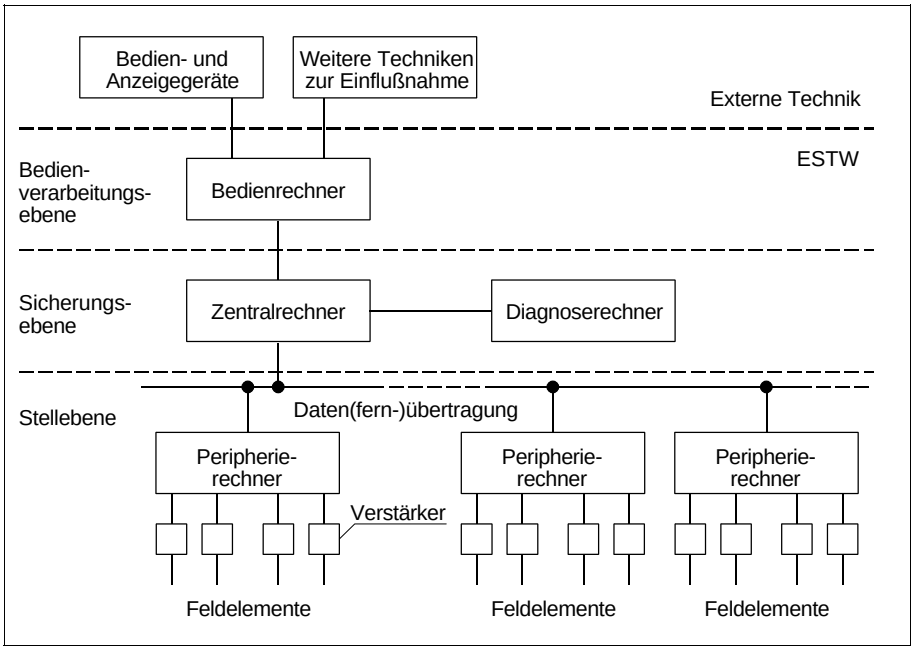


Abbildung 3: Typische Struktur eines ESTW

Jede Ebene wird durch einen oder mehrere Rechner repräsentiert. Auch wenn die Aufgabengebiete von Rechnern, die auf gleicher Ebene liegen, jedoch unterschiedlichen Systemen angehören, nicht immer deckungsgleich sind, so soll doch, um die Vergleichbarkeit der Systeme zu gewährleisen, an dieser „starren“ Dreiteilung festgehalten werden.

Bei jedem ESTW wurden die Rechner den jeweiligen Hauptaufgaben zugeordnet und die Grenzen der Ebenen zwischen den Rechnern gezogen. Gemäß dieser Hauptaufgabe wurden die Rechner benannt in „Bedienrechner“, „Zentralrechner“, „Diagnoserechner“ und „Peripherierechner“.

2.2 Interne und externe Kommunikation

Im Abschnitt „Interne Kommunikation“ wird die sichere Datenverbindung zwischen dem Zentralrechner und den Peripherierechnern beschrieben. Je nach Bauform beinhaltet sie auch die Verbindung zum Bedienrechner und zu benachbarten Stellwerken. Die externe Kommunikation (z. B. die Verbindung ESTW **S** Zuglenksystem) soll nur genannt, jedoch nicht näher beschrieben werden, da diese meist keinen sicherheitsrelevanten Charakter trägt.

3 Auswahl der Stellwerkssysteme und Inhalt der Beschreibungen

Leider sind nicht alle Systeme so ausführlich und öffentlich dokumentiert wie beispielsweise der SSI-Standard von British Rail. Deshalb wird es im Umfang der einzelnen Beschreibungen Unterschiede geben. Außerdem kann es sich in den Einzelheiten nur um eine Momentaufnahme der innovationsfreudigen Industrie handeln.

Die vorliegende Arbeit konzentriert sich zunächst auf die wichtigsten, derzeit weltweit eingesetzten ESTW. Obwohl gemäß der Aufgabenstellung nicht gefordert, wird das ESTW der Bauform El S (SIEMENS), auf Wunsch von SIEMENS Verkehrstechnik in die Arbeit einbezogen. Im Abschnitt „Weitere elektronische Stellwerkssysteme“ werden ESTW beschrieben, zu denen entweder nur wenige Informationen vorlagen oder deren Bedeutung zur Zeit noch gering ist.

Um dem Leser eine gute Vergleichbarkeit der einzelnen Systeme zu ermöglichen, wird für jedes ausführlich behandelte ESTW die gleiche Gliederung verwendet, auch wenn bei einigen Systemen zu manchen Gliederungspunkten aus systemeigenen Gründen oder wegen Nichtverfügbarkeit von Informationen keine Aussagen getroffen werden können.

Die Beschreibung der Stellwerkssysteme konzentriert sich hauptsächlich auf das Sicherheitskonzept und die Struktur der Hardware. Sofern es möglich ist, werden auch Aussagen zu Leistungsparametern, zur Software und zu den Möglichkeiten der Einflußnahme auf das Stellwerk getroffen. Nicht in dieser Arbeit behandelt werden solche speziellen Themen wie der mechanische Aufbau, die Realisierung der Stromversorgung oder die getroffenen Maßnahmen zur Erdung. Weiterhin sollen BÜ-Techniken sowie Systeme des Streckenblocks und der Zugbeeinflussung ausgeklammert werden.

4 Allgemeine Aussagen zur Sicherheit

Um Redundanzen bei der Beschreibung der einzelnen Systeme zu vermeiden, ist es notwendig, einige allgemeine Aussagen zur Sicherheit voranzustellen.

In den meisten Systemen sind das Sicherheits- und Verfügbarkeitskonzept eng miteinander verzahnt (z. B. 2v3-Konfiguration einer Komponente). Deshalb werden sie gemeinsam im Abschnitt „Sicherheits- und Verfügbarkeitskonzept“ behandelt, wobei der Schwerpunkt auf dem Sicherheitskonzept liegt. Die Begriffe „Zuverlässigkeit“ und „Verfügbarkeit“ werden inhaltlich identisch verwendet.

4.1 Software

Die meisten Systeme arbeiten mit a priori fehlerfreier und funktionsrichtiger Software. Erreicht wird das durch die bekannten Methoden der sicherheitsrelevanten Softwareentwicklung (z. B. Einschränkung des Befehlsumfangs, Verbot von direkten Sprungbefehlen etc.), die hier nicht weiter erläutert werden sollen. Nur bei Systemen, die mit diversitärer Software arbeiten, sollen die getroffenen Maßnahmen, die die Diversität gewährleisten, genannt werden.

Ein umfangreicher Test der Software und strenge Maßnahmen zur Qualitätssicherung sind bei allen ESTW-Typen üblich. Auch Prüfprogramme gehören zum Standard aller ESTW.

4.2 Bedienung und Anzeige

Einige Bahnverwaltungen (z. B. DB AG, ÖBB) fordern, daß Bedienung und Anzeige sicher aufgebaut sind. Diesen Forderungen kann bei Stelltischen und -tafeln, die aus der Relaistechnik bekannt sind, entsprochen werden; jedoch sind sie, vor allem aus Mangel an Flexibilität, heute nicht mehr zeitgemäß.

Alle Bediensysteme für ESTW stützen sich in der Anzeige zumindest vorwiegend auf Monitore. Diese und die sie ansteuernden Baugruppen können aber – wenn überhaupt – wegen der Komplexität der Elektronik nur mit unverhältnismäßig hohem Aufwand fail-safe aufgebaut werden. Deshalb werden besondere Verfahren eingesetzt, um die Sicherheit zu gewährleisten. Die Verfahren führen letztlich immer darauf hinaus, in zwei unabhängigen Kanälen Bildinformationen zu generieren, die dann miteinander auf Übereinstimmung geprüft werden. Dieser Vergleich kann entweder elektronisch im Bildspeicher oder, bei zyklischer Umschaltung auf den Monitor, visuell durch den Bediener erfolgen.

Ein ähnliches Problem zeigt sich bei der Eingabe sicherheitsrelevanter Bedienkommandos. Auch hier wird die Sicherheit durch bestimmte Verfahren gesichert. Einzelheiten dazu können [16] entnommen werden.

Teil II:

Vorstellung der Systeme

1 ESTW El S (SIEMENS)

Aufbauend auf der jahrzehntelangen Erfahrung im Stellwerksbau hat SIEMENS Verkehrstechnik die Entwicklung der elektronischen Stellwerke maßgebend beeinflußt. Die Entwicklungsinitiative ging dabei vom Hersteller aus. Bei der DB AG wird das SIEMENS-ESTW unter dem Namen „El S“ (**El**ektronisches Stellwerk der Bauform **S**IEMENS) eingesetzt. SIEMENS-intern ist auch die Bezeichnung „ESTW SIMIS-C“ gebräuchlich.

Die frühe Entwicklung und das damit verbundene Privileg, einer der ersten Anbieter elektronischer Stellwerke auf dem Weltmarkt zu sein, brachte den Nachteil ein, daß andere Anbieter, die ihre ESTW später entwickelten, in bestimmten Punkten gleich auf modernere Konzepte und Komponenten zurückgreifen konnten. *„Das ... El S ist das Ergebnis einer kontinuierlichen, langjährigen und ausgereiften Entwicklung ... Wegen der pionierhaften Entwicklung ohne Vorbild mußten bei dem nicht unkritischen Technologiewechsel in Zusammenarbeit mit dem Anwender neben der eigentlichen Entwicklung auch viele Grundsatzfragen gelöst werden, die dadurch erst jetzt zum Stand der Technik gehören.“*[5]

Ein weiteres Problem ist die Tatsache, daß das El S für die DB AG, die einen „High End“-Kunden darstellt, entwickelt wurde. Das vom Eisenbahnbundesamt (EBA) geforderte Sicherheitsniveau gehört zu den höchsten Sicherheitsanforderungen, die für eine Bahnverwaltung gestellt werden. Daraus resultieren höhere Kosten für das Stellwerk, die sich ihrerseits hemmend für den Absatz auf dem Weltmarkt auswirken [3]. Wichtige Merkmale des El S sind außerdem die Verwendung von eigenentwickelten Hardwarekomponenten und Software, die beim Bilden von Fahrstraßen nach dem Logikmodell des Spurplanprinzips verfährt.

Seit Mitte der 80er Jahre wird das El S erfolgreich bei Bahnverwaltungen wie DB AG, ÖBB, SBB, NS und VR sowie deutschen Stadt- und Industriebahnen eingesetzt [1].

Die technischen Einzelheiten der folgenden Beschreibung wurden, sofern nicht anders gekennzeichnet, [2] entnommen.

1.1 Sicherheits- und Verfügbarkeitskonzept

1.1.1 Datenverarbeitung

Um eine sichere Datenverarbeitung zu gewährleisten, werden eigenentwickelte Rechner in verschiedenen Konfigurationen verwendet, die nach dem SIMIS-Prinzip (**S**icheres **Mi**krocomputersystem von **S**IEMENS) arbeiten. Aus der SIMIS-Rechnerfamilie werden im El S Rechner der Bauarten SIMIS-C (8 Bit, 2v2) und SIMIS 3216 (16 Bit, 2v3) eingesetzt.

Rechnersysteme, die nach dem SIMIS-Prinzip konzipiert sind, bestehen aus mindestens zwei voneinander unabhängigen, identisch aufgebauten, taktsynchron arbeitenden und identisch programmierten Mikrocomputern. In den Kanälen werden die Prozeßdaten parallel verarbeitet. Die

Steuerwertausgaben an die Peripherie werden durch einen Hardware-Vergleicher fail-safe verglichen. Nur wenn die Ergebnisse mehrheitlich übereinstimmen, werden erarbeitete Befehle ausgegeben.

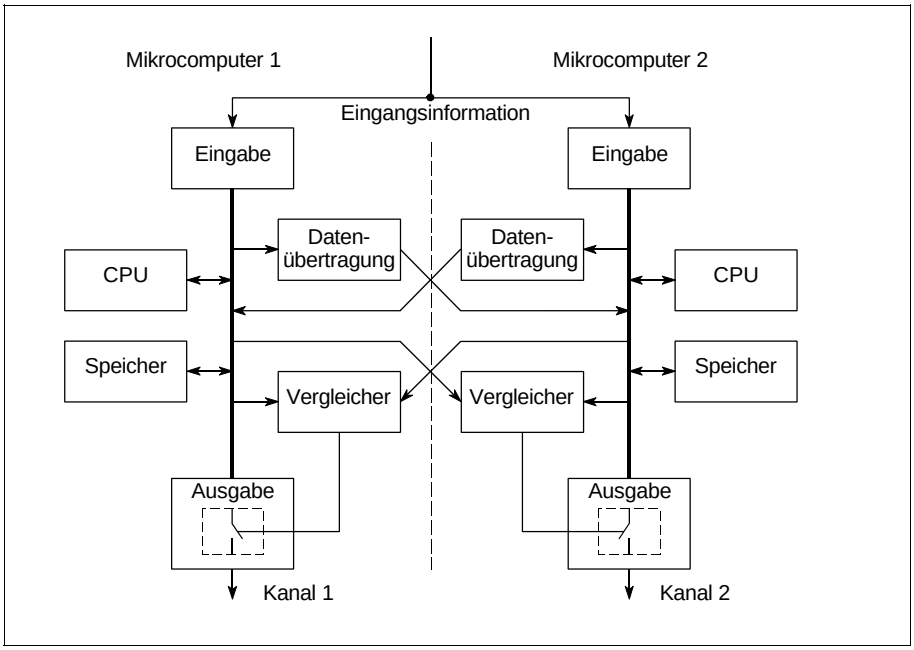


Abbildung 4: SIMIS-Prinzip bei 2v2-Konfiguration

Im Hintergrund der Prozeßbearbeitungsebene läuft das SIMIS-Online-Prüfprogramm (SOPP) ab. Die Laufzeit des SOPP wird überwacht, damit sichergestellt werden kann, daß es mindestens einmal innerhalb der maximal zulässigen Fehleroffenbarungszeit durch alle zu prüfenden Baugruppen gelaufen ist. Sobald der erste Fehler erkannt ist, wird das einzelne Rechnersystem vom Prozeß abgetrennt, so daß ein zufällig hinzukommender, weiterer Fehler sich nicht gefährlich auswirken kann. Neben dem SOPP gibt es weitere Prüfprogramme.

Ausfälle werden in den meisten Schaltungsteilen der Rechner, so auch in der Peripherie, per Programm durch Soll-Ist-Vergleich offenbart. So wird z. B. die Wirkung ausgegebener Befehle rückgelesen und mit den Solleinstellungen verglichen. Eine Sicherheitsabschaltung erfolgt nur dann, wenn eine weitere Verarbeitung nicht zulässig ist. Anderenfalls wird eine Fehlermeldung ausgegeben und eine Software-Sperre für die betreffende Funktion gesetzt.

1.1.2 Datenübertragung

Der interne Datenaustausch erfolgt in Form von normierten Telegrammen. Ein Sicherungsanhang von zwei Byte sichert die Daten mit einer Hamming-Distanz von d = 5; das bedeutet, daß bis zu vier gleichzeitig in einem Telegramm auftretende Bitfehler immer erkannt werden.

Sollte ein Kanal des Stellwerksbusses gestört sein, so arbeitet das ansonsten zweikanalig arbeitende Bussystem einkanalig weiter. Obwohl aus Sicht der Entwickler, die meines Erachtens richtig ist, die Datensicherung durch den Sicherungsanhang ausreichend ist, erfolgt die Kommunikation dann über Langtelegramme, die die doppelte Länge des Normaltelegramms haben. Die erste

Hälfte ist identisch mit dem Normaltelegramm, die zweite Hälfte ist bis auf die Sicherung invertiert gegenüber der ersten. Die einkanalige Arbeitsweise kann nach deutschem Standard acht Stunden aufrecht erhalten werden, danach erfolgt eine Zwangsabschaltung.

Beide Funktionen, sowohl die Langtelegramme als auch die Zwangsabschaltung, sind Forderungen des damaligen Bundesbahnzentralamtes (BZA, heute EBA), die die hohen deutschen Sicherheitsanforderungen erkennen lassen. Die SBB, bei der das El S ebenfalls eingesetzt wird, verzichtet beispielsweise auf die Zwangsabschaltung.

Um die Funktion der Verbindung zwischen den einzelnen Rechnern zu prüfen, werden Betriebsfähigkeitstelegramme ausgetauscht. Bei einkanaligem Betrieb kommt auch hier eine entsprechende Langversion zum Einsatz.

1.1.3 Bedienung und Anzeige

Sicherheitsrelevante Anzeige

Bisher wurde die Sicherheit durch die Sichtgeräte-Doppelsteuerung (SIDOS) realisiert. Der SIDOS wird das Videosignal immer zweikanalig aus dem Bedien- und Anzeigerechner (BAR 16) zugeführt. Aus diesen zwei Signalen erstellt die SIDOS zwei Bilder, die wechselseitig auf den Lupenbildmonitor aufgeschaltet werden. Unstimmigkeiten in den Kanälen führen zu einem Blinken des Bildes oder eines Bildteiles.

Die Überwachung der vollen Funktion der SIDOS erfolgt mittels Kontrollmelder auf dem Lupenbildmonitor. Ein im Umschalttakt wechselnder Balken (Umschaltmelder) zeigt an, daß das Bild von zwei unabhängigen Kanälen erzeugt wird. Vor jeder sicherheitsrelevanten Bedienung sind die Kontrollmelder durch den Bediener auf ordnungsgemäße Funktion zu prüfen.

Beim neuen Bedienplatzsystem (BPS) 901 wird auf die SIDOS verzichtet und statt dessen der Lupenbildmonitor vom Bedienplatzrechner (BPR) gesteuert. Für das Erreichen der Sicherheit werden die Lupenbilder von einem dem BPR parallelgeschalteten Referenzrechner (RR) ebenfalls erzeugt und bei Bedarf die Bildspeicher verglichen. Ein Unterschied in der Speicherbelegung weist auf einen Fehler im BPS oder in der Datenübertragung hin und führt zum Abbruch einer eventuell stattfindenden Bedienhandlung. Weiterhin laufen zyklische Prüfungen ab, die in allen BPR und RR die wesentlichen Funktionen testen. Die Datenübertragung vom ESTW zu den Rechnern des BPS 901 wird durch Sequenznummer und Sicherungsanhang verfahrensgesichert [7].

Sicherheitsrelevante Bedienung

Um die geforderte Sicherheit in der Bedienung zu gewährleisten, wurde das Kommandofreigabe (KF-) verfahren entwickelt. Dazu wird vom Bediener die nochmalige Bestätigung des kritischen Befehls gefordert, die dieser durch das Drücken der KF-Taste gibt. Diese Taste ist das einzige Eingabegerät in Sicherheitsbauform und direkt mit dem Stellwerk, ohne Nutzung des Bedien-

platzrechners, verbunden. Durch eine Zeitverzögerung bis zur Annahme der KF-pflichtigen Bedienung durch das Stellwerk wird erreicht, daß der Bediener sich der Tragweite seines Befehls bewußt werden kann.

Beim BPS 901 ist die KF-Taste nicht mehr vorgesehen. Die KF-Bedienungen werden jetzt über das Bedientablett gegeben, wobei die Sicherheit nun durch ein spezielles Verfahren mit zwei Tablettfeldern (KF1, KF2) erreicht wird: Nach der bisherigen Aufforderung, die KF-Taste zu drücken, hat der Bediener das Feld KF1 und danach KF2 zu bedienen. Verfahrensgesichert wird die Bedienhandlung an das ESTW übertragen. Die Sicherung erfolgt nach dem Prinzip „Prüfschleife“. Das beim ESTW angekommene Kommando wird dazu in das BPS 901 zurückgespiegelt und dort mit dem abgeschickten Kommando verglichen; beide Rechner, BPR und RR, sind an der Prüfung beteiligt [7].

Vermutlich rührt die Forderung nach einer KF-Taste in Sicherheitsbauform aus einer Zeit, da die Elektronik noch nicht so weit entwickelt und zuverlässig wie heute war. Ein Rechner beispielsweise, der nach kurzer Betriebszeit seinen Dienst versagt, ist heute indiskutabel [3]. Das Integrieren der KF-Taste in das Bedientablett und die weitere Verarbeitung und Weiterleitung durch den BPR zeigt, daß inzwischen größeres Vertrauen in die Elektronik gesetzt wird.

1.2 Systemstruktur

1.2.1 Hardwarearchitektur

Die Grafik zeigt die grundsätzliche Konfiguration des El S mit dem bisher verwendeten BPS 900. Die Rechner werden gemäß der Grafik in die drei Ebenen eingeordnet. Dabei soll angemerkt werden, daß es keinen Zentralrechner im Sinne der in dieser Arbeit verwendeten Definition gibt, da der Eingabe-, Kontroll- und Interpretationsrechner (EKIR) nur allgemeine Steuerungsaufgaben übernimmt und die Fahrstraßenlogik in den Bereichsstellrechnern (BSTR) realisiert wird.

Ein über die Bedienperipherie eingegebener Befehl gelangt vom BPR über den Kommunikations-Server (COM-Server) zum BAR 16. Der COM-Server paßt die Telegramme, die zwischen BAR 16 und den an den Betriebsleitbus (BLT-Bus) angeschlossenen Komponenten übertragen werden, an und dient somit als Schnittstellenumsetzer. Die seriellen Datenverbindungen zum BAR 16 und die COM-Server sind aus Verfügbarkeitsgründen redundant ausgeführt.

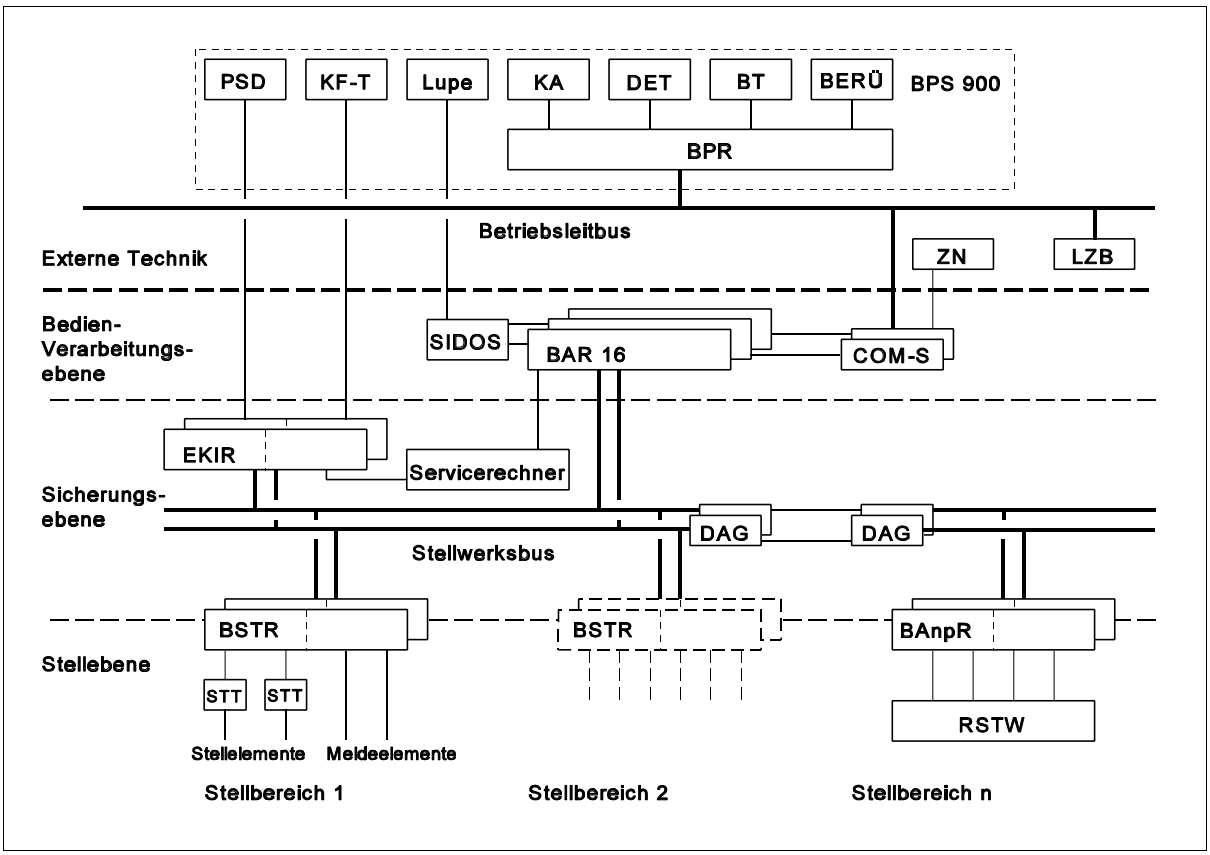


Abbildung 5: Systemstruktur des ESTW El S mit BPS 900

BAnpR	Bedien-Anpaßrechner
BAR16	Bedien- und Anzeigerechner (16 Bit)
BERÜ	Bereichsübersicht
BPR	Bedienplatzrechner
BPS	Bedienplatzsystem
BSTR	Bereichsstellrechner
BT	Bedien-Tablett
COM-S	Kommunikations-Server
DAG	Datenanschlußgerät
DET	Daten-Eingabetastatur
EKIR	Eingabe-, Kontroll- und Interpretationsrechner
KA	Kommunikationsanzeige
KF-T	Kommandofreigabe-Taste
LZB	Linienförmige Zugbeeinflussung
PSD	Protokoll- und Störungsdrucker
RSTW	Relaisstellwerk
SIDOS	Sichtgeräte-Doppelsteuerung
STT	Stellteil
ZN	Zugnummernmeldeanlage

Im BAR 16 erfolgt die weitere Bearbeitung des Befehls. Über den Stellwerksbus verteilt er die Aufgaben an die BSTR, die die Verknüpfung der Feldelemente untereinander und mit dem Stellwerk gewährleisten. Die Ausgangssignale der BSTR werden an die Stellteile weitergeleitet. Sie sind die Leistungsschalter bei der Ausgabe von Stellaufträgen an die Elemente der Peripherie. Auch die Rückmeldungen von der Außenanlage werden über die Stellteile geleitet. Gleisfreimeldeanlagen werden direkt an den BSTR angeschlossen, da deren Ein- und Ausgangssignale keinen Leistungspegel erfordern.

Bei großen Arbeitsbereichen werden dezentrale Stellbereiche gebildet. Dabei wird der Stellwerksbus mit dem Bus jedes dezentralen Stellbereichs gekoppelt. Ein im Arbeitsbereich des ESTW liegendes Relaisstellwerk kann über einen Bedienanpaßrechner in das ESTW integriert werden.

1.2.2 Rechner und Verstärker

1.2.2.1 Bedienrechner

Der Bedien- und Anzeigerechner (BAR 16) ist aus dem früheren Anzeige- und Schnittstellenrechner (ANSR) hervorgegangen. Er ist als 2v3-System nach dem SIMIS 3216-Konzept gestaltet und hat eine Verarbeitungsbreite von 16 Bit. Seine drei Einzelrechner werden als Kanal A, B und C bezeichnet.

Die Aufgaben des BAR 16 bestehen unter anderem in der Auswertung und Verarbeitung der empfangenen Daten vom BPR. Der BAR 16 ist im ESTW der Rechner, welcher alle Eingabekommandos auf ihre inhaltliche Richtigkeit (Syntax) überprüft und die Zulassungsprüfung der angestrebten Bedienungshandlung veranlaßt. In seinem Speicher sind alle bedienbaren Elemente der Anlage enthalten und entsprechend ihrer topografischen Lage miteinander verknüpft. Weitere Aufgaben sind die Speicherung von aktuellen Zustandsdaten aus den Stellbereichen, so daß bei Ausfall eines BSTR keine aktuellen Daten verloren gehen. Bei Stellwerken mit BPS 900 werden durch den BAR 16 die Informationen an die SIDOS zur Erzeugung der Lupenbilder ausgegeben.

Eine Verbindung mit dem Stellwerksbus wird über die Busanschluß-Baugruppe (BUREP) realisiert. Dabei werden nur die Kanäle A und B an jeweils eine Leitung des redundanten Stellwerksbusses angeschlossen. Das bedeutet, daß bei Ausfall des Kanals C der nun als 2v2-System arbeitende BAR 16 weiterhin über beide Busleitungen kommuniziert. Fällt dagegen einer der Kanäle A oder B aus, arbeitet der BAR 16 ebenfalls als 2v2-System, kann aber nur noch über eine Busleitung Informationen austauschen. Die hierfür verwendeten Telegramme haben dann Langformat (s. a. 1.1.2).

1.2.2.2 Zentralrechner

Der Overheadrechner 2 (OHR2) ist ein 8 Bit-Rechner der SIMIS-C-Technik. Er ist aus dem Eingabe-, Kontroll- und Interpretationsrechner (EKIR) hervorgegangen. Dem allgemeinen Sprachgebrauch folgend, soll er in den nachstehenden Ausführungen weiterhin „EKIR“ genannt werden.

Durch den Einsatz des BAR 16 sind die Aufgaben des EKIR auf das Vorhalten der Software für die BSTR und den BAR 16, die Steuerung des Protokoll- und Störungsdruckers (PSD), die Überwachung der Stromversorgungsmeldungen und die Verwaltung der Weichenlaufkette eingeschränkt. In Zukunft werden auch diese Aufgaben dem BAR 16 übertragen werden, womit der EKIR entbehrlich wird.

Als Rechner der SIMIS-C-Familie wird der EKIR in der 2×(2v2)-Konfiguration eingesetzt. Im Gegensatz zum BSTR bietet der Redundanzrechner des EKIR eine wirklich heiße Redundanz, da er parallel zum Arbeitsrechner läuft und gleichzeitig alle Operationen ausführt, ohne daß Ausgaben wirksam werden.

Der EKIR verwaltet alle Adressen der Rechner und ist der oberste Verwalter des Systems. Er erhält Informationen über jeden Ablauf und jede auftretende Störung in der Anlage. Deshalb steuert er auch den PSD als zentrales Dokumentationsmedium.

1.2.2.3 Peripherierechner

Während BAR 16 und EKIR die Koordinierung der Aufgaben vornehmen, ist der Bereichsstellrechner (BSTR) das ausführende Element in der Rechnerhierarchie. Er enthält zwei Grundfunktionen, die früher durch zwei separate Rechner (Bereichs- und Stellrechner) realisiert wurden. Diese Trennung besteht softwaremäßig immer noch.

Als **Bereichsrechner** beinhaltet er die Bearbeitungsprogramme (Zulassungsprüfung, Anschaltung, Überwachung, Flankenschutz usw.) für alle auftretenden Elementtypen, unabhängig von der topografischen Anordnung. Die bahnhofsspezifischen Daten für die Elemente, die Nachbarschaftsbeziehungen zwischen ihnen und die Elementbezeichnungen werden dem Bereichsrechnerteil in der Aufrüstphase vom EKIR übersandt. Weiterhin fragt der Bereichsrechner während des Aufrüstens die letzten sicherheitsrelevanten Zustandsdaten beim BAR 16 ab. Die Daten speichert der BSTR in seinem RAM.

Auf Grundlage der allgemeinen Bearbeitungsprogramme und unter gleichzeitigem Zugriff auf die bahnhofsspezifischen Daten bearbeitet der Bereichsrechnerteil die Prüf-, Einstell-, Überwachungs- und Auflösevorgänge. Die Istzustände der Feldelemente werden dem Bereichsrechnerteil vom Stellrechnerteil mitgeteilt.

In seiner Funktion als **Stellrechner** bildet der BSTR die Schnittstelle zwischen Stellwerk und Außenanlage. Er beinhaltet die Stell- und Überwachungslogik für alle Feldelemente. Welche Elemente an den BSTR angeschlossen sind, werden diesem in der Aufrüstphase mitgeteilt.

1.2.2.4 Diagnoserechner

Als Diagnoserechner (im El S Servicerechner genannt) kommt ein IBM-kompatibler PC zum Einsatz. Er wird über eine serielle Schnittstelle mit dem BAR 16 und dem EKIR verbunden. Um eine gezielte Störungsdiagnose durchführen zu können, werden ständig folgende Daten von allen Rechnern und sonstigen Komponenten aufgezeichnet:

- Baugruppenausfallmeldungen
- Prozeßdaten (Bedienungshandlungen, Störungsmeldungen usw.)
- Systemdaten.

Die von den Stellwerksrechnern eingehenden Meldungen werden in Text konvertiert und in eine Datenbank geschrieben. Durch die ständige Speicherung der Daten können der genaue Zeitpunkt des Eintretens einer Störung ermittelt und eventuell Rückschlüsse auf deren Ursache gezogen werden.

1.2.2.5 Leistungsschalter

Bindeglied zwischen den Bereichsstellrechnern und ihren Stellelementen sind Stellteile, die aus einer Kombination von Elektronik und Signalrelais bestehen. Sie stellen und kontrollieren die Elemente der Außenanlage. Die Stellentfernung beträgt bei Kupferkabelverbindungen für Weichen und Signale 6,5 km. Bei Verwendung von Lichtwellenleitern für die Verbindung zu Signalen sind größere Stellentfernungen realisierbar.

Zur Anschaltung der Außenanlage stehen eine Vielzahl verschiedener Stellteile zur Verfügung. Es wird unterschieden in Relaisstellteile, die zur Anschaltung von Geräten für Block, Schlüsselabhängigkeiten und Weichen verwendet werden, und in Signalstellteile, deren Partner in der Außenanlage Signalmodule sind. Signalmodule sind kleine, passive Elektronikbaugruppen, die in einem Schrank am Signalmast untergebracht sind und die Lampenfäden überwachen. Durch diese Intelligenz am Signal werden für jede Signallampe nur zwei Kabeladern zwischen Stellwerk und Außenanlage benötigt.

1.2.3 Interne Kommunikation

1.2.3.1 Aufbau

Der Stellwerksbus ist sternförmig aufgebaut. Im Mittelpunkt befindet sich die Buszentrale. Sie wird zentral im Stellwerk angeordnet, damit die Verbindungswege zu allen angeschalteten Rechnern möglichst kurz sind. Alle Rechner besitzen Busanschluß-Baugruppen (BUREP), die über Kabel mit den Bus-Verstärkerbaugruppen (BUVER) der Buszentrale verbunden sind. Die BUVER hat die Aufgabe, die auf den Daten- und Steuerleitungen laufenden Signale zu regenerieren, um den schädlichen Einfluß der Kabelkapazität auf die Signale zu vermindern.

Der eigentliche Bus besteht aus acht Datenleitungen und sechs Steuerleitungen. Außerdem gibt es zu jeder Baugruppe eine Anforderungsleitung. Anforderungs- und Steuerleitungen kommen von der Bus-Steuerung, die aus der Zentralen Bus-Steuerbaugruppe (ZEBUS) und – bei Bedarf – der Zentralen Bus-Erweiterungsbaugruppe (ZEBER) besteht.

Sollen einzelne BSTR ausgelagert werden, wie es bei der Steuerung großer Bereiche unumgänglich ist, so werden die Stellwerksbusse durch Modems, die hier Datenanschlußgeräte (DAG) genannt werden, über (nicht öffentliche) Fernmeldeleitungen verbunden. Dazu wird das DAG an die Buszentrale angeschlossen. Eine Kopplung über Lichtwellenleiter ist ebenfalls möglich. In Zukunft werden die Stellwerksbusse auch über öffentliche Netze miteinander kommunizieren. Dafür ist eine zusätzliche Verschlüsselung der Daten erforderlich, auf die hier nicht näher eingegangen werden soll.

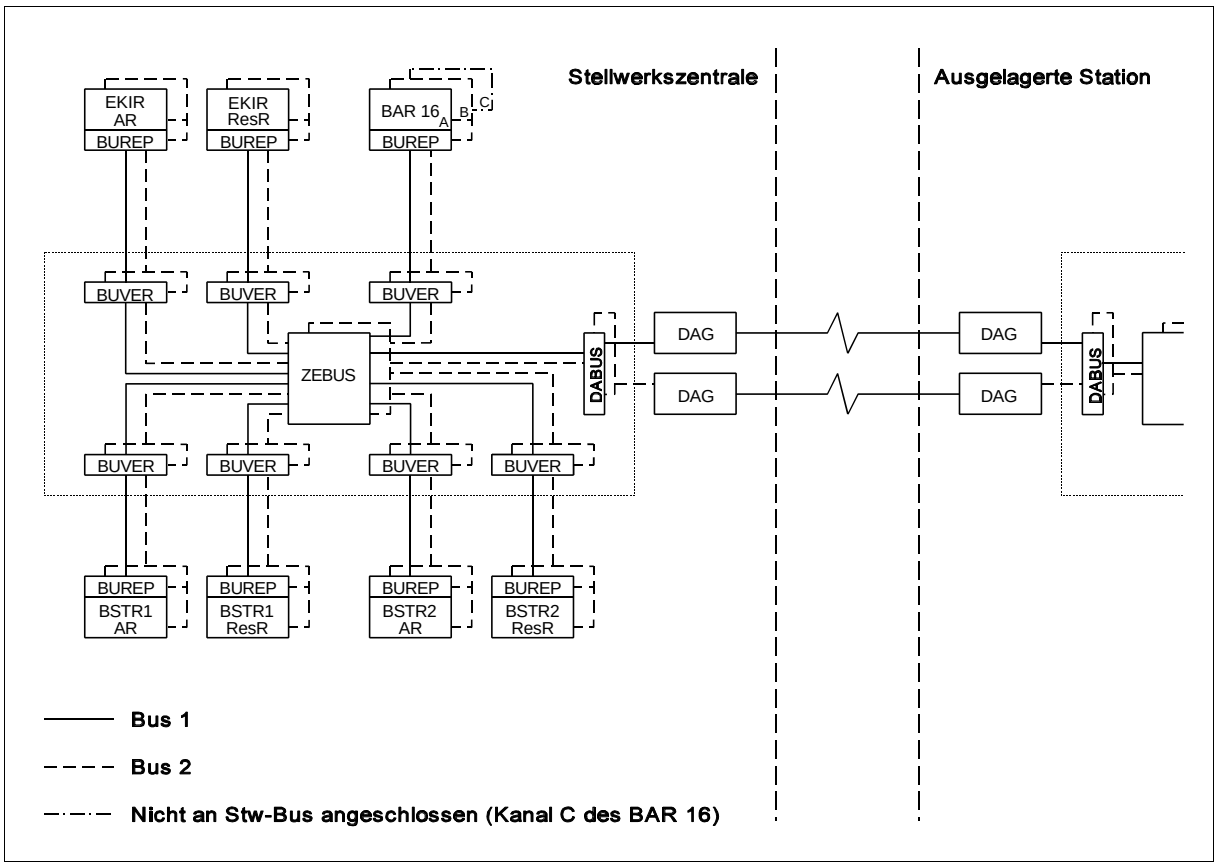


Abbildung 6: Typische Bus-Konfiguration im El S

AR	Arbeitsrechner	DAG	Datenanschlußgerät
BAR	Bedien- und Anzeigerechner	EKIR	Eingabe-, Kontroll- und Interpretationsrechner
BUREP	Busanschluß-Baugruppe für Rechner (parallel)	ResR	Reserverechner
BUVER	Busverstärker-Baugruppe	ZEBUS	Zentrale Bussteuer-Baugruppe
DABUS	Datenanschluß-Baugruppe		

1.2.3.2 Datenübertragung

Der Datenaustausch zwischen den Rechnern oder den einzelnen Verarbeitungsprogrammen innerhalb eines Rechners erfolgt in Form von normierten Telegrammen. Das 17 Byte lange Normaltelegramm enthält Telegrammkopf, Datenteil und Sicherungsanhang.

Jeder an den Stellwerksbus angeschlossene Rechner verfügt zum Datenaustausch über zwei Adressen:

- die Betriebsadresse, die während der Aufrüst-Routine im Rechner gespeichert wird, und
- die Drahtadresse, die hardwaremäßig im Wrapfeld der Buszentrale codiert ist.

Byte	Inhalt	Funktion
0	Empfängeradresse	Kopf
1	invertierte Empfängeradresse	
2	Telegrammauftragsart	
3	Absenderadresse	
4	Sequenznummer	
5	Datenbyte 1	Datenteil
6	Datenbyte 2	
…	…	
14	Datenbyte 10	
15	Sicherungsanhang	Sicherung
16	Sicherungsanhang	

Tabelle 1: Aufbau eines Normaltele gram ms

Jeder Rechner (BAR 16, BSTR) meldet sich nach dem Einschalten unter seiner Drahtadresse beim EKIR an und tauscht mit diesem zweikanalig zunächst Entsperr-Telegramme aus. Danach werden die Aufrüst-Telegramme übertragen. Nachdem der EKIR den entsprechenden Rechner mit seinen Anlagedaten aufgerüstet hat, nimmt dieser seine Arbeit unter der softwaremäßigen Betriebsadresse auf. Erst wenn alle Rechner aufgerüstet sind, können sie Auftrags-Telegramme senden.

Die Datenübertragung erfolgt im Anruf-Vermittlungsverfahren. Dabei wird die ZEBUS von der sendewilligen BUREP angerufen. Bei Empfangsbereitschaft der Empfänger-BUREP und freiem Bus wird die Verbindung hergestellt.

1.2.4 Leistungsparameter

An ein Bussystem (somit in einem ESTW) können maximal 127 Rechner angeschlossen werden. Diese Grenze ergibt sich aus der Anzahl der zur Verfügung stehenden Adressen. Um dem wachsenden Umfang der Stellbereiche gerecht zu werden, wurde die Möglichkeit geschaffen, in einem ESTW mehrere BAR 16-Rechner einzusetzen. Weiterhin können bis zu drei Bedienanpaßrechner in das El S integriert werden.

Je BSTR können 30 bis 40 Feldelemente angesteuert bzw. deren Meldungen eingelesen werden. Insgesamt wird von einem ESTW El S ein Umfang von ca. 1000 Stelleinheiten beherrscht.

1.3 Software

1.3.1 Struktur und Logikmodell

Die Software läßt sich in drei Kategorien einteilen:

- System-Software
- Stellwerks-Software
- Anlagenspezifische Daten.

Mit der **Systemsoftware** werden alle Grundfunktionen der SIMIS-Rechner realisiert; aus diesem Grund ist sie in allen sicherheitsrelevanten Rechnern installiert. Sie organisiert sowohl die Zusammenarbeit der Rechner und Rechnerkomponenten als auch den erforderlichen Datenaustausch. Außerdem steuert sie die Eigen- und Baugruppenprüfung und rüstet die Rechner mit elementspezifischen Daten auf.

Die **Stellwerkssoftware** wird für jede Bahnverwaltung gemäß deren Pflichtenheft entwickelt. Sie unterteilt sich in mehrere funktionsspezifische Programme (Softwarebausteine), von denen jedes zur Bearbeitung eines Teils der Anlage (z. B. Weichen, Gleise, Signale) dient. Diese Programme werden auf EPROM gespeichert und in den BSTR installiert. Im Gegensatz zur Relaistechnik ist es nicht mehr nötig, die Logik eines Elements so oft einzusetzen, wie das Element vorhanden ist, da der Rechner beim Abarbeiten des Prozesses immer wieder auf das eine Programm zurückgreifen kann.

Die **anlagenspezifischen Daten** in EPROM des EKIR hinterlegt. Bei Inbetriebnahme des ESTW oder bei Wiederinbetriebnahme eines Rechners werden diese Daten in einer Aufrüstphase den BSTR sowie dem BAR 16 übermittelt und dort im RAM gespeichert. Die zunächst anlagenneutralen Rechner sind erst nach diesem Aufrüstvorgang (Boot-Vorgang) einsatzbereit.

Als einziges von allen beschriebenen ESTW wird im El S beim Bilden von Fahrstraßen nach dem Spurplanprinzip verfahren. Die Verbindung der Elemente untereinander wird als Nachbarschaftsbeziehung bezeichnet und drückt sich u. a. im Elementverbindungsplan aus.

1.3.2 Projektierung

Für die Projektierung der Hardware wird das System APOLLO eingesetzt, welches aus einer Workstation mit den entsprechenden Peripheriegeräten wie Drucker und Plotter sowie spezieller Software besteht. Die von diesem System aufgebauten Grunddaten werden im Projektierungssystem für Anlagendaten mit der Anwendersoftware PRADES weiterverarbeitet. Der Arbeitsplatz hierfür besteht aus einem IBM-kompatiblen DOS-PC, der mit dem Rechenzentrum sowie einem Drucker verbunden ist [26].

1.4 Externe Einflußnahme (Bedienung und Anzeige)

1.4.1 Allgemeines

Die externen Techniken werden größtenteils über den seriellen Betriebsleitbus angeschlossen. Dieser ist ein genormtes lokales Netzwerk (Ethernet). Einige Techniken werden jedoch auch direkt über den COM-Server mit dem Stellwerk verbunden.

Die **Zugnummernmeldung (ZN)** soll automatisch die Zugstandorte ermitteln und diese durch eine übersichtliche Anzeige der Zugnummern in einer schematischen Gleisnachbildung dem Stellwerksbediener für die Disposition zur Verfügung stellen.

Die **Zuglenkung (ZL)** soll Fahrwege in Bahnhöfen und an Streckenverzweigungen im Zusammenwirken mit der ZN und dem ESTW automatisch auswählen und Stellbefehle an das ESTW geben. Die ZL erarbeitet beim Zulauf eines Zuges die erforderlichen Stellaufträge für die einzustellende Fahrstraße auf der Basis der ZN-Meldungen und gespeicherter Lenkvorgaben. Die Realisierung erfolgt durch einen eigenständigen Rechner mit dem Zuglenkmanager.

Zukünftig ist die Ansteuerung von **Zugzielanzeigern (ZZA)** als Bestandteil eines Fahrgastinformationssystems vorgesehen. Der Zugzielanzeiger wird ebenfalls durch einen eigenständiger Rechner realisiert und benötigt für die Ermittlung der Steuerkommandos außer seinen Projektierungsdaten die Zugnummern vom ZN-System und weitere Informationen über die Fahrstraßeneinstellung vom ESTW.

1.4.2 Bedienplatz

Die Grundausstattung eines Bedienplatzes besteht aus:

- Tastatur
- Lupenbildmonitor
- Kommunikationsanzeigemonitor
- Protokoll- und Störungsdrucker und
- KF-Taste (bei BPS 900).

Abhängig von den betrieblichen Erfordernissen können darüber hinaus folgende Bedienkomponenten eingesetzt werden:

- Bedientablett
- max. ein weiterer Lupenbildmonitor
- max. zwei Bereichsübersichtsmonitore
- Meldetafel
- Videoprojektionswand
- Maus oder Rollkugel.

Die Bereichsübersicht (Berü) erzeugt ein vollgrafisches Bild, das den Stellwerksbezirk ganz oder teilweise darstellt und als nicht sicher gilt. Die Lupe dagegen zeigt ein sicheres und (beim BPS 900) semigrafisches Bild eines kleineren Ausschnitts. An Stelle von Bereichsübersichtsmonitoren kann auch eine Videoprojektionswand oder eine Meldetafel vorgesehen werden, deren Anzeigen für alle Bedienplätze relevant sind. Bei Einsatz einer Meldetafel ist ein zusätzlicher

Meldetafelrechner (METARE) notwendig; der Trend bei der DB AG geht jedoch dahin, von Meldetafeln abzusehen, wohingegen andere Bahnverwaltungen (z. B. NS) dies noch fordern.

Das BPS 901 ist die konsequente Weiterentwicklung des BPS 900 und kommt erstmalig in der Betriebszentrale Magdeburg zum Einsatz. Neuerungen dabei sind die bereits beschriebene Integration der KF-Taste in das Bedientablett sowie die Ansteuerung der Lupen vom BPR mit Vergleich durch den Referenzrechner.

Eine weitere, wichtige Neuerung ist, daß die Lupe jetzt ein vollgrafisches Bild zeigt. Somit können jetzt die Bilder für Lupe und Berü gemeinsam projektiert werden. Während des Einsatzes werden sie dann in zwei unterschiedlichen Zoom-Stufen dargestellt [7].

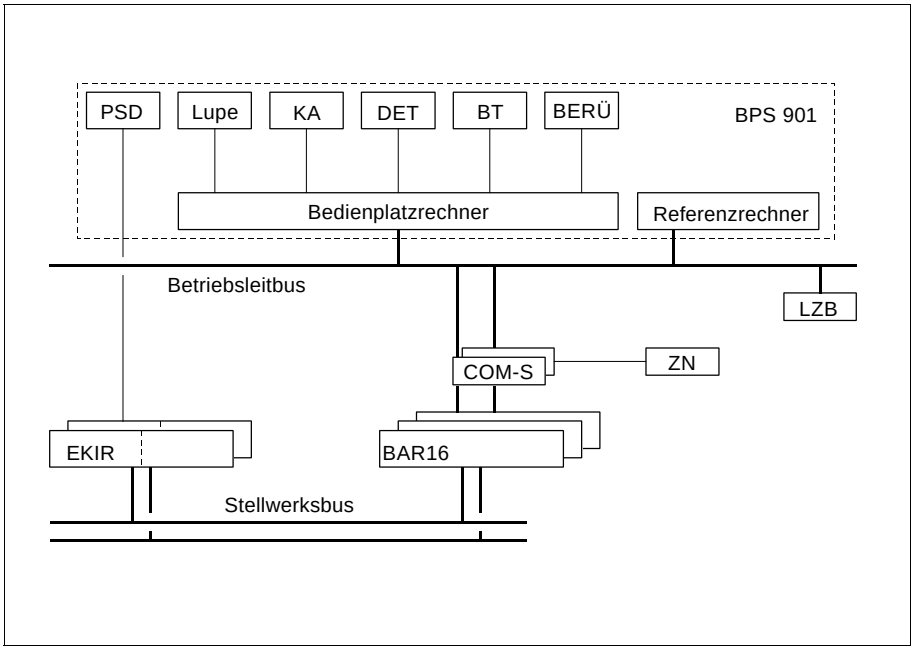


Abbildung 7: Konfiguration des BPS 901

An den BPR sind nun, bis auf den PSD, alle Geräte der Ein-/Ausgabeperipherie angeschlossen. Da er, wie der Referenzrechner, ein handelsüblicher Rechner ist, muß die geforderte Sicherheit durch die bereits beschriebenen Verfahren erbracht werden.

Eine Verfügbarkeitsredundanz ist nicht vorgesehen, da sich in der Regel in einem Stellwerk mehrere Bedienplätze befinden, von denen aus jeder Stellbereich wahlweise gesteuert werden kann.

Der Arbeitsbereich eines elektronischen Stellwerkes kann in mehrere Bedienbereiche untergliedert werden, die wiederum freizügig den einzelnen Fahrdienstleiter-Arbeitsplätzen zugeordnet werden können. Entsprechend der Aufgabe und der Verantwortung des Bedieners können die Bedienplätze mit unterschiedlichem Befugnisumfang ausgestattet sein [1]. Mit der Einrichtung von Betriebszentralen erlangt diese Eigenschaft an Bedeutung, da die Zuständigkeiten dort in Zuglenker und örtlichen Fahrdienstleiter unterteilt sind.

2 ESTW El L (ALCATEL SEL)

Als große deutsche Signalbaufirma bietet auch ALCATEL SEL (im folgenden kurz SEL genannt) ein ESTW weltweit an. Vermarktet wird es mit der Bezeichnung „ESTW L90“. Analog zur Namensgebung des ESTW von SIEMENS wird es bei der DB AG unter dem Namen „El L“ eingesetzt. Um diese Analogie beizubehalten, soll das „ESTW L90“ in dieser Arbeit als „El L“ bezeichnet werden.

Die Entwicklung begann 1978 durch Initiative des Herstellers. Nach ausgiebigen Tests konnte 1989 das erste ESTW mit voller Sicherheitsverantwortung in Betrieb gehen. Heute sind zahlreiche ESTW El L in Deutschland, Spanien, Luxemburg und Portugal im Einsatz.

Kennzeichnend für das El L ist die konsequente Nutzung handelsüblicher Hardware, sowohl bei Rechnern, als auch bei Komponenten zur Datenübertragung.

2.1 Sicherheits- und Verfügbarkeitskonzept

Bis 1983 *„wurde das Ziel verfolgt, aus Gründen der Instandhaltung als Sicherheitsbaustein für das ESTW das von SIEMENS und SEL gemeinsam entwickelte Konzept SIMIS (Sicheres Mikrocomputer-System) zugrunde zu legen. Alle nicht im sicherheitstechnischen Bereich liegenden Bausteine ... sollten dem Wettbewerb unterworfen sein. Im Verlauf der Verhandlungen mit den beiden Signalbaufirmen und nach eingehenden weiteren Untersuchungen hatte es sich jedoch als für die DB und die Firmen gleichermaßen vorteilhaft herausgestellt, für SEL einen eigenen Sicherheitsbaustein zuzulassen.“*[8] Offensichtlich bekam SIMIS erst danach die Bedeutung **Si**cheres **Mi**krocomputer-System von **S**IEMENS.

2.1.1 Datenverarbeitung

Der Sicherheitsbaustein SELMIS wird in allen Modulen des El L mit Sicherheitsverantwortung eingesetzt. Um eine Technologieunabhängigkeit zu erreichen, wird der Kern des sicheren Bausteins, der aus marktgängigen Rechnerbaugruppen besteht, trotzdem aber Sicherheit zu gewährleisten hat, in eine „Sicherheitsschale“ eingebunden. Dadurch ist es möglich, auch zukünftige, leistungsstärkere Rechner und damit das immer günstiger werdende Preis/Leistungsverhältnis von Rechentechnik für das El L zu nutzen. Dazu muß lediglich die schnittstellenkompatible Zentraleinheit ohne Veränderung des Aufbausystems der Software ausgetauscht werden.

Die Sicherheit des SELMIS beruht auf Mehrfachverarbeitung in voneinander unabhängigen parallelen Rechnerkanälen und dem Vergleich der Eingabe-, Prüf-, Zwischen- und Ausgabedaten mittels Software in den Rechnerkanälen selbst.

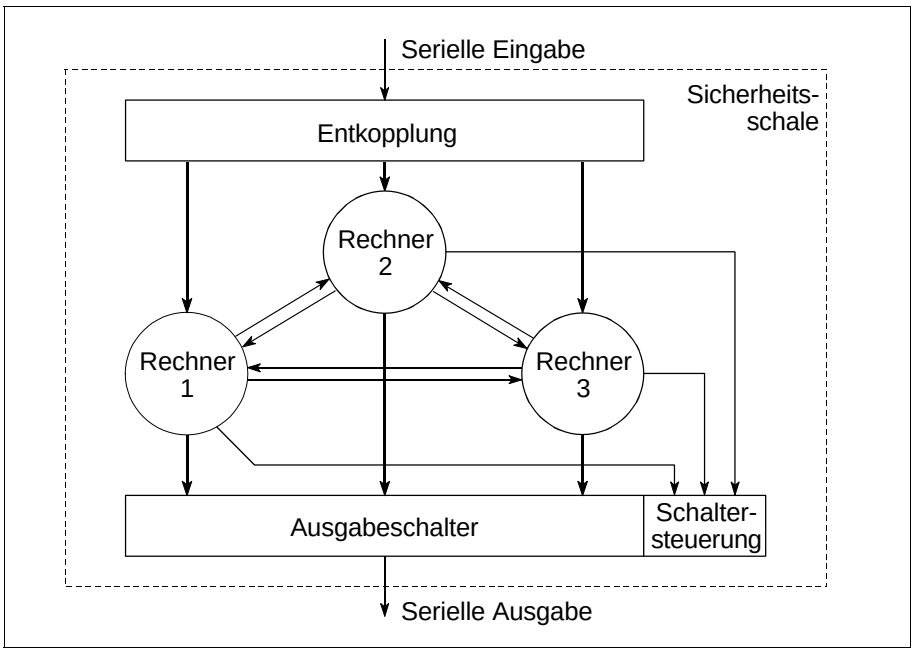


Abbildung 8: Der Sicherheitsbaustein SELMIS

Um eine hohe Verfügbarkeit zu erreichen wurde für die Rechner des El L vorrangig die 2v3-Konfiguration gewählt. Zwei Rechnerkanäle wechseln sich in der Ausgabe von Daten zyklisch ab, während der dritte Kanal als heiße Reserve mitläuft. Auf ihn wird im Störungsfall unmittelbar und ohne Betriebsbehinderung automatisch umgeschaltet. Im Betrieb mitlaufende Prüfprogramme stellen sicher, daß Ausfälle nicht nur schnell entdeckt, sondern auch gezielt Hinweise zur Fehlerbeseitigung gegeben werden [9].

2.1.2 Datenübertragung

Die sicheren Mikrorechnerbausteine werden über serielle Schnittstellen miteinander verbunden. Im SELMIS-Baustein erfolgt die Berechnung der Coderedundanz und die Parallel-Serien-Wandlung in mindestens zwei unabhängigen Rechnern. Analog wird im Empfängerbaustein verfahren. Zur Sicherung der Nachrichtenübertragung werden zwei Verfahren kombiniert: Einzeltelegrammsicherung durch Coderedundanz und antivalente Doppeltelegramme.

2.1.3 Bedienung und Anzeige

Die Sicherheit in Bedienung und Anzeige wird analog des BPS 900 von SIEMENS durch zyklische Umschaltung des Meldebildes auf den Monitor und durch die KF-Taste erreicht. Die Umschaltung der Anzeige stellt das Bildschirmmodul (BM) sicher, das, wie die SIDOS, aus zwei unabhängigen Grafiksystemen aufgebaut ist.

2.2 Systemstruktur

2.2.1 Hardwarearchitektur

Bereits bei der Entwicklung des El L wurde eine Einteilung in vier Ebenen vorgenommen, die dem Drei-Ebenen-Modell plus einer externen Ebene entspricht. Daß das Bedienplatzsystem von SEL im grundsätzlichen Aufbau dem von SIEMENS entspricht, liegt an der Spezifizierung durch die DB AG. Ein Unterschied zum Bedienplatzsystem von SIEMENS ist, daß sich direkt an das Stellwerk ein örtlicher Bedienplatz ohne Arbeitsplatzrechner (El S: Bedienplatzrechner) anschließen läßt.

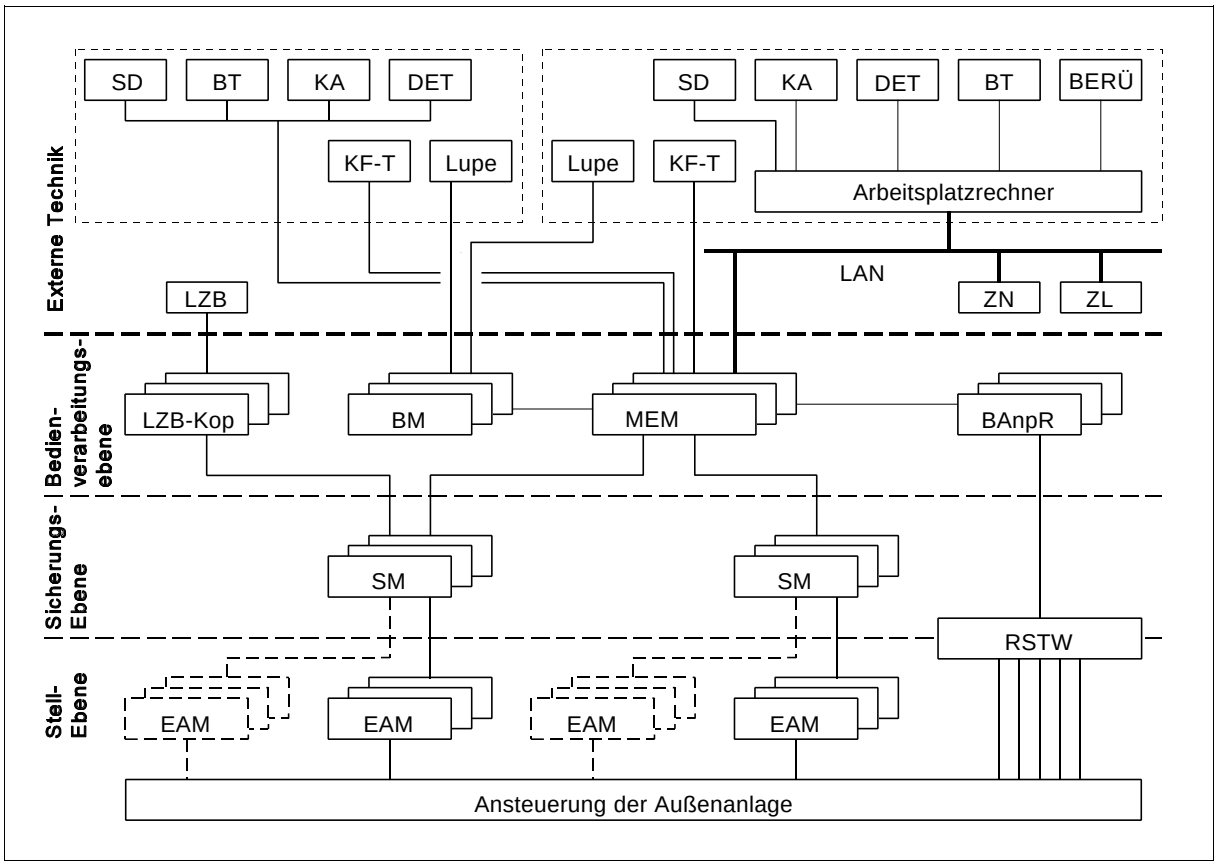


Abbildung 9: Systemstruktur des ESTW El L

BAnpR	Bedienanpaßrechner	Lupe	Lupenbildmonitor
BERÜ	Bereichsübersicht	LZB-Kop	LZB-Koppelbaustein
BT	Bedientablett	MEM	Melde- und Eingabe-Modul
BM	Bildschirm-Modul	RSTW	Relaisstellwerk
DET	Dateneingabetastatur	SD	Störungsdrucker
EAM	Elementansteuer-Modul	SM	Sicherungs-Modul
KA	Kontrollanzeige	ZL	Zuglenkung
KF-T	KF-Taste	ZN	Zugnummernmeldeanlage

In der Bedienverarbeitungsebene arbeitet das Melde- und Eingabe-Modul, dessen Aufgaben mit denen des BAR 16 vergleichbar sind. Die Trennung der Funktionen des Zentral- und Peripherierechners, die beim El S im BSTR vereint wurden und somit die Grenze zwischen diesen Ebenen hardwaremäßig verschwimmen ließ, ist im El L in Form des Sicherungs-Moduls (Sicherungs-

ebene) und des Elementansteuer-Moduls (Stellebene) gegeben. Ein weiterer Unterschied zum El S ist, daß die LZB nicht über das externe Netzwerk, sondern über einen Koppelbaustein an den Zentralrechner (Sicherungsmodul) angeschlossen wird. Auch im El L läßt sich ein Relaisstellwerk über einen Bedienanpaßrechner integrieren.

2.2.2 Rechner und Verstärker

Kennzeichnend für die Bedien-, Zentral- und Peripherierechner ist, daß sie in der 2v3-Konfiguration des SELMIS eingesetzt werden. Nach Aussage von SEL hat sich die Strategie, handelsübliche Komponenten einzusetzen, bewährt. Die Leistungsfähigkeit der in den Modulen eingesetzten Rechner wurde den bisherigen Anforderungen gerecht und kann auch weiterhin durch neuere Rechner an erhöhte Anforderungen angepaßt werden [10].

2.2.2.1 Bedienrechner

Das Melde- und Eingabe-Modul (MEM) bearbeitet die Eingaben des Fahrdienstleiters und der Betriebsleitkomponenten und gibt die geprüften Stellanforderungen an die Sicherungsebene weiter. Die aus der Sicherungsebene zu verteilenden Meldeinformationen werden von ihm aufgeschlüsselt und an das Bildschirm-Modul, die Kontrollanzeigen und den Störungsdrucker weitergegeben [9].

2.2.2.2 Zentralrechner

Das Sicherungs-Modul (SM) bearbeitet die zentralen Stellwerksfunktionen wie Prüfung, Sicherung und Auflösung von Fahrstraßen. Bei größeren Stellwerken können mehrere Sicherungs-Module seriell gekoppelt werden.

Die im SM auf Zulässigkeit geprüften Stellanforderungen aus der Bedienverarbeitungsebene werden bei positivem Ergebnis an die Stellebene weitergeleitet. Element- und fahrstraßenspezifische Zustände, wie Verschlüsse, Sperren, aus der Stellebene übermittelte aktuelle Elementzustandsdaten sowie weitere interne Zustände, die sich aus der Verknüpfung der Elemente zu Fahrstraßen ergeben, werden im SM gespeichert. Ebenfalls gibt es die daraus resultierenden aktuellen Daten zur Meldebilderstellung an die Bedienverarbeitungsebene weiter. Die aus der Stellebene übermittelten Belegungsmeldungen werden auf korrekte Folge von Belegt- und Freimeldungen der einzelnen Abschnitte geprüft, woraus die Haltstellung von Signalen und die Auflösung von Fahrstraßen abgeleitet werden [9].

2.2.2.3 Peripherierechner

Die zentral oder dezentral angeordneten Elementansteuer-Module (EAM) sind die Rechner der Stellebene. Sie sind über serielle Schnittstellen mit dem jeweils übergeordneten Sicherungs-Modul verbunden und haben die Aufgabe, die Elemente der Außenanlage zu steuern und zu überwachen.

Neben der SELMIS-Logik enthalten die EAM einen Ansteuerungsteil mit Energieschaltern und Überwachungseinrichtungen für die Außenanlagen. Die Struktur der Module erlaubt es, sowohl vorhandene Außenanlagen in Relaistechnik als auch elektronische Außenanlagen zu steuern und zu überwachen [9].

2.2.2.4 Diagnoserechner

Ein spezieller Rechner zur Diagnose ist nicht vorhanden; diese Funktionen werden vom MEM wahrgenommen, der seine Diagnosedaten über die reguläre Ausgabeperipherie zur Verfügung stellt.

2.2.2.5 Leistungsschalter

Bei den ersten El L wurde dem Wunsch der damaligen DB entsprochen, die herkömmlichen Relaisschnittstellen der Außenanlage zu verwenden. Diese wurden in langer Entwicklung zusammen mit den Relaisgruppen der Spurplanrelaisstellwerke optimiert und stellen eine kostengünstige Lösung dar. Allerdings konnten diese Lösungen für andere Bahnverwaltungen nicht verwendet werden, da diese eine weitgehende Reduzierung elektrisch aktiver Elemente am Gleis fordern. Außerdem verlangte die Ansteuerung von Ks-Signalen nach neuen Lösungen.

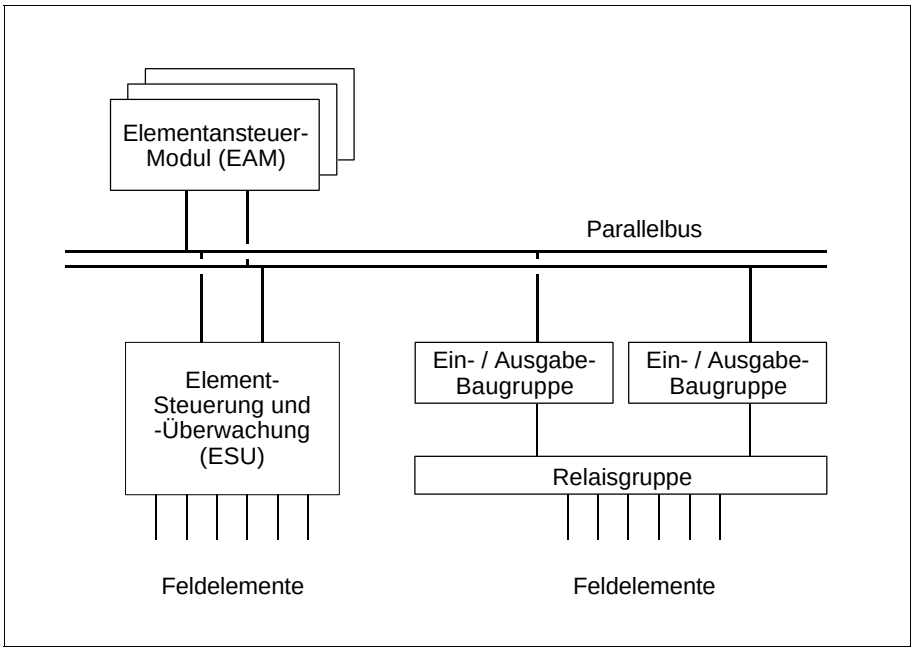


Abbildung 10: Mögliche Ansteuerungen der Außenanlage

Das mittelfristige Ziel, die zahlreichen Relaisschaltungen durch wenige Elektronik-Baugruppen zu ersetzen, wurde durch Einsatz der elektronischen Signalansteuerung erreicht. Die neue elektronische Ansteuerung wird als Element-Steuerung und -Überwachung (ESU) bezeichnet und im Rechnerraum untergebracht. Neben der Typisierung von Baugruppen wurde verlangt, daß ein EAM sowohl die bisherige Relaisgruppe, als auch eine ESU ansteuern kann. Die bisherige Schnittstelle stellt der redundant aufgebaute Parallelbus dar; er wird somit auch als Schnittstelle für die ESU genutzt. Die Protokolle sind miteinander kompatibel.

Kernstück der ESU ist die Elementsteuerlogik mit 16 Bit-Prozessor, die abweichend von der sonst verwendeten 2v3-Konfiguration als ein 2v2-Rechnersystem aufgebaut ist. Sie steuert und überwacht die eigentliche Außenanlage mit Hilfe der Elementleistungsschaltung. Der Elementspeicher enthält projektierte Daten. Die Verbindung zum EAM erfolgt über redundante Buskoppler.

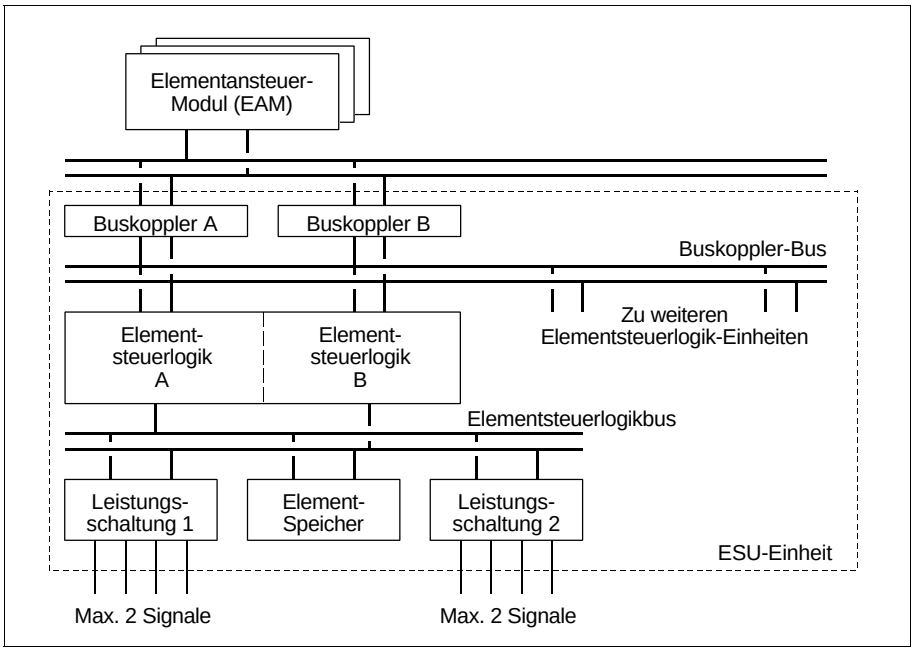


Abbildung 11: Struktur der ESU-Einheit für Lichtsignale

Um die ESU auf bestimmte Bedürfnisse abzustimmen, ist nur der Elementleistungsschalter als besonderer Baugruppentyp auszuführen. Alle anderen Baugruppen bleiben gleich. Die ESU für Signale kann maximal 8 Lampenstromkreise ansteuern [11].

Der oben angesprochene Verzicht auf aktive Elemente und damit Intelligenz am Signal stellt einen wesentlichen Unterschied zum El S dar. Dort befindet sich durch die Signalmodule Intelligenz am Signal, was eine adersparende Verbindung Stellwerk – Signal ermöglicht. Im El L dagegen wird der Vorteil, alle aktiven Elemente im zentralen oder ausgelagerten Rechnerraum unterzubringen, mit dem Nachteil aderintensiver Signalansteuerung erkauft.

2.2.3 Interne Kommunikation

Ein spezielles Bussystem zur Kopplung der Rechner wie im El S ist im El L nicht vorhanden; die Rechner werden über genormte serielle Schnittstellen, die aus Verfügbarkeitsgründen verdoppelt sind, miteinander verbunden. Dies fügt sich in die Philosophie ein, handelsübliche Komponenten zu nutzen. In der Stellebene wird dieser konsequente Weg verlassen; dort werden spezielle Parallelbussysteme eingesetzt. Die Kommunikation erfolgt in jedem der Fälle mit Telegrammen.

2.2.4 Leistungsfähigkeit

Die einzelnen Module besitzen folgende Maximalkapazität:

- BM: 4 Monitore bzw. 20 aufschaltbare Bilder
- MEM: 4 SM, 2 BM, 2 BAnpR
- SM: 4 EAM, 1 LZB-Koppelmodul, 508 Elemente
- EAM: 126 Feldelemente [17].

Für sehr große Stellwerke können mehrere MEM eingesetzt werden. Eine obere Grenze ist dabei mit etwa 2000 Elementen erreicht.

2.3 Software

2.3.1 Struktur und Logikmodell

Der Ablauf der Software erfolgt durch eine zyklische Folge von Bearbeitungen. Jede begonnene Bearbeitung wird nur durch einen zyklischen Interrupt zur Behandlung der seriellen Schnittstellen kurzzeitig unterbrochen, dann aber fortgesetzt und vollständig zu Ende bearbeitet. Auf diese Weise kann eine Bearbeitung nicht durch eine andere unterbrochen werden.

Ähnlich der Softwareeinteilung im El S wird auch die Software des El L strukturiert. SEL unterscheidet zunächst in Grund- und Stellwerkssoftware. Die **Grundsoftware** ist in allen SELMIS-Bausteinen gleich. Sie hat die Aufgabe, die Aufrufe der stellwerksspezifischen Software zu steuern, die Informationen von und zu den Schnittstellen aufzubereiten und den Gleichlauf der Rechner zu garantieren. Die **Stellwerkssoftware** untergliedert sich weiterhin in die

- allgemeinen Stellwerksfunktionen,
- bahnspezifischen Stellwerksfunktionen und
- projektabhängigen Daten.

Modulabhängig sind die allgemeinen Stellwerksfunktionen. Es sind jedoch für alle ESTW-Größen die gleichen. In den bahnspezifischen Stellwerksfunktionen sind die Anforderungen der einzelnen Bahnverwaltungen implementiert. Die projektabhängigen Daten beinhalten das Gleisbild und die Art der Elemente des jeweils projektierten Stellwerks. Sie werden durch Projektierungstools erstellt. Die Projekt-Software besteht aus den Elementdatensätzen, welche die Elemente der Bahnanlage beschreiben, und aus den Fahrstraßentabellen (Verschlußtabellen), welche die Fahrstraßen oder die Fahrstraßenteile enthalten, die im Bereich des jeweiligen Sicherungs-Moduls liegen. Diese statischen Beschreibungsteile der Projekt-Software werden durch dynamische Daten ergänzt, welche den jeweils aktuellen Zustand eines Elementes wiedergeben.

Die Fahrstraßentabellen enthalten eine Auflistung aller Elemente, die zu der jeweiligen Fahrstraße gehören. Des weiteren ist in der Tabelle für jedes beteiligte Element ein Beanspruchungsfall eingetragen. Damit wird vorgegeben, nach welchen Algorithmen das Element in dieser Fahrstraße zu behandeln ist [12].

2.3.2 Projektierung

Die Projektierung erfolgt mittels einer „Projektierungstoolchain“, d.h. eine über eine Datenbank verkettete Anzahl von Programmen, mit denen die spezifischen Projektierungen der Hard- und Software durchgeführt werden. Im einzelnen sind das folgende Programme:

- PROMAT – Projektierung und Materialisierung der Hardware
- PROSOFT – Projektierung der Softwaredaten für MEM und SM
- PROFAHR – Projektierung der Fahrstraßenlisten
- PROMON – Projektierung der Monitorbilder
- PROGRAF – Projektierung des Grafiktabletts.

Generell werden alle Daten eines Bauvorhabens in einer zentralen Datenbank gespeichert. Zunächst wird über die Eingabe des Elementverbindungsplanes (EVP) ein leerer Datensatz für jedes Element erzeugt, der anschließend vom Projektant mittels Bildschirmmasken in Bezug auf Hardware der Innen- und Außenanlage sowie Software-Funktionalität gefüllt wird [10]. Im Gegensatz zum El S, bei dem der EVP Bestandteil der anlagespezifischen Daten ist, werden beim El L aus dem EVP erst Fahrstraßenlisten erstellt, die dann Bestandteil der projektabhängigen Daten werden.

2.4 Externe Einflußnahme

2.4.1 Allgemeines

Das El L läßt sich in eine Betriebszentrale integrieren, wobei auch mehrere Stellwerke an die Zentrale angeschlossen werden können. Realisiert wurde dieses bereits an der 471 km langen Hochgeschwindigkeitsstrecke Madrid – Sevilla mit 21 Bahnhöfen bzw. Überleitstellen, 9 ESTW El L und der Betriebsleitzentrale Madrid [10]. Auch die Einbindung eines Relaisstellwerkes in eine solche Zentrale ist möglich.

Weiterhin können ZN-Funktionen sowie ZL-Anlagen integriert werden. SEL bietet für die Zuglenkung das System „ZLL 800“ an, auf das hier nicht näher eingegangen werden soll. Bis auf die LZB, für die ein eigenes Koppelmodul verwendet wird, werden die externen Techniken über ein LAN angeschlossen, das „Betriebsleittechnikbus“ genannt wird.

2.4.2 Bedienplatz

Der Bedienplatz, von SEL „BO L900“ genannt, unterscheidet sich in der Geräteausstattung nicht wesentlich vom BPS 900 von SIEMENS. Wie bereits erwähnt, liegt das in der Spezifikation der DB AG begründet.

Um den Informationsinhalt mehrerer Lupenbilder oder der Bereichsübersicht auch einem größeren Kreis (Disponent, Fahrdienstleiter, Zugansage u.a.) zur Kenntnis zu bringen, ist die Video-Projek-

tion als flexibler Meldetafelersatz geeignet. In den ersten ESTW von SEL wurde die Auflichtprojektion und die Durchlichtprojektion erprobt, wobei sich letztere bei der das Bild auf die Rückseite der Leinwand projiziert wird, für die Raumhelligkeit günstiger erwiesen hat [15]. Je nach Einsatzfall wird der Projektor wie die Bereichsübersicht oder die Lupe angesteuert. Somit kann die Projektion auch ein sicheres Meldebild anzeigen.

Während die Vidoeprojektion in vielen ausländischen Betriebszentralen zum Standard gehört, hat sie sich in Deutschland nicht oder noch nicht durchgesetzt. In allen neuen ESTW setzt die DB AG ausschließlich Monitore zur Meldungsausgabe ein.

3 ELEKTRA (Alcatel Austria)

Mitte der achtziger Jahre entschloß sich die Österreichische Bundesbahn (ÖBB) elektronische Stellwerke in ihrem Netz einzuführen. Nach Ausarbeitung der Pflichtenhefte wurde im September 1987 mit den österreichischen Signalbaufirmen Alcatel Austria AG und Siemens AG Österreich ein Rahmenvertrag für die Entwicklung von ESTW sowie die Errichtung je eines Prototypstellwerks abgeschlossen. Dieser Vertrag gewährte den Firmen größtmögliche Freiheit bezüglich der technischen Lösung, denn nur dadurch – so die Auffassung der ÖBB – war es ihnen möglich, den gestellten Bedingungen von Sicherheit und Wirtschaftlichkeit gerecht zu werden [13].

Während SIEMENS das ESTW El S den Forderungen der ÖBB anpaßte und es dort unter dem Namen „SMC 86“ verkaufte, entwickelte Alcatel Austria, ein Tochterunternehmen des ALCATEL-Konzerns, das Stellwerkssystem „ELEKTRA“. Sämtliche Basistechnologien, die in ELEKTRA implementiert sind, werden auch in öffentlichen und privaten Kommunikationssystemen des ALCATEL-Konzerns verwendet. Teilweise waren diese Technologien bereits vor der Entwicklung des Systems ELEKTRA im Einsatz. Durch die gemeinsame Nutzung der Basistechnologien in den verschiedenen Produktlinien ist es ALCATEL gelungen, Kostenvorteile in Entwicklung und Wartung zu erzielen [13].

Beim Vergleich des ESTW El L (ALCATEL SEL) und des ESTW ELEKTRA (Alcatel Austria) sind einige Gemeinsamkeiten zu verzeichnen, obwohl sie vollkommen unabhängig voneinander entwickelt wurden. Dazu gehören beispielsweise die Wahl handelsüblicher oder zumindest auch außerhalb der Sicherungstechnik eingesetzter Rechner und die Art der Datenübertragung. Die Ursache hierfür liegt wahrscheinlich darin, daß beide Firmen in der Branche der Kommunikationstechnik ihre Wurzeln haben. Außerdem ist der ALCATEL-Konzern, dem beide Unternehmen angehören, ebenfalls dieser Branche zuzuordnen.

Das erste ESTW ELEKTRA ging 1989 in Betrieb. Zum Jahresende 1995 waren in Österreich 20 Stellwerke dieser Bauform im Einsatz. Weiterhin bestehen Verträge mit der SBB und mit Ungarn.

3.1 Sicherheits- und Verfügbarkeitskonzept

3.1.1 Datenverarbeitung

Um die Sicherheitsanforderungen zu erfüllen, werden alle sicherheitsrelevanten Aktionen grundsätzlich zweikanalig verarbeitet. Deshalb ist das System in einen Logikkanal (A) und einen Sicherheitskanal (Safety Bag, B) geteilt [13]. Das bedeutet, daß hier die Sicherheitsredundanz auf Systemebene realisiert wird, während das bei allen anderen Systemen, die Hardwareredundanz zur Gewährleistung der Sicherheit nutzen, auf Baugruppen- oder Geräteebene geschieht! Außerdem wird bei ELEKTRA streng zwischen der Implementierung des Sicherheits- und des Verfügbarkeitskonzeptes getrennt. Eine hohe Verfügbarkeit wird durch redundante Rechner, die nach dem VOTRICS-Prinzip arbeiten, erreicht. Die Sicherheit wird durch das zweikanalige, diversitär programmierte System gewährleistet.

Safety Bag-Verfahren

Eingegebene Befehle werden zuerst im Logikkanal nach betrieblichen und sicherheitsrelevanten Bedingungen geprüft; bei positivem Ergebnis wird die Ausgabe an die Elemente der Außenanlage vorbereitet. Vor der Ausgabe erfolgt jedoch eine Rückfrage an den Sicherheitskanal, um zu überprüfen, ob das Ergebnis des Logikkanals tatsächlich zu keinem gefährlichen Zustand führt (Safety-Bag-Verfahren). Wenn auch diese Bearbeitung zu einem positiven Resultat führt, geben beide Kanäle die erforderlichen Stellbefehle an eine Relaisschnittstelle aus. In dieser Schnittstelle erfolgt ein nochmaliger Hardware-Vergleich der beiden Kommandos, bevor letztendlich die Elemente der Außenanlage angesteuert werden [18].

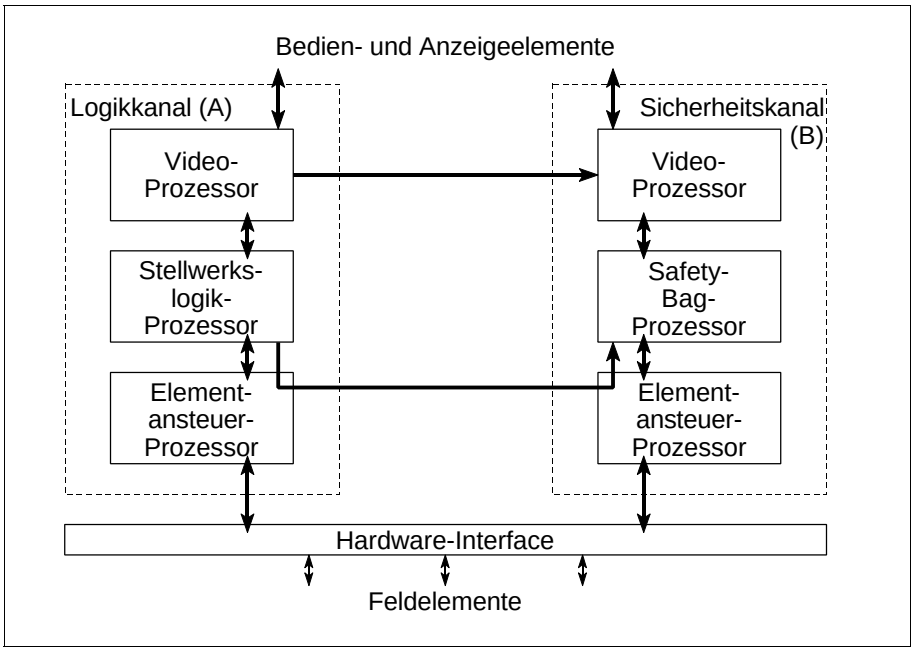


Abbildung 12: Sicherheitsstruktur des Systems ELEKTRA

Diversitäre Software

Alcatel Austria geht davon aus, daß es nach dem heutigen Stand der Technik nicht möglich ist, die Software eines komplexen Echtzeitsystems (wie die eines ESTW) fehlerfrei zu realisieren. Aus diesem Grund wird in den zwei Rechnerkanälen diversitäre Software eingesetzt. Um ein Maximum an Diversität zu erreichen, wurde sorgfältig spezifiziert. Das ist notwendig, um die Möglichkeit von gemeinsamen Fehlern zu minimieren, bei welchen zur selben Zeit unter denselben externen Bedingungen ein Software-Entwurfsfehler in beiden Kanälen zum gleichen falschen Resultat führt.

Die Software des Logikkanals ist in der prozeduralen Programmiersprache CHILL implementiert. Im Sicherheitskanal wird in der Sicherungsebene die regelorientierte Programmiersprache PAMELA verwendet, welche auf CHILL übersetzt wird. Diese Regeln sind eine direkte Festlegung der sicherheitsrelevanten Abhängigkeiten. Da das auf CHILL übersetzte Programm völlig unterschiedlich zu den CHILL-Programmen im Logikkanal ist, wird die Möglichkeit gemeinsamer

Fehler minimiert. In den Rechnern der Bedienebene wird in beiden Rechnerkanälen CHILL verwendet, wobei am Beginn des Designs die Merkmale der Diversität definiert werden (z. B. unterschiedliche Algorithmen) [18].

Das fehlertolerante Kommunikationssystem VOTRICS

VOTRICS (**Vo**ting **Tri**ple Modular Redundant **C**omputing **S**ystem) ermöglicht die Realisierung der Systemarchitektur des ELEKTRA mit einfach-, zweifach- und dreifachredundanten Systemkomponenten. Diese Redundanz dient nur zur Erhöhung der Verfügbarkeit. VOTRICS ist von den eigentlichen Anwenderprogrammen unabhängig und dient der Verwaltung, dem synchronen Betrieb, der Fehlererkennung und der Wiedereinbindung von Systemkomponenten. Um diese Technologie sowohl breit einsetzen zu können als auch die permanent erfolgende Weiterentwicklung auf dem Gebiet der Rechnertechnologie leicht nutzbar zu machen, ist VOTRICS durch Software realisiert.

In der dreifach redundanten Konfiguration wird jeder Hardware-Fehler erkannt; durch einen 2v3-Vergleich der Rechnerergebnisse wird ein defekter Rechner eindeutig identifiziert. Das übereinstimmende Resultat der beiden anderen Rechner wird als das richtige weitergeleitet. Damit können beliebige Fehler der Rechnerhardware unabhängig von ihren Auswirkungen toleriert werden.

Die gleichen VOTRICS-Mechanismen werden für zweifach redundante Systemkomponenten eingesetzt. Da in dieser Konfiguration kein Mehrheitsentscheid möglich ist, wird die Diagnose des fehlerhaften Rechners durch zusätzliche Entscheidungshilfen (z. B. Selbstprüfungen) unterstützt.

Sämtliche VOTRICS-Mechanismen zur Verwaltung der Redundanz werden ebenfalls in drei- bzw. zweifacher Redundanz ausgeführt. Dadurch kann auch ein einzelner Hardwarefehler, der die VOTRICS-Mechanismen beeinträchtigt, nicht zum Ausfall aller redundanten Rechner einer Systemkomponente führen [18].

3.1.2 Datenübertragung

Über die Sicherung der Datenübertragung konnte nichts näheres ermittelt werden. Da die Kommunikation ähnlich der SEL-Lösung arbeitet (Punkt-Punkt-Verbindung), kann angenommen werden, daß auch die Sicherung in ähnlicher Form erfolgt.

3.1.3 Bedienung und Anzeige

Wie die DB AG fordert auch die ÖBB Sicherheit in Bedienung und Anzeige. Durch den grundsätzlich zweikanaligen Aufbau des ESTW ELEKTRA sind für die Realisierung dieser Forderung bereits gute Voraussetzungen gegeben.

Die Ansteuerung der Monitore geschieht etwa im Sekundentakt abwechselnd aus den beiden Kanälen. So wird, wie beim BPS 900, bei Unstimmigkeiten in den Kanälen ein blinkendes Bild erzeugt, das die Aufmerksamkeit des Bedieners auf sich zieht.

Die Eingabe dokumentationspflichtiger Bedienhandlungen geschieht folgendermaßen: Zunächst werden das Element und das Gruppenfunktionssymbol auf dem Bildschirm mit der regulären Eingabeperipherie aktiviert. Diese Eingabe erfolgt nur in den Logikkanal, von dort wird sie in den Sicherheitskanal übertragen. Von beiden Kanälen erfolgt die gleiche Kennzeichnung des aktivierten Symbols am Bildschirm. Der Bediener muß sich nun davon überzeugen, ob das System seinen Befehl richtig interpretiert hat. Bei positivem Ergebnis hat er 10 Sekunden Zeit, um die „Ausführungstaste“ (DB AG: KF-Taste), die mit beiden Kanälen verbunden ist, zu betätigen [13].

3.2 Systemstruktur

3.2.1 Hardwarearchitektur

Die aus der gewählten Sicherheitsphilosophie entstammende Einteilung in Logikkanal und Sicherheitskanal sowie die Trennung des Sicherheits- und Verfügbarkeitskonzeptes drückt sich deutlich in der Hardwarearchitektur aus. Das Drei-Ebenen-Modell läßt sich ohne weiteres auf ELEKTRA übertragen.

Die Bedienverarbeitungsebene bilden die Video Control Computer (VC-A, VC-B), die mit Hilfe der Bildschirmsteuerung die Monitore des Bedienplatzes ansteuern. Die zentrale Stellwerkslogik in der Sicherungsebene bearbeiten die Central Control Computer (CC-A, CC-B) mit dem Stellwerkslogikprozessor (Interlocking Processor, ILP) und dem Safety Bag Prozessor (SBP). Für Diagnosezwecke steht ein Diagnostic Processor (DGP) zur Verfügung, mit dem der Instandhalter über einen PC kommunizieren kann. Außerdem steht ein Drucker als Anzeigemedium zur Verfügung.

In der Stellebene steuern die Peripheral Control Computer (PC-A, PC-B) über ein Relaisinterface die Elemente der Außenanlage an. Die Ansteuerung eines Relaisstellwerks ist ebenfalls möglich. Durch dezentrale Anordnung der Peripherierechner besteht die Möglichkeit, große Bereiche zu steuern. Seitens der ÖBB wurde für die Datenfernübertragung die standardisierte Schnittstelle X.25 vorgegeben, über die sowohl sicherer als auch nicht sicherer Datenaustausch zu ausgelagerten Stellrechnern und zu peripheren Systemen stattfindet.

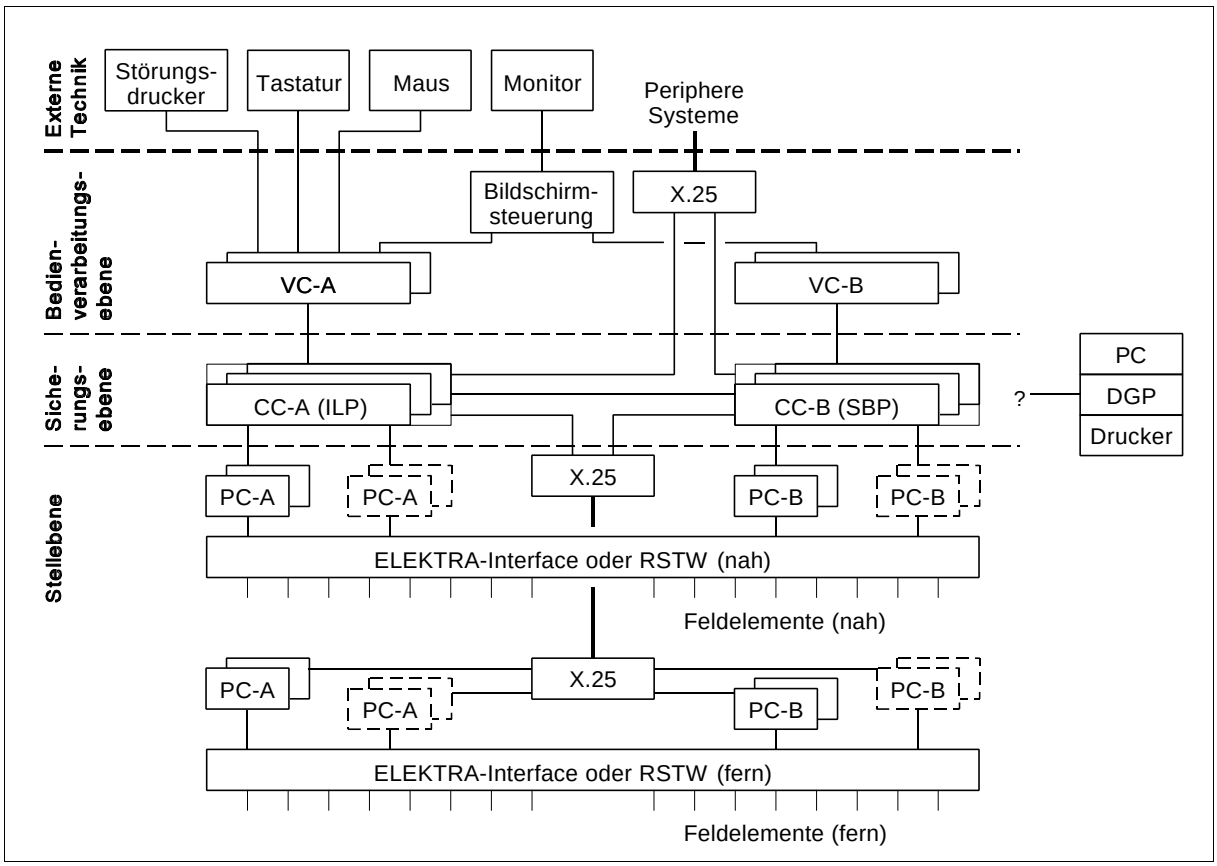


Abbildung 13: Systemstruktur des ESTW ELEKTRA

CC-A, CC-B	Central Control Computer	RSTW	Relaisstellwerk
DGP	Diagnostic Processor	SBP	Safety Bag Processor
ILP	Interlocking Processor	VC-A, VC-B	Video Control Computer
PC	Personalcomputer	X.25	Genormte serielle Schnittstelle X.25
PC-A, PC-B	Peripheral Control Computer		

3.2.2 Rechner und Verstärker

3.2.2.1 Bedienrechner

Der Bedienrechner wird zwar Video Control Computer (VC-A, VC-B) genannt, nimmt aber auch die Bedieneingaben entgegen und führt eine erste Vorverarbeitung durch. VC-A und VC-B arbeiten zweifach redundant nach dem VOTRICS-Prinzip.

Für den Bedienrechner werden Komponenten aus der Alcatel-Prozeßrechnerfamilie 16-Plus verwendet. Die zentralen Rechnerbaugruppen basieren auf Mikroprozessoren der Reihe 80286 und 80486 [13].

3.2.2.2 Zentralrechner

Im Zentralrechner, hier Central Control Computer (CC-A, CC-B) genannt, wird die Stellwerkslogik realisiert. Um sicherheitsrelevante Zwischenergebnisse auszutauschen, ist der Stellwerksprozessor des CC-A direkt mit dem Safety Bag Prozessor des CC-B verbunden. Es soll noch

einmal erwähnt werden, daß im Sicherheitskanal und damit im CC-B nur die sicherheitsrelevanten Bearbeitungen parallel ausgeführt werden.

CC-A und CC-B sind jeweils dreifach redundant gestaltet und arbeiten nach dem VOTRICS-Prinzip. Die einzelnen Rechner entstammen, wie beim Bedienrechner, ebenfalls der Prozeß-rechnerfamilie 16-Plus [13].

3.2.2.3 Peripherierechner

Die Peripherierechner (Peripheral Control Computer; PC-A, PC-B) steuern die Relaisinterfaces oder Relaisstellwerke. Ihre Anzahl richtet sich nach dem Umfang der zu steuernden Anlage.

Es werden Komponenten der Prozeßrechnerfamilie 0802 verwendet, die auf Mikroprozessoren der Reihe 8085 aufbauen. Wie die Bedienrechner, arbeiten die Peripherierechner zweifach redundant nach dem VOTRICS-Prinzip [13].

3.2.2.4 Diagnoserechner

Ein effizientes Wartungshilfsmittel ist der Diagnostic Processor (DGP), mit dessen Hilfe interne Anlagenzustände, Zustände der Außenanlage und Bedienvorgänge am ESTW abgefragt werden können. Zusätzlich bietet der DGP dem Wartungspersonal auch noch direkte Unterstützung beim Auffinden defekter Leiterplatten, indem Informationen über die Baugruppen abgefragt werden können, welche für ein bestimmtes Element der Außenanlage relevant sind [13].

Wie der DGP an das Stellwerk angeschlossen wird, war nicht genau zu ermitteln. Vermutlich wird der DGP – gemäß der sonstigen Hardware – über eine serielle Schnittstelle mit den wichtigsten Rechnern des Systems verbunden sein.

3.2.2.5 Leistungsschalter

Als Leistungsschalter im „ELEKTRA-Interface“ kommen Sicherheitsrelais auf Leiterplatten zum Einsatz. Hier erfolgt ein nochmaliger Hardware-Vergleich der Kommandos aus Logik- und Sicherheitskanal.

3.2.3 Interne Kommunikation

Die interne Kommunikation erfolgt über genormte serielle Schnittstellen. Leider konnten auch hier keine genauen Angaben zu Aufbau und Art der Datenübertragung zwischen den Rechnern im Nahbereich gewonnen werden.

Für die Datenfernübertragung zu ausgelagerten Peripherierechnern und für die Datenübertragung zu externen Techniken wird die bereits genannte genormte Schnittstelle X.25 verwendet. Sie ist kompatibel zum öffentlichen DATEX-P-Netz. Über eine physikalische Verbindung können gleich-zeitig mehrere virtuelle Links hergestellt werden. Bei der sicheren Übertragung werden zwei derartige Links zwischen den Komponenten des System ELEKTRA und/oder den externen

Techniken hergestellt. Sichere Verbindungen werden über eigene Übertragungsleitungen (Fernmeldekabel oder LWL) geführt, während für den nicht sicheren Datentransfer öffentliche Netze verwendet werden [13].

3.2.4 Leistungsparameter

Daten zur Leistungsfähigkeit lagen nicht vor.

3.3 Software

3.3.1 Struktur und Logikmodell

Wie die Software strukturiert ist, war aus der verwendeten Literatur nicht ersichtlich. Aus [14] geht hervor, daß die Fahrstraßenlogik in „Fahrstraßenlisten“ (Verschlußtabellen) realisiert wird.

3.3.2 Projektierung

Zur Projektierung von ELEKTRA wurde das interaktive Projektierungstool ELEPRO entwickelt, welches eine UNIX-Applikation ist. Ausgehend vom später auf dem Monitor ersichtlichen Gleisbild wird dabei die Topologie der Bahnanlage mit allen Funktionsbedingungen im Dialog mit dem Projektierungstool erstellt. Nach Abschluß der Eingabe aller Projektierungsdaten erstellt das Tool die für das Stellwerkssystem erforderlichen Datenbanken und ermöglicht die Programmierung der EPROM-Sätze.

Das Programmpaket ELEPRO besteht aus folgenden Komponenten:

- **Bildeditor** zur grafischen Erstellung der Monitorbilder
- **Topologieeditor** zur Eingabe von topologischen Elementen, die nicht am Monitorbild sichtbar sind (z. B. Durchrutschwegende)
- **Elementeditor** zur dialoggesteuerten Eingabe der Funktionsbedingungen jedes Elements
- **Fahrstraßeneditor** zur automatischen Suche aller topologisch möglichen Fahrstraßen und zur Priorisierung von Regel- und Umfahrstraßen
- **Konfigurationstool** zur grafikgestützten Eingabe der Hardwarekonfiguration der Innenanlage und zur automatischen Berechnung der Verdrahtung und Verkabelung.

Der ELEPRO-Compiler erstellt aus der gemeinsamen ELEPRO-Datenbasis die Datenbanken für die verschiedenen Rechnersysteme des ESTW ELEKTRA [14].

3.4 Externe Einflußnahme

3.4.1 Allgemeines

Das Betriebsführungskonzept der ÖBB

Das betriebliche Konzept „Neue Bahn“ der ÖBB baut auf eine weitgehende Automatisierung des Eisenbahnbetriebs auf. Ein zukünftiger integrierter Taktfahrplan mit einem Geschwindigkeitsniveau bis 200 km/h auf den Hochleistungsstrecken sowie ein hoher Anteil an gleichzeitigen Zugfahrten und Mischbetrieb bedingen einen hohen Grad an Pünktlichkeit. Um diese hochgesteckten Ziele zu erreichen, führt die ÖBB das „Betriebsführungssystem“ (BFS) ein. Dieses System besteht im wesentlichen aus drei Ebenen.

In der überregionalen Ebene wird das System „Rechnergestützte Zugüberwachung“ (RZÜ) eingesetzt. Vier derartige Zugüberwachungszentralen bilden die überregionale Disposition im gesamten Netz der ÖBB. Zusätzliche Einzelsysteme wie Wagenstandsanzeiger, Zugzielanzeiger u.a. werden mit den RZÜ zum „Betriebsinformationssystem“ BIS zusammengefaßt. Die regionale Ebene ist für die Steuerung und Disposition des Zugverkehrs innerhalb eines Streckenbereiches bis zu 60 km zuständig. Dafür ist die Entwicklung eines „Betriebsoperationssystem“ (BOS) notwendig. Die lokale Ebene schließlich besteht aus den Stellwerken der einzelnen Bahnhöfe [18].

Das Stellwerks- und Betriebsoperationssystem ELEKTRA

Die funktionellen Anforderungen des BOS wurden während des ELEKTRA-Entwurfs bereits berücksichtigt. Daraus resultierend wurde eine einheitliche Systemarchitektur für das „Stellwerks- und Betriebsoperationssystem ELEKTRA“ entwickelt. Im wesentlichen beinhaltet dieses System das ELEKTRA-Stellwerk im Kern mit der bereits beschriebenen Möglichkeit der Fernsteuerung entfernter liegender Stellbereiche und der Kopplungsmöglichkeit zu externen Techniken. Auch bereits bestehende Fernsteuersysteme können angeschlossen werden, wenn eine Konvertierung zur X.25-Schnittstelle möglich ist.

Die den Eisenbahnbetrieb unterstützenden Funktionen werden als sogenannte „Betriebsführungspakete“ durch Software in der zentralen Rechnerebene des Stellwerks integriert, teilweise aber auch in externe Komponenten ausgelagert. Vollständig im Zentralrechner ist die Zugnummernmeldung realisiert. Durch die Verwendung geeigneter Schnittstellenumsetzer (Serial Peripheral Controller, SPC) können jedoch auch bereits vorhandene, nicht dem Standard entsprechende Schnittstellen vom ELEKTRA-System verarbeitet werden.

In einem eigenen externen Rechner (Disposition Management Computer, DMC), der über einen Massenspeicher verfügt, können die Fahrplandaten für das BOS aufbereitet werden. Weiterhin ist die Implementierung von Funktionen geplant, die, basierend auf Meldungen und Daten von den Fahrleitungsunterwerken, energieoptimiertes Fahren auf Hochleistungsstrecken unterstützen [18].

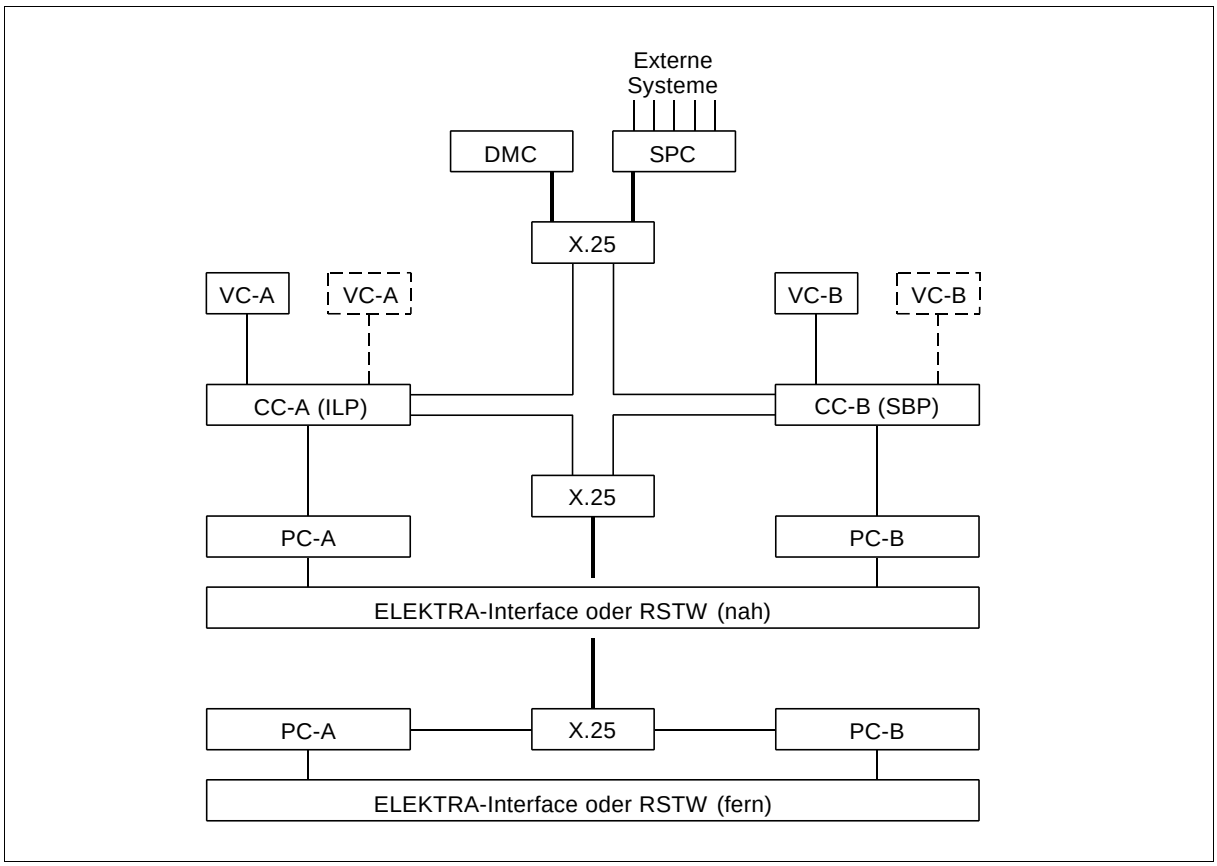


Abbildung 14: Betriebsoperationssystem ELEKTRA-BOS

CC-A, CC-B	Central Control Computer	RSTW	Relaisstellwerk
DMC	Disposition Management Computer	SBP	Safety Bag Processor
		SPC	Serial Peripheral Computer
ILP	Interlocking Processor	X.25	Genormte serielle Schnittstelle X.25
PC-A, PC-B	Peripheral Control Computer		

3.4.2 Bedienplatz

Ebenso wie die DB AG hat die ÖBB, hier unter dem Namen „Einheitliche Bedienoberfläche“ (EBO), einen einheitlichen Bedienplatz spezifiziert. Dieser verwendet Bildschirme für die sichere Anzeige und eine Maus als primäres Eingabemedium.

Abhängig von der Größe des Einflußbereiches und vom Verkehrsaufkommen können in einem Stellwerks- und Betriebsoperationssystem ELEKTRA bis zu zehn Bedienplätze eingerichtet werden. Vermutlich ist für jeden Arbeitsplatz ein Bedienrechner (VC-A, VC-B) notwendig.

Im wesentlichen baut die Mensch-Maschine-Schnittstelle des Systems ELEKTRA auf der Technik des Betriebsführungssystems „VIDEOPULT“ von Alcatel Austria auf, das bisher in großen Relaisstellwerken verwendet wurde [13]. Auf diese Weise konnte bereits auf Erfahrungen in der Gestaltung von rechnergestützten Bedienoberflächen zurückgegriffen werden. Eine wesentliche Neuerung ist, daß die Eingaben nicht mehr mit Lichtstift, sondern mit einer Maus erfolgen.

An einem Bedienplatz können, abhängig von der Größe des gesteuerten Bereichs, bis zu fünf Farbmonitore zum Einsatz kommen. Auf den Monitoren werden einerseits die aktuellen Meldungen des Stellwerks dargestellt, andererseits die Cursorführung der Maus und die jeweiligen Menüfelder zur Eingabe von Stellbefehlen.

4 EBILOCK (ABB)

1978 übergab die schwedische Firma Ericsson Signal das erste ESTW der Welt in Göteborg (Schweden) dem Betrieb. Ericssons Erfahrungen im Signalbau gehen bis in das Jahr 1915 zurück. Inzwischen gehört Ericsson Signal zur Firmengruppe ABB Signal (im folgenden kurz „ABB“ genannt), die dem Asea Brown Boveri (ABB)-Konzern angehört. Mit der Übernahme durch ABB erfolgte auch die Namensänderung des Stellwerks von ERILOCK in EBILOCK. Inzwischen schlossen sich die Verkehrstechnik-Bereiche von ABB und Daimler zur ADTRANZ (**A**BB und **D**aimler bieten **TRAN**sporttechnik von A bis **Z**) zusammen. Ob davon neue Impulse für die ESTW-Technik ausgehen, bleibt abzuwarten; diese Spekulation ist insofern interessant, da die AEG, die bereits erfolglos ein ESTW entwickelte, zum Daimler-Konzern gehörte. Der Verkehrstechnik-Bereich der mittlerweile aufgelösten AEG ging in die ADTRANZ ein.

Wurden in den ersten EBILOCK-Stellwerken noch Relais eingesetzt, um einen fail-safe Vergleich zu erreichen, so werden seit der Version EBILOCK 850 alle Funktionen vollelektronisch realisiert [21]. Nach einiger Zeit des Einsatzes von EBILOCK 850 stellte sich heraus, daß diese Bauform für viele Einsatzzwecke überdimensioniert war. Deshalb erfolgte eine Weiterentwicklung zum EBILOCK 950 mit einer geringeren Kapazität, welches zur Zeit noch nicht im Einsatz ist. Wenn in der folgenden Beschreibung von EBILOCK die Rede sein wird, so sind damit immer die Bauformen EBILOCK 850 und EBILOCK 950 gemeint. Bei Unterschieden in den beiden Versionen wird darauf eingegangen.

EBILOCK ist Teil einer kompletten Produktfamilie von Sicherungssystemen mit einheitlicher Technik. Dazu gehören die elektronischen Stellwerkssysteme (EBILOCK), Streckenblöcke (EBILINE) und Bahnübergangssicherungssysteme (EBIGATE) [22]. Um Betriebszentralen bilden zu können, wird das System EBICOS 900 [23] angeboten; zur Zugbeeinflussung steht das ATC-System EBICAB 700, 800 und 900 [24] zur Verfügung.

EBILOCK ist zur Zeit hauptsächlich in Skandinavien im Einsatz; ABB drängt jedoch zunehmend auf den Weltmarkt. Die Einführung von EBILOCK in Deutschland ist im Moment noch schwierig, da die Sicherheitsstruktur – diversitäre Software auf einkanaliger Hardware – für Eisenbahnsicherungsanlagen hier nicht üblich und nach Mü 8004 auch nicht zugelassen ist. Es bleibt abzuwarten, inwieweit es hier, im Zuge der Liberalisierung des europäischen Marktes und der Einführung von EU-Normen, in Zukunft Veränderungen geben wird.

Meines Erachtens ist die EBILOCK-Familie ein kostengünstiges und modernes System, dessen Einsatz zumindest bei Industriebahnen auch in Deutschland vorstellbar ist. Der bereits viele Jahre währende Einsatz von EBILOCK auf Magistralen, auf denen Hochgeschwindigkeitszüge (X2000) verkehren, zeigt, daß das System Personenverkehr sicher steuern kann, auch wenn es bei theoretischer Betrachtung ein geringeres Sicherheitsniveau bietet (siehe auch Teil III dieser Arbeit).

4.1 Sicherheits- und Verfügbarkeitskonzept

4.1.1 Datenverarbeitung

Alle sicheren Verarbeitungen werden sequentiell von zwei diversitären Programmen (A und B) berechnet. Diese haben zwar identische Funktionen und arbeiten auf einkanaliger Hardware, sie nutzen jedoch die Hardware diversitär (z. B. Benutzung unterschiedlicher Register). Jedes Programm wird von einem eigenen Entwicklungsteam programmiert.

Die Berechnungen der Programme A und B werden nacheinander zum Peripheriерechner übertragen, wo sie verglichen werden. Nur wenn die Ergebnisse übereinstimmen, wird ein Stellbefehl ausgeführt [22]. Ob der Vergleich im Peripheriерechner per Software oder per Hardware erfolgt, ging aus der Literatur nicht hervor. In älteren EBILOCK-Stellwerken (vor Version 850) erfolgte der Vergleich mit Signalrelais. Die nacheinander übertragenen, durch diversiäre Software errechneten Meldungen des Peripheriерechners an den Zentralrechner werden im Zentralrechner durch Software verglichen.

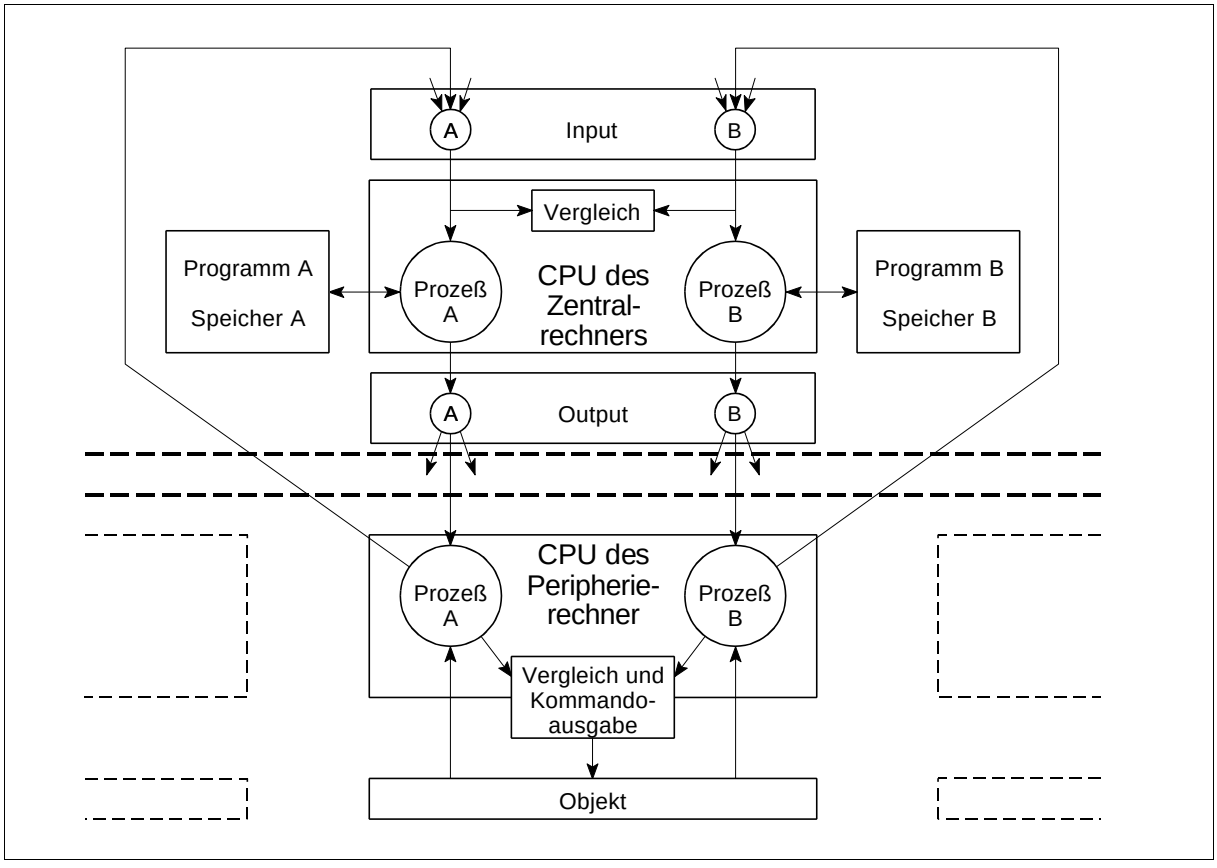


Abbildung 15: Sicherheitsprinzip im EBILOCK-Stellwerk

Um die Verfügbarkeit zu erhöhen, kann der Zentralrechner verdoppelt werden. Der Redundanzrechner erhält ständig alle Daten vom Arbeitsrechner. Es wird garantiert, daß diese nicht älter als 20 Sekunden sind. Nach einer Umschaltung arbeitet der Redundanzrechner mit den Daten weiter und aktualisiert sie gemäß der Meldungen von den Peripheriерechnern. Freigebende Befehle werden jedoch für zwei Minuten blockiert [25].

4.1.2 Datenübertragung

Die interne Datenübertragung wird durch Kabelschleifen realisiert, die am Zentralrechner beginnen und enden. Redundanz in den Telegrammen sorgt dabei für Fehlererkennung. Sollte sich ein Kabelbruch an beliebiger Stelle einer Schleife ereignen, so arbeitet das System ohne Einschränkung weiter [25].

4.1.3 Bedienung und Anzeige

Anforderungen an die Sicherheit in Bedienung und Anzeige werden nicht gestellt.

4.2 Systemstruktur

4.2.1 Hardwarearchitektur

Kern der Anlage ist der Zentrale Sicherheitsbaustein (Interlocking Processor). Für Bedienung und Anzeige steht ein Terminal zur Verfügung, das direkt mit dem Interlocking Processor verbunden ist. Ist die Anlage sehr umfangreich, und sollen weitere Techniken integriert werden, so werden Bedienplatzsysteme vorgesehen. Das oben genannte Terminal wird dann für Instandhaltungszwecke oder als Rückfallebene für die Bedienung genutzt [25].

Die Bearbeitung der Stellwerksfunktionen sowie die Steuerung der Übertragungsschleifen erfolgt im Zentralen Sicherheitsbaustein. Um umfangreiche Anlagen steuern zu können, werden mehrere dieser Bausteine eingesetzt und mit einer seriellen Datenleitung, die zur Erhöhung der Verfügbarkeit redundant ausgeführt wird, verbunden.

Jedes Feldelement hat sein eigenes Objektsteuergerät. Mittels Konzentratoren werden die Objektsteuergeräte in die bereits erwähnten Schleifen eingebunden. Während EBILOCK 850 **dreizehn** solcher Schleifen steuern kann, sind es bei EBILOCK 950 **zwei** Schleifen.

Eine spezielle Kopplung zu einem Zugbeeinflussungssystem (analog LZB-Kopplung) ist nicht notwendig, da die Zugbeeinflussung über Balisen erfolgt, die vom Objektsteuergerät für Signale angesteuert werden. Diese Balisen übertragen mehr Informationen als nur den aktuellen Signalbegriff und bilden damit die streckenseitige Kommunikationseinrichtung des ATC-Systems „EBICAB 900“. Eine Kopplungsmöglichkeit zur deutschen LZB ist nicht möglich, befindet sich aber, nach Aussage eines deutschen ABB-Mitarbeiters, in der Entwicklung. Über die Einbeziehung von Relaisstellwerken ist nichts bekannt; vermutlich ist es nicht möglich.

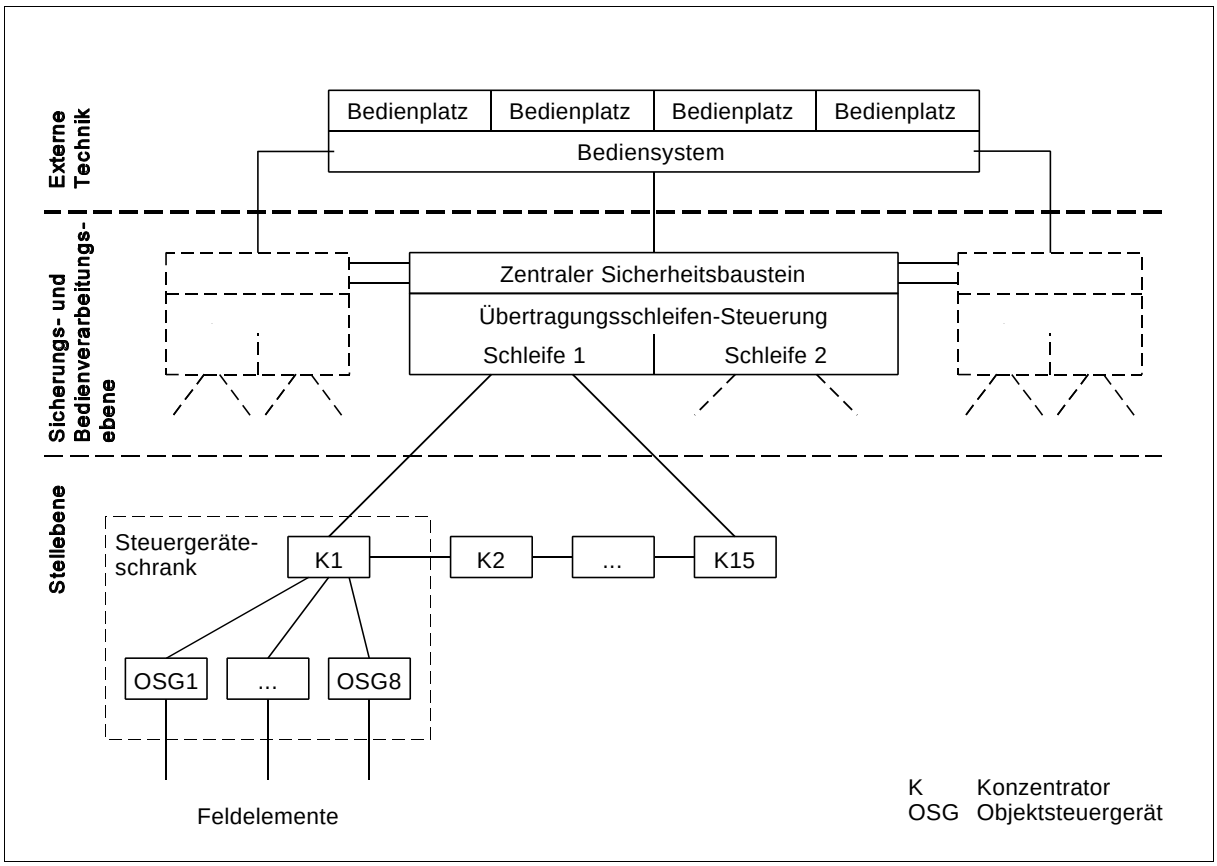


Abbildung 16: Systemstruktur des ESTW EBILOCK

4.2.2 Rechner und Verstärker

4.2.2.1 Bedienrechner

Ein Bedienrechner ist nicht vorhanden; seine Aufgaben werden vom Zentralrechner wahrgenommen.

4.2.2.2 Zentralrechner

Der Zentrale Sicherheitsbaustein (in EBILOCK 950 „POLARIS“ genannt [22]) ist ein 16 Bit-Rechner mit eigenen und kommerziellen Baugruppen und beinhaltet die gesamte Stellwerkslogik. Die Funktionen zur Steuerung der Schleifen sind im Zentralen Sicherheitsbaustein integriert. Zur Erhöhung der Verfügbarkeit kann er als 1v2-System ausgebildet werden.

4.2.2.3 Peripherierechner

Jedes Element der Außenanlage wird von einem Objektsteuergerät (OSG) überwacht und angesteuert. Dabei gibt es verschiedene OSG-Typen. Im einzelnen sind das Geräte für

- Signale
- Weichen
- Gleissperren
- BÜ-Technik

C Spezielle Objekte.

Ein Objektsteuergerät beinhaltet einen Mikroprozessor, diversitäre Software für den speziellen Anwendungsfall sowie Baugruppen für die Verbindung zum Zentralrechner und für die Ansteuerung der Elemente [25].

Wie beim später noch beschriebenen SSI-Stellwerk wird auch hier der Peripheriерechner ohne Redundanz verwendet, was an kritischen Elementen (z. B. Einfahrweiche) meines Erachtens im Fehlerfall zu merklichen Betriebseinschränkungen führen kann.

4.2.2.4 Diagnoserechner

Das Stellwerk verfügt über eingebaute Statistik- und Diagnosefunktionen, die Bestandteil des Zentralen Sicherheitsbausteins sind. Diagnosedaten können beim EBILOCK 950 über Modem von einer zentralen Wartungskonsole abgerufen werden. Die Konsole kann an mehrere EBILOCK-Stellwerke angeschlossen sein [22]. Im EBILOCK 850 sind die Diagnoseinformationen von einem fest angeschlossenen Terminal abrufbar [25].

4.2.2.5 Leistungsschalter

Die Leistungsschalter sind in den Peripheriерechnern integriert.

4.2.3 Interne Kommunikation

4.2.3.1 Aufbau

In einem Steuergeräteschrank sind die Objektsteuergeräte zusammen mit den Konzentratoren untergebracht. Letztere bilden in einer Schleife Knoten, an die die Objektsteuergeräte angeschlossen werden. Außerdem übernehmen sie die Regenerierung der Signale.

Über Modem kommunizieren die Konzentratoren untereinander und mit dem Zentralen Sicherheitsbaustein. Bei Ausfall der Versorgungsenergie eines Konzentrators werden die Signale durchgeschaltet, so daß die anderen Schleifenelemente davon nicht betroffen sind. Die Verbindung der Schleifenelemente wird durch vieradriges Kupferkabel oder durch LWL realisiert [25]. Im EBILOCK 950 ist sowohl der Einsatz des speziellen Schleifensystems als auch die Verwendung eines standardisierten Ethernet-Übertragungssystems möglich [22].

4.2.3.2 Datenübertragung

Im EBILOCK 850 wird ein standardisiertes Datenübertragungsprotokoll nach ISO 3309 und 4335 genutzt [25]. Es ist anzunehmen, daß diese Aussage auch für das EBILOCK 950 zutrifft.

4.2.4 Leistungsparameter

Etwa 300 Objektsteuergeräte (OSG) können von einem Zentralen Sicherheitsbaustein des EBILOCK 850 gesteuert werden, wobei es eine Begrenzung von 32 OSG pro Schleife gibt [25]. Für EBILOCK 950 sind die Angaben widersprüchlich. In [22] werden maximal 140 OSG pro ESTW angegeben, ein ABB-Produktblatt gibt 100 an. Letztere Aussage ist vermutlich richtig, da an eine Schleife 64 OSG angeschlossen werden können und sich damit eine maximale Anzahl von 128 OSG pro ESTW ergibt. Die verbleibende Differenz (28) ist möglicherweise zur Reserve vorgesehen.

4.3 Software

4.3.1 Struktur und Logikmodell

„Das Betriebssystem von EBILOCK 950 ist so ausgelegt, daß sowohl Spurplan- oder freiprogammierte Stellwerkslogik und eine Kombination beider Systeme realisiert werden kann. Dank dieses Auslegungsprinzips kann Spurplan-Logik für allgemeine und häufig wiederkehrende Sicherheitsregeln eingesetzt werden. Die flexible, freiprogrammierte Lösung wird angewandt, falls nicht auf eine Standardlösung zurückgegriffen werden kann.“[22] Ob der, einem ABB-Werbeprospekt entstammende Begriff der Spurplan-Logik wirklich dem entspricht, wie er im El S verwendet wird, ist nicht geklärt. Mitunter wird diese Aussage bezweifelt [3].

Die Programmierung der Verschluß- und Abhängigkeitsbedingungen erfolgt in STERNOL, der von ABB verwendeten, höheren Programmiersprache für Sicherheitslogik [22].

Die Verarbeitung der Stellwerksdaten erfolgt zyklisch. Während eines Zyklus, dessen Dauer 0,6 Sekunden beträgt, werden zunächst die Zustandsdaten aller Objektsteuergeräte in den Speicher des Zentralrechners eingelesen, in dessen CPU anschließend zeitlich nacheinander die diversitären Bearbeitungsprogramme ablaufen. Danach werden die ermittelten Kommandos an die Objektsteuergeräte ausgegeben. Nicht im Zyklus integriert sind die Programme, die den Datenaustausch mit externen Systemen organisieren. Sie laufen als Hintergrundprogramm neben der zyklischen Bearbeitung der Stellwerkslogik.

4.3.2 Projektierung

Mittels eines Projektierungssystems (EBILOCK 850: GEN 285; EBILOCK 950: EBITOOL) auf einer Workstation werden alle Hard- und Softwaredaten zusammengestellt. Die Generierung der Stellwerksdaten erfolgt automatisch anhand der grafischen Eingaben. Änderungen, Aktualisierungen und Tests können damit auch vom Betreiber der Anlagen vorgenommen werden [22].

Für das EBILOCK 850 steht das Testsystem ELBAN zur Verfügung, vermutlich ist dieses beim EBILOCK 950 im System EBITOOL integriert.

4.4 Externe Einflußnahme (Bedienung und Anzeige)

4.4.1 Allgemeines

Wie bereits erwähnt, kann die Bedienung über ein einzelnes Terminal oder über Bedienplatzsysteme erfolgen. Im folgenden soll das „Traffic Management System EBICOS 900“, welches in der Funktionalität einer Betriebszentrale entspricht, kurz vorgestellt werden.

Zum Leistungsumfang des EBICOS 900 gehört die Zugnummernmeldung (Train describer) als unverzichtbare Voraussetzung für ein Zuglenk-System (Automatic routing). Der aktuelle Fahrplan kann auf einem Bildschirm angezeigt und, falls es die aktuelle Betriebslage erfordert, temporär vom Bediener geändert werden. Ob sich eine solche Änderung auf das Zuglenk-System auswirkt oder ob sie nur der visuellen Konflikterkennung dient, ging aus der Literatur nicht hervor [27].

4.4.2 Bedienplatz

Wie beim deutschen Bedienplatzsystem, kann der Arbeitsbereich eines EBILOCK-Stellwerkes in verschiedene Bedienbereiche aufgeteilt werden. Abhängig vom Verkehrsaufkommen kann ein Bediener ein oder mehrere Bedienbereiche steuern.

Jedem Bediener steht ein Bedienplatz zur Verfügung, der mit Farbmonitoren und einer Tastatur ausgerüstet ist. Die Bedienplätze sind so angeordnet, daß alle Bediener auf eine Videoprojektionswand blicken können, die die Ausmaße bisheriger Anzeigetafeln mitunter weit überschreitet. Die Monitore der Bedienplätze können die Anlagen im „Overview“ (analog Bereichsübersicht) oder im „Detail View“ (analog Lupenbild) anzeigen.

Bedienungen werden in Form von alphanumerischen Zeichen über die Tastatur eingegeben. Ein durchaus positiv zu bewertendes Merkmal des Bediensystems ist, daß, im Gegensatz zum El S, Fahrstraßen gespeichert werden können [27], wie es bereits in den meisten WSSB-Relaisstellwerken möglich war. Die Speicherung bezieht sich auf Fahrstraßen, deren Einstellung zum Zeitpunkt der Bedienung, z. B. durch eingestellte feindliche Fahrstraßen, noch nicht möglich ist. Sobald die feindliche Fahrstraße aufgelöst ist, läuft die vorher eingespeicherte Fahrstraße ein. Dadurch wird der Bediener entlastet und der Betriebsablauf flüssiger.

5 British Rails SSI (Westinghouse, GEC ALSTHOM)

Solid **S**tate **I**nterlocking (SSI) ist die englische Sammelbezeichnung für elektronische Stellwerkstechnik. British Rails SSI ist ein offener Standard, der Anfang der 80er Jahre von den englischen Signalbaufirmen GEC-General Signal Ltd und Westinghouse Signals Ltd unter Führung von British Rail (BR) entwickelt wurde. Das erste Stellwerk dieser Art wurde 1985 in Betrieb genommen.

Folgende Komponenten sind im Standard enthalten:

- Hardwarearchitektur
- Datenübertragung
- Hardware-Redundanz
- Software.

Aufgrund des festgeschriebenen Standards ist das Stellwerkssystem sehr gut dokumentiert; deshalb kann hier detailliert darauf eingegangen werden. Alle Angaben wurden im wesentlichen [37] entnommen. Wenn im folgenden von SSI die Rede sein wird, so ist damit immer das durch den SSI-Standard von British Rail genormte ESTW gemeint.

Als sich 1989 die Signalbaufirmen GEC (Großbritannien), ACEC Transport (Belgien) und Alsthom (Frankreich) zu GEC ALSTHOM zusammenschlossen, hatte jede der Firmen bereits eigene Entwicklungen auf dem Gebiet der elektronischen Stellwerke getätigt. Dabei war die Entwicklung des SSI von GEC am weitesten fortgeschritten und hatte sich schon in mehreren Stellwerken weltweit bewährt. In einer Untersuchung über Rationalisierungsmöglichkeiten im jetzigen Firmenverbund zeigte sich, daß das SSI den Anforderungen von SNCB und SNCF sowie von Kunden in Übersee entsprechen würde. Allein das zeigt schon die Flexibilität des Systems. Auf diese Weise wurde es international noch weiter verbreitet [36].

Heute gehört SSI zu den weltweit am häufigsten eingesetzten ESTW, die u. a. eingesetzt sind bei Stadt- und Fernbahnen in:

- Großbritannien
- Belgien
- Dänemark
- Portugal
- Spanien
- Australien
- Hong Kong
- Indien
- Südafrika.

Der weltweite Erfolg läßt sich u. a. durch die bereits erwähnte große Flexibilität erklären, da das SSI große Vorteile bei der Anpassung des Systems an die Bedingungen fremder Bahngesellschaften bietet, wenn sich alle betrieblichen Bedingungen in Verschlußtabellen darstellen lassen. Komplizierte Funktionen wie z. B. Ersatzschutzsuche sind dabei zwar nicht zu realisieren, werden aber auch nicht gefordert. Die Umsetzung der Verschlußtafeln ist gleichzeitig die Anpassung an die Stellwerksfunktionen einer fremden Bahnverwaltung [6].

5.1 Sicherheits- und Verfügbarkeitskonzept

Da das SSI unter der Leitung von BR entwickelt worden ist, gibt es für das Stellwerk keine Sicherheitsnachweise. BR bescheinigt den Herstellern aber, daß SSI von BR für den Einsatz auf Bahnen mit Personenverkehr zugelassen ist. Daß die sicherungstechnischen Einrichtungen gemäß der von BR geforderten Qualitätsnorm hergestellt werden, wird von BR überprüft und in einem Zertifikat bescheinigt [28]. Beide Aussagen treffen auch für das anschließend beschriebene System WESTRACE zu.

5.1.1 Datenverarbeitung

Die Sicherheit im Zentralrechner wird durch ein klassisches 2v3-Rechnersystem mit Softwarevergleich erreicht, das „Triple Modular Redundancy“ genannt wird. Alle drei Rechnermodule vergleichen ihre Ausgaben, ihren Speicherinhalt und ausgewählte Systemdaten. Für die Abschaltung im Fehlerfall steht eine Sicherheits-Abschalt-Baugruppe zur Verfügung, die den betroffenen Rechner spannungslos schaltet. Diese Sicherheitsabschaltung kann durch den Rechner selbst oder durch die anderen zwei Rechner erfolgen.

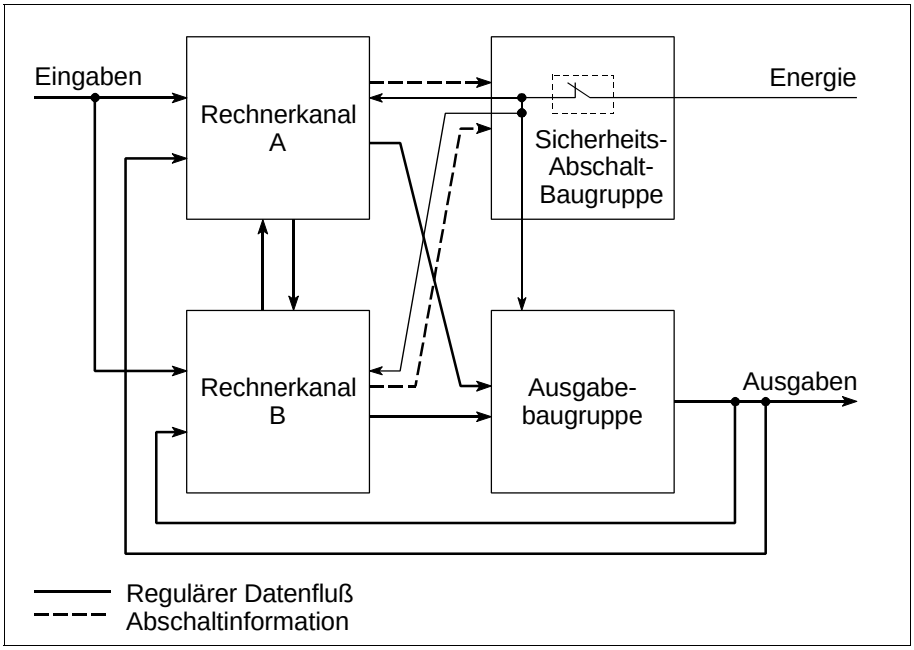


Abbildung 17: Sicherheitsprinzip in SSI-Rechnern bei Verwendung der 2v2-Konfiguration

Ebenso wird im Peripherierechner verfahren, mit dem Unterschied, daß dieser als 2v2-System ausgebildet ist. Im Fehlerfall steht damit keine Verfügbarkeitsredundanz zur Verfügung! Im Gegensatz zum BSTR steuert der Peripherierechner hier zwar nur zwei bis vier Weichen bzw. ein oder zwei Signale, wodurch die Auswirkungen lokal beschränkt bleiben, dennoch sind die betroffenen Elemente dann weder überwach- noch steuerbar. Fällt beispielsweise der Peripherierechner aus, der die Weichenverbindung mit der Einfahrweiche steuert, so ist keine Fahrstraße dieses Bahnhofskopfes mehr einstellbar.

Tritt ein Fehler im Peripheriерechner auf, so wird er durch die Sicherheits-Abschalt-Baugruppe abgeschaltet, und der Datenverkehr mit dem Zentralrechner wird eingestellt. Wird dagegen ein Fehler im Ein- oder Ausgabestromkreis lokalisiert, so wird nur dieser abgeschaltet. Datentelegramme werden weiterhin beantwortet, dann allerdings mit entsprechenden Störungsmeldungen. Ebenso wird verfahren, wenn sich Unregelmäßigkeiten in den Datenverbindungen zur Stellwerkszentrale zeigen.

5.1.2 Datenübertragung

Die Sicherheit in der Datenübertragung wird durch Telegramme mit Coderedundanz erreicht. Der Einsatz des Manchester II-Codes gibt zusätzliche Sicherheit gegen Verfälschung.

Im Normalbetrieb wird seitens des Peripheriерechners zwischen den beiden Bus-Kanälen regelmäßig umgeschaltet, so daß die Funktionstüchtigkeit beider Kanäle ständig geprüft wird. Bei Ausfall eines Kanals wird der Datenverkehr ohne Einschränkung der Sicherheit und ohne Änderung des Telegrammformats einkanalig aufrecht erhalten.

5.1.3 Bedienung und Anzeige

Bedienung und Anzeige unterliegen keiner Sicherheitsrelevanz.

5.2 Systemstruktur

5.2.1 Hardwarearchitektur

Im Gegensatz zu anderen Systemen fällt es beim SSI leicht, die einzelnen Rechner den Ebenen zuzuordnen. Kern des Systems ist das sichere Interlocking Multi-Processor Modul (I/L MPM). Über das nicht sichere Panel Processor Modul (PPM) werden die Ein- und Ausgaben vom und zum Bediener bearbeitet. Zusammen mit dem Diagnostic Multi-Processor Modul (Diag MPM) und den Data Link Modulen (DLM) bilden sie das Interlocking Cubicle – den Stellwerkskern. Ein Interlocking Cubicle kann einen mittelgroßen Bahnhof steuern. Ist mehr Kapazität nötig, so werden weitere Interlocking Cubicles hinzugefügt. Für Diagnosezwecke steht das Technician’s Terminal zur Verfügung, welches über das Diag MPM mit den Interlocking Cubicles kommuniziert.

Die Verbindung zur Außenanlage und zu weiteren Stellwerken wird durch Data Link Modules, an die das Bussystem angeschlossen ist, erreicht. Die Trackside Functional Modules (TFM) schließlich bilden die Stellrechner in der Nähe der zu steuernden Elemente.

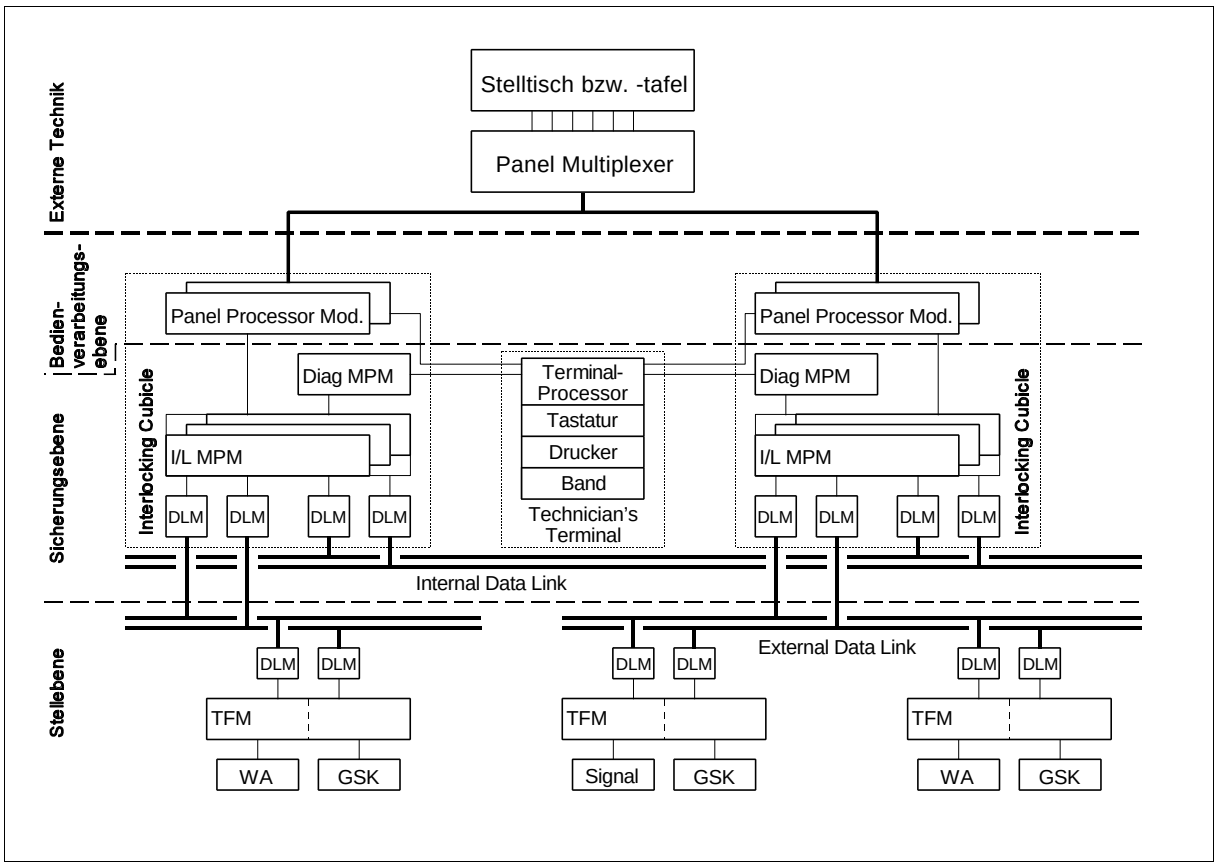


Abbildung 18: Systemstruktur des ESTW SSI mit Stelltisch

Diag MPM	Diagnostic Module	Multi-Processor	GSK	Gleisstromkreis
DLM	Data Link Module		TFM	Trackside Functional Module
I/L MPM	Interlocking Multi-Processor Module		WA	Weichenantrieb

Die Rechner des Interlocking Cubicles sind mit standardisierten Schnittstellen untereinander verbunden. Alle Verbindungen zwischen den Rechnern sind optisch voneinander entkoppelt.

5.2.2 Rechner und Verstärker

5.2.2.1 Bedienrechner

Der Bedienrechner, hier Panel Processor Modul (PPM) genannt, ist ein nicht sicherer Rechner, der zur Erhöhung der Verfügbarkeit redundant ausgeführt wird. Beide Rechner arbeiten gleichzeitig nach dem gleichen Programm und empfangen alle Eingaben. Bei den Ausgaben wechseln sie sich ab. Fällt ein Rechner aus, so übernimmt der andere ohne Unterbrechung den Betrieb.

Das PPM bearbeitet alle Informationen, die zwischen dem Stellwerk und dem Bediener ausgetauscht werden. So wandelt es die Eingaben des Bedieners beispielsweise in eine Fahrstraßenanforderung um, die an den Zentralrechner weitergeleitet wird. Im Gegenzug werden die Daten vom

Zentralrechner für die Bedieneinrichtungen aufbereitet. Weiterhin stellt es Schnittstellen für externe Techniken bereit.

Wird für Bedienung und Anzeige eine Stelltafel oder ein -tisch benutzt, so werden von einem weiteren Rechner – dem Panel Multiplexer – die Lampen gesteuert und die Tasten abgefragt. Der Panel Multiplexer ist durch eine serielle Schnittstelle mit dem PPM verbunden. Er ist ebenfalls kein sicherer Rechner, kann aber, um eine hohe Verfügbarkeit zu gewährleisten, verdoppelt werden.

5.2.2.2 Zentralrechner

Das Interlocking Multi-Processor Modul (I/L MPM) arbeitet als sicheres System in einer 2v3-Konfiguration mit Softwarevergleich und ist in allen Kanälen in Hard- und Software identisch. Hier werden alle sicherungstechnischen Verknüpfungen ausgeführt. In jedem Rechner behandeln zwei Hilfs-Prozessoren die Kommunikation mit den Trackside Data Links und ein dritter mit den Internal Data Links.

5.2.2.3 Peripheriерechner

Im SSI-Stellwerk ist die Trennung zwischen Peripheriерechner und Leistungsschalter nicht eindeutig gegeben. Beide Aufgaben werden durch die Trackside Functional Modules (TFM) übernommen. Sie bieten, als direkte Schnittstelle zur Außenanlage, jeweils acht sichere Ein- und Ausgänge. Es wird in Signal- und Weichen-TFM unterschieden, die nachfolgend beschrieben werden sollen. Es wurden jedoch inzwischen, vor allem, um sich an die Bedürfnisse anderer Bahnverwaltungen anzupassen, weitere Arten entwickelt. So wurden von ACEC Transport, dem belgischen Teil von GEC ALSTHOM, die TFM, für die auch der Name „Trackside Controller“ üblich ist, überarbeitet und das Achszähler- sowie das Universal-Modul entwickelt.

Die TFM sind 2v2-Rechnersysteme mit Softwarevergleich. Auch hier sind die Rechnerkanäle in Hard- und Software identisch aufgebaut.

In Schaltschränken, die sich in der Außenanlage befinden, werden die TFM untergebracht. Das setzt voraus, daß sie extremen Umweltbedingungen standhalten müssen, hat jedoch den Vorteil, daß die Länge der leistungsführenden Kabeladern kurz ist und demzufolge die Verstärkerlogik einfach ausfällt. Westinghouse gibt die maximale Stellentfernung mit 700 m an, British Rail läßt aber nur 180 m zu. Nachteilig ist, daß viele Schränke in der Außenanlage aufgestellt werden müssen, wodurch die Peripheriерechner nicht zentral angeordnet sind. Die Wartung vereinfacht sich aber dadurch, daß in den Schränken lediglich drei verschiedene Modultypen benötigt werden, die im Fehlerfall leicht ausgetauscht werden können.

Die TFM übernehmen die Kommandos von den I/L MPM, geben entsprechende Befehle aus und überwachen deren Ausführung. Weiterhin lesen sie die Meldungen der Außenanlage ein, senden die Istzustände an die I/L MPM und überprüfen die Ausgangstreiber und Eingangsstufen.

Die Verbindung zu den Trackside Data Links im Interlocking Cubicle wird durch zwei Data Link Module erreicht, die jeweils an einen der verdoppelten Busse angeschlossen sind.

Signal Modul

Das Signal Modul besitzt acht reguläre Ausgänge, von denen die Signallampen direkt angesteuert werden. Zusätzlich werden die Lampen der roten Signallaternen an einen besonderen Ausgang angeschlossen, der im Falle eines Fehlers im Modul oder bei Unterbrechung der Kommunikation mit dem Interlocking Cubicle gewährleistet, daß das Signal „Halt“ zeigt. Neben den Signallampen kann von einem der regulären Ausgänge ein AWS-Magnet angesteuert werden. Das „Automatic Warnig System“ (AWS) ist das britische Punktförmige Zugbeeinflussungssystem.

Zwei Eingänge stellen die Rückleitung von den Lampen sicher. Falls Lampen mit unterschiedlicher Spannung verwendet werden, erfolgt die Spannungsauswahl durch die Wahl des Rückleiter-Eingangs. Die verbleibenden sechs Eingänge werden genutzt, um Meldungen von Gleisstromkreisen oder anderen Einrichtungen einzulesen. Je nach Bestückung des Lichtsignals können von einem Signal Modul ein oder zwei Signale angesteuert werden.

Weichen Modul

Der Standard-Weichenantrieb von British Rail arbeitet elektro-hydraulisch. Um die Weiche zu stellen treibt ein Elektromotor eine Pumpe an. Die Auswahl eines von zwei Ventilen bestimmt, ob die Weiche die Position „normal“ oder „reverse“ einnimmt („Plus- oder Minusstellung“).

Nach englischer Sicherungsphilosophie werden in der Regel gekuppelte Weichen eingesetzt. Die Topologie der Bahnhöfe ist zumeist so gestaltet, daß auf diese Weise der Flankenschutz gewährleistet wird. Man spricht dabei von einem „Set of points“, nachfolgend „Weichenpaar“ genannt. Durch die Trennung der Ausgänge eines Weichen Moduls in zwei unabhängige Gruppen zu je vier Ausgängen, kann ein Modul zwei Weichenpaare ansteuern, insgesamt also zwei bis vier Weichen des bei BR eingesetzten Typs.

Die Ventile eines Weichenpaares werden immer parallel geschaltet und die Motoren einzeln angesteuert. Durch Kontakte an den Spitzenverschlüssen (Clamp Locks) wird ein codiertes Signal erzeugt, welches in das Weichen Modul eingelesen wird. Weitere Eingänge stehen für Meldungen von Gleisstromkreisen bereit.

Im Fehlerfall kann jede der beiden Ausgabegruppen separat abgeschaltet werden. Meldungen werden, soweit noch möglich, weiterhin eingelesen. Fällt das Weichen-Modul ganz aus oder bricht die Verbindung zur Zentrale ab, so werden die Weichen in ihrer letzten Stellung festgehalten, so daß eine betriebsgefährdende Stellung ausgeschlossen wird.

5.2.2.4 Diagnoserechner

Diagnostic Multi-Processor Modul

Das Diagnostic Multi-Processor Modul (Diag MPM) liest alle Daten, die über die Data Links ausgetauscht werden, mit und decodiert die Antworttelegramme, die über Störungen Auskunft geben. Es analysiert und lokalisiert die eingehenden Fehlermeldungen und leitet die so gewonnenen Daten an das Technician's Terminal weiter.

Zustandsmeldungen des I/L MPM werden als Telegramm mit der Empfängeradresse 0, die an kein TFM vergeben wird, an das Diag MPM gesendet. So kann das Diag MPM auch Daten vom Zentralrechner empfangen, verarbeiten und weiterleiten. Außerdem wird jede Änderung der Meldungen von der Außenanlage an das Technician's Teminal weitergeleitet, um es dort aufzuzeichnen. Wahrscheinlich werden auch alle Stellbefehle aufgezeichnet.

Technician's Terminal

An ein Technician's Terminal können bis zu sechs Diag MPM angeschlossen werden. Außerdem erhält es Informationen vom PPM.

Zu einem Terminal gehören der Rechner als Kernstück, ein Bandlaufwerk, ein Modem, ein Drucker und eine Tastatur. Der Zugriff auf das Teminal ist passwortgeschützt. Im einzelnen hat es folgende Aufgaben zu bewältigen:

- Ausdruck aller Fehlermeldungen im Klartext
- Aufzeichnung aller Zustandsänderungen (Weichenumstellung, Fahrstraßenauflösung usw.)
- Gezielter Test der Außenanlage und der Datenübertragung durch den Instandhalter
- Sperren von Fahrstraßen oder Weichen und anderer Kommandos durch den Instandhalter
- Bereitstellung der Systemzeit
- Unterstützung des Instandhalters bei Inbetriebnahme des Stellwerks.

5.2.2.5 Leistungsschalter

Beim SSI wird nicht zwischen Peripherierechner und Leistungsschalter unterschieden. Aus diesem Grund wurden die Leistungsschalter bereits unter 5.2.2.3 beschrieben.

5.2.3 Interne Kommunikation

Innerhalb der internen Kommunikation wird im SSI zwischen internem und externem Datenaustausch unterschieden. Leider ergibt sich hier eine Begriffsüberschneidung; externer Datenaustausch darf nicht mit externer Kommunikation verwechselt werden!

Interner Datenaustausch („Internal Data Link“) wird zwischen den Interlocking Cubicles praktiziert, der externe Datenaustausch („External Data Link“) erfolgt zwischen der Zentrale und den TFM. Beide werden über serielle Busse mit identischem Aufbau realisiert.

Eine Alternative zur Kommunikation über DLM wurde von ACEC Transport mittels LWL-Schleifen entwickelt. Diese werden zusammen mit den von ACEC entwickelten TFM (s. a. 5.2.2.3) in Belgien eingesetzt. Im folgenden werden die Standardmethoden vorgestellt.

5.2.3.1 Aufbau

Übertragung über Data Link Module

Alle über den Bus kommunizierenden Elemente werden über Data Link Module (DLM) angeschlossen. Die Datenverbindungen sind nur zur Erhöhung der Verfügbarkeit verdoppelt. Als Übertragungsmedium kommt ein abgeschirmtes, zweiadriges Kupferkabel (screend twisted pair) zum Einsatz. Bis zu 63 TFM können an einen Bus angeschlossen werden.

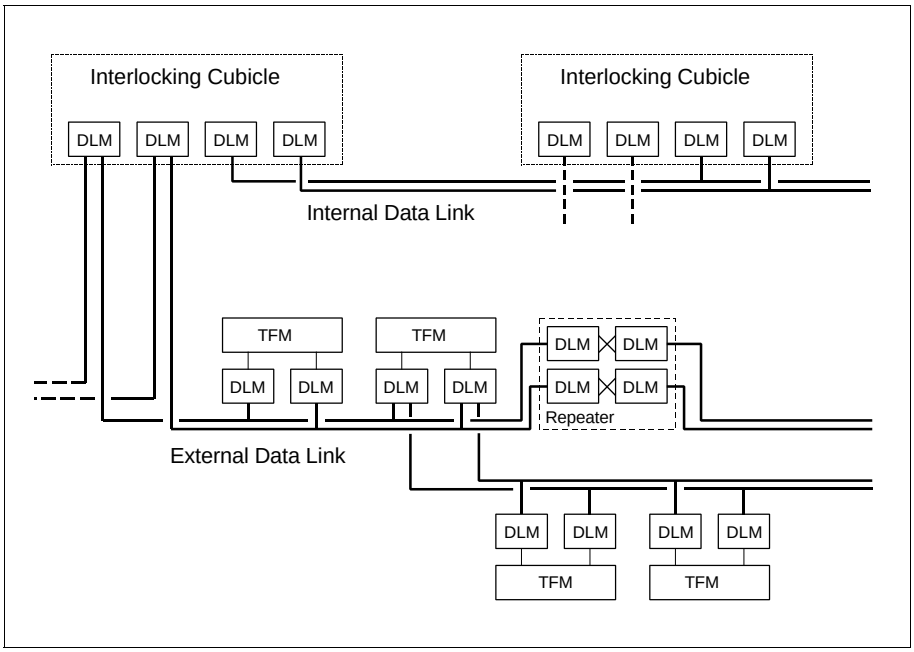


Abbildung 19: Mögliche Konfigurationen der Trackside Data Links

Jedes DLM besitzt zwei Bus-Anschlüsse, um Verzweigungen zu realisieren (Abbildung 19). Da sie wie die TFM in der Außenanlage eingesetzt werden, müssen sie ebenso robust konstruiert sein. In der Innen- wie Außenanlage wird die gleiche Bauform verwendet.

Die Entfernung, die mit den DLM überbrückt werden kann, ist auf 10 km begrenzt. Muß eine größere Entfernung überwunden werden, so sind Repeater notwendig. Diese Zwischenverstärker bestehen aus zwei DLM, die „Rücken an Rücken“ verbunden sind und damit einen kompletten bidirektionalen Repeater bilden. Maximal können vier Repeater in einer Leitung eingesetzt werden, dann allerdings mit einem maximalen Abstand von 8 km. Somit ergibt sich eine Entfernung von maximal 40 km, die mit DLM überbrückt werden kann.

Long Line Link

Um größere Fernsteuerbereiche zu bilden, wird das Verfahren „Long Line Link“ verwendet. Dieses Verfahren erlaubt eine sichere Datenübertragung über herkömmliche Telekommunikationskanäle bis zu mehreren hundert Kilometern, je nach Qualität des Netzes.

Ein spezielles SSI-Modul das „Long Distance Terminal“ (LDT) verbindet das Stellwerk (Innen- und Außenanlage) mit dem öffentlichen Netz; die DLM entfallen. Das LDT ist vermutlich ein 2v2-Rechnersystem. Es erhält vom Stellwerk Daten mit der Standard-Datenrate von 10 kbit/s, und leitet sie mit 64 kbit/s weiter. Die höhere Datenrate ist notwendig, um einen zusätzlichen, 11 Bit langen Sicherungsanhang übertragen zu können. Dieser gewährleistet einen hohen Grad an Sicherheit gegen Verfälschung, der notwendig ist, um die Informationen über ein offenes Telekommunikationssystem zu übertragen. Ob die Daten verschlüsselt werden und es sich bei dem Sicherungsanhang um einen sogenannten Message Authentication Code („Fingerabdruck der Daten“) handelt, war aus den verwendeten Unterlagen nicht ersichtlich.

5.2.3.2 Datenübertragung

Die Datenübertragung erfolgt in Form von Telegrammen mit einer Länge von 30 Bit, also deutlich kürzer als im El S (128 Bit). Dieser Unterschied erklärt sich daraus, daß es im El S nur einen Stellwerksbus für alle sicheren Rechner gibt, beim SSI dagegen für jedes Interlocking Cubicle einen. Außerdem sind die im I/L MPM zusammengefaßten Stellwerksfunktionen beim El S auf mehrere Rechner verteilt, was ein größeres Volumen an Datenverkehr nach sich zieht und eine größere Anzahl von Adressen erforderlich macht.

Ein über DLM übertragenes Telegramm besteht aus Richtungsbit, Adresse, Daten und Sicherung. Das Richtungsbit zeigt an, ob das Telegramm von der Zentrale oder der Außenanlage kommt. Jedes Interlocking Cubicle hat sein eigenes Bussystem mit der Außenanlage, jedes Bussystem seine eigene Systemadresse zur Identifizierung (System-Identifizierung). Diese dient dazu, benachbarte Interlocking Cubicles zu unterscheiden. Damit kann im Falle eines Übersprechens von Busleitungen kein Data Link Modul unbeabsichtigt angesprochen werden.

Bit	Inhalt	Funktion
1	Richtungsbit	Richtung
2-6	System-Identifizierung	Adresse
7-12	Rechneradresse	
13-20	Stellwerksdaten	Daten
21-25	Diagnosedaten	
26-30	Parität	Sicherung

Tabelle 2: Aufbau eines Telegramms für den Datenaustausch über Trackside Data Links

Das Interlocking Cubicle sendet Steuertelegramme zu den TFM. Diese werden durch ein Antworttelegramm vom jeweiligen Empfänger bestätigt. Auf diese Weise werden alle 64 Adressen

nacheinander angesprochen (Polling-Modus), auch wenn nicht alle Adressen vergeben sind. Die Zeit für einen kompletten Zyklus beträgt 850 ms. Für TFM sind 63 Adressen verfügbar; die Adresse Null wird immer für den Diagnoserechner vergeben.

5.2.4 Leistungsparameter

Wie bereits erwähnt, kann ein Interlocking Cubicle maximal 63 TFM steuern. Geht man davon aus, daß zu jedem Stellelement ein Gleisstromkreis gehört und eine weitere Anzahl von Gleisstromkreisen hinzukommt, so kann die Gesamtkapazität eines Stellwerkskerns auf etwa 200 Feldelemente geschätzt werden. Weitere Aussagen zur Leistungsfähigkeit, insbesondere bei der Bildung von Betriebszentralen, werden im Abschnitt 5.4 getroffen.

5.3 Software

5.3.1 Struktur und Logikmodell

Die Software des SSI unterteilt sich im Gegensatz 2 Ebenen. Die Systemprogramme sind modular aufgebaut und durch Vermeiden von Interrupts leicht prüfbar. Sie sind in Assembler geschrieben und anwenderunabhängig. Die anlageabhängigen Daten und kundenspezifischen Bedingungen bilden ein Software-Paket, welches in Form von Verschlußtabellen aufgebaut ist. Damit ist das SSI in seinem Grundaufbau bahnverwaltungsunabhängig.

Das System arbeitet zyklisch. Im Hauptzyklus (ca. 850 ms) tauschen die I/L MPM mit allen maximal 63 TFM und dem Diag MPM Daten aus. In jedem darin enthaltenen kleinen Zyklus (ca. 8 ms) synchronisiert sich jedes Modul mit seinen Partnern, führt Prüfungen seines eigenen Sicherheitsabschalters und der seiner Partner durch, tauscht Speicherinhalte aus und führt entsprechende Vergleiche durch. Weiterhin werden Aufträge vom PPM und Meldungen der TFM bearbeitet, die Fahrstraßenbearbeitung unter Berücksichtigung der Verschlußtabellen wird durchgeführt und Kommandos und Meldungen an TFM und PPM ausgegeben.

5.3.2 Projektierung

Bei der Entwicklung eines Projektierungs-Tools wurde davon ausgegangen, daß die Projektierung von Signalingenieuren ohne spezielle Computerkenntnisse durchgeführt wird. Das Ergebnis ist die SSI Design Workstation.

Basis für die anlagenabhängige Softwareprojektierung sind die Verschlußtabellen. Sie werden vom Projektant in einer symbolischen Sprache in die Workstation eingegeben. Diese Datenlisten werden in Maschinencode übersetzt und können dann vom Projektant auf dem Simulationssystem auf ihre Richtigkeit getestet werden. Nach erfolgreichem Test werden die Daten direkt auf EPROM gespeichert.

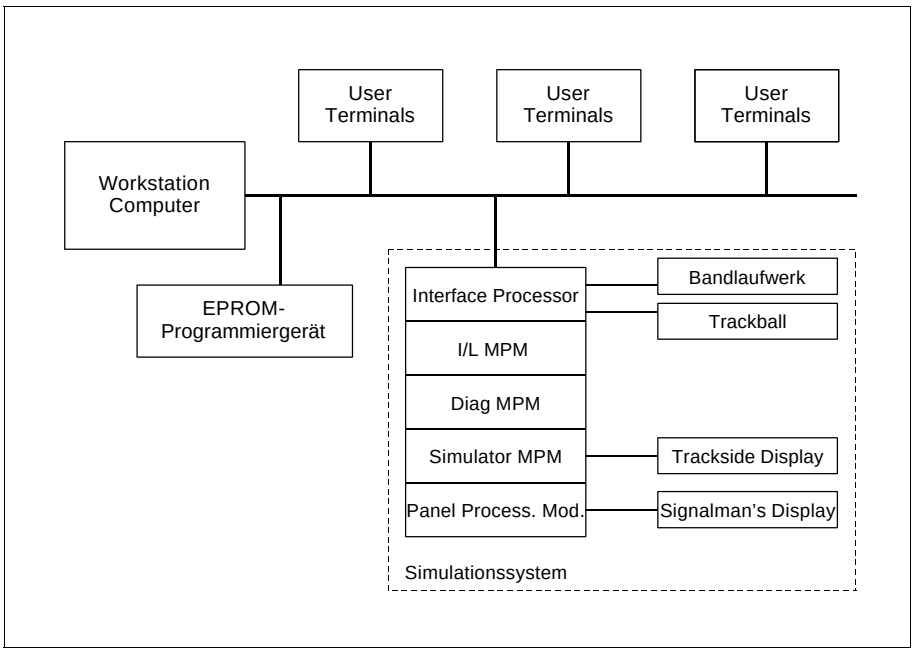


Abbildung 20: SSI Design Workstation

5.4 Externe Einflußnahme (Bedienung und Anzeige)

5.4.1 Allgemeines

In den ersten SSI-Stellwerken stellte die Schnittstelle Stellwerk – Mensch ein herkömmlicher Stelltisch dar, der über den bereits erwähnten Panel Multiplexer an das PPM angeschlossen wurde. Auf diese Art der Bedienung soll hier nicht weiter eingegangen werden.

Wesentlich moderner gestaltet sich die Bedienung mit dem Integrated Electronic Control Centre (IECC), in dem die Funktionen einer Betriebszentrale integriert sind. Bis auf den Timetable Processor, in dem sämtliche Fahrplandaten gespeichert werden, sind alle Komponenten des IECC aus Verfügbarkeitsgründen redundant ausgeführt.

Das Signalman's Display System (SDS) stellt den Bedienplatz dar, auf den noch eingegangen wird. Automatic Route Setting (ARS) ist ein Zuglenksystem. Es dient dem automatischen Einlaufen von Zug- und in beschränkter Weise auch Rangierfahrstraßen. Diese Funktionen werden auch wahrgenommen, wenn es Abweichungen vom Fahrplan gibt. In einem solchen Fall errechnet das System die optimale Reihenfolge der Züge.

SDS und ARS wirken hauptsächlich auf das Stellwerk ein. Für eine Diagnose des IECC steht der System Monitor zur Verfügung. Der Data Protocol Converter dient als Schnittstellenumsetzer für weitere Techniken. Das Zugnummernmeldesystem genannt „Train Describer" ist vermutlich in der Software des Bedienrechners integriert. Das Gateway System stellt die Verbindung der nachfolgend aufgeführten Netzwerke her und dient außerdem als Filter für die Daten, die in das Signalling Network gelangen.

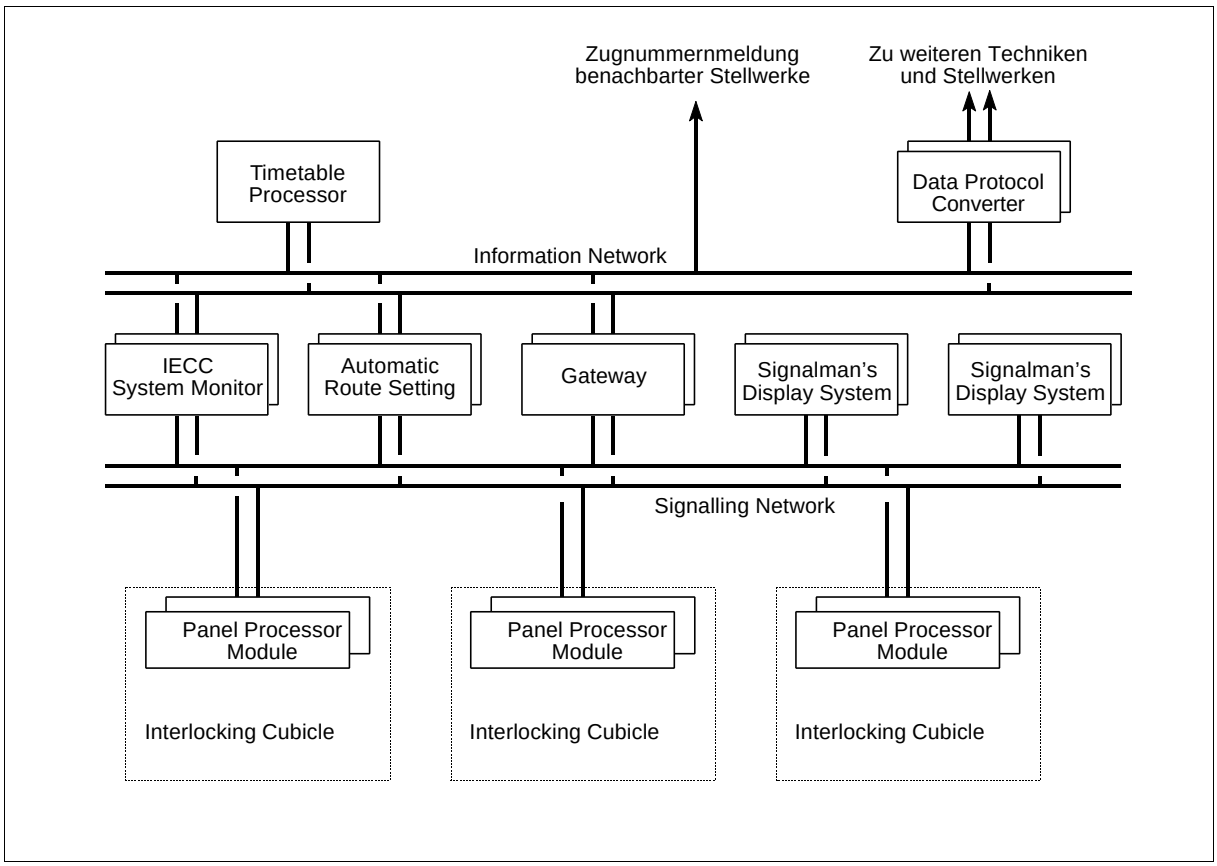


Abbildung 21: Konfiguration des IECC

Zwei Netzwerke stehen für die Kommunikation zur Verfügung. Das Signalling Network stellt die Verbindung zum ESTW sicher; das Information Network dient dem Informationsaustausch mit weiteren Systemen wie z. B. Fahrgastinformationsanlagen sowie der Kommunikation mit benachbarten IECC oder herkömmlichen Stellwerken. Die Trennung der beiden Netze ist notwendig, um die Datenmengen auf dem Signalling Network zu begrenzen, was sich wiederum positiv auf die Antwortzeiten des ESTW auswirkt. Da der Datenaustausch auch hier im Polling-Modus erfolgt, ist, um die Antwortzeiten zu begrenzen, die Anzahl der an das Signalling Network anschließbaren Systeme begrenzt. Maximal können angeschlossen werden:

12 Interlocking Cubicles
3 Signalman's Display Systems
1 Automatic Route Setting
1 Gateway System
1 System Monitor.

5.4.2 Bedienplatz

Kern des Bedienplatzes ist ein zur Erhöhung der Verfügbarkeit redundant ausgelegter Bedienrechner, an den bis zu vier Monitore sowie ein Trackball mit mehreren Tasten und eine Tastatur angeschlossen sind.

Zwei Monitore bilden den „Overview“, der den Bereich des SDS anzeigt (analog Bereichsübersicht). Ein weiterer Monitor zeigt den „Detail View“ (analog Lupe). Hier können bis zu sechs verschiedene Bilder des Bedienbereiches aufgeschaltet werden. Overview und Detail View werden semigrafisch in einer Auflösung von 128×48 Zeichen wiedergegeben. Bei beiden Anzeigen sind unter dem jeweiligen Gleisbild Buttons angeordnet, mit denen sich spezielle Funktionen wie z. B. die Umschaltung des Detail View-Bildes ansprechen lassen.

Der vierte Monitor, genannt „General Purpose Display“, spiegelt die Eingaben des Bedieners, gibt Alarm- und allgemeine Meldungen aus (analog Kommunikationsanzeige) und dient der Kommunikation mit dem ARS und dem Train Describer.

Die Bedienung wird größtenteils über den Trackball abgewickelt, der in den Bedientisch integriert ist. Um ihn herum sind mehrere Tasten angeordnet. Drei dienen der Weicheneinzelbedienung, zwei weitere ahmen die Funktionen „Drücken“ und „Ziehen“ von Tasten herkömmlicher Bedientische nach. Diese beiden, hauptsächlich genutzten Tasten sind doppelt vorhanden für Rechts- und Linkshänder!

Um ein Element oder eine Funktion anzusprechen, wird der Cursor mittels des Trackballs auf dem Element oder dem Funktions-Button positioniert. Mit einer der beiden hauptsächlichen Bedientasten wird das Element angesprochen. Vermutlich wurden deswegen zwei Tasten vorgesehen, um in der Bedienung eine weitgehende Übereinstimmung mit herkömmlichen Stelltischen zu erreichen. Zugfahrstraßen können durch Start-Ziel-Bedienung auf Over- oder Detailview eingegeben werden, Rangierfahrstraßen oder Einzelbedienungen nur auf Detailview.

6 Westrace (Westinghouse)

Für die Planung der „Elektronischen Sicherungstechnik der zweiten Generation“ führten die Tochterfirmen der „Hawker-Siddeley Group“ – Westinghouse Brake and Signal (Großbritannien), Westinghouse Brake and Signal (Australien), Safetran (USA) und Dimetronic (Spanien) – Ende der 80er Jahre eine Marktanalyse mit der Aufgabe einer grundsätzlichen Neubeurteilung der Signalisierungssysteme durch. Das Projekt erhielt den Namen WESTRACE (**Wes**tinghouse **T**rain **R**adio and **A**dvanced **C**ontrol **E**quipment). Im Ergebnis dieser Untersuchung herrschte bei den Experten die übereinstimmende Meinung, daß das Projekt die Möglichkeiten der modernen Funktechnik ausnutzen sollte, um eine „sichere Zweiwege-Kommunikation“ zwischen Zügen und ortsfesten Einrichtungen zu erhalten.

Das bisherige ESTW SSI war nach Meinung von Westinghouse sehr erfolgreich und hatte weltweit eine große Akzeptanz gefunden. SSI bildet aber keine optimale Lösung für lange Strecken mit kleinen Betriebsstellen, wie sie weltweit im Fern- (meist außerhalb Europas) und Nahverkehr (U- und Stadtbahnen) anzutreffen sind. Außerdem sollte das neue System noch flexibler als SSI sein.

Westinghouse bevorzugt SSI für mittlere und große Stellwerke. Darüber hinaus wird daran gedacht, SSI mit WESTRACE als Bereichsrechner (statt TFM) zu kombinieren.

WESTRACE ist für eine fortschreitende Vervollständigung mit Funktionsmodulen vorgesehen. Dabei wurde mit Kleinstellwerken begonnen. Während die Grundmodule von allen Tochterfirmen gemeinsam entwickelt wurden, werden weitere Spezialmodule in den einzelnen Landesgesellschafen (Erstanwender) unter Einhaltung der vorgegebenen Spezifikation entwickelt, wie z. B. das ATP-Modul WESTECT von Westinghouse Australien [28]. Inzwischen wurde auch ein Funkkommunikationssystem (ESTW – Fahrzeug) entwickelt.

Erste Einsätze des ESTW WESTRACE erfolgten in Australien, Spanien (Nahverkehr) und Großbritannien (U-Bahn).

6.1 Sicherheits- und Verfügbarkeitskonzept

6.1.1 Datenverarbeitung

WESTRACE ist ein System mit einkanaliger Hard- und zweikanaliger Software. Jedes Modul (Rechner) enthält einen Prozessor, der für sein Modul einen Selbsttest durchführt. Zusätzlich wird auch jedes Nachbar-Modul geprüft, was durch einen eigenen Bus geschieht, der die Module ringförmig miteinander verbindet. Über den „Data and Primary Negation Bus“ werden, neben dem Austausch von Betriebsdaten, auch die Informationen über diese Funktionstests an das Zentralmodul (Zentralrechner) gesendet. Bei einem negativen Ergebnis wird über den Data and Primary Negation Bus ein Befehl zur Systemabschaltung ausgegeben [29].

In der Minimalkonfiguration arbeiten drei Module zusammen und überwachen sich dabei gegenseitig. Mit diesem Verfahren begründet Westinghouse die Mehrkanaligkeit seines Systems (3v3) [28]! Das entspricht allerdings nicht der allgemeinen Auffassung von Mehrheitsentscheidungssystemen (mvn), da ein solches System immer einen Vergleich von n unabhängig ermittelten Ergebnissen voraussetzt. Hier werden aber keine Ergebnisse verglichen, sondern nur gegenseitige Funktionsprüfungen vorgenommen.

Bei einem erkannten Fehler werden die Ausgänge durch das Output Power Control Relay (OPCR) abgeschaltet. Dieses Klasse I-Relais wird durch zwei Kanäle angesteuert und ist im Ordnungszustand angezogen. Der erste Kanal (Primary Negation) wird direkt vom Zentralmodul gesteuert und leitet damit den Abschaltbefehl weiter, den im Fehlerfall das Zentralmodul selbst auslöst oder der über den Data and Primary Negation Bus von den Ein-/Ausgabemodulen (Peripherierechner) übermittelt wird. Der zweite Kanal (Second Negation) ist ein Überwachungskanal, der alle Module verbindet und am OPCR endet. In beiden Kanälen werden dynamisch wechselnde Signale verwendet, die mit Hilfe eines Übertragers sicher UND-verknüpft werden. Nur bei erfüllter UND-Bedingung (beide Eingänge wechseln dynamisch) bleibt das OPCR angezogen [38].

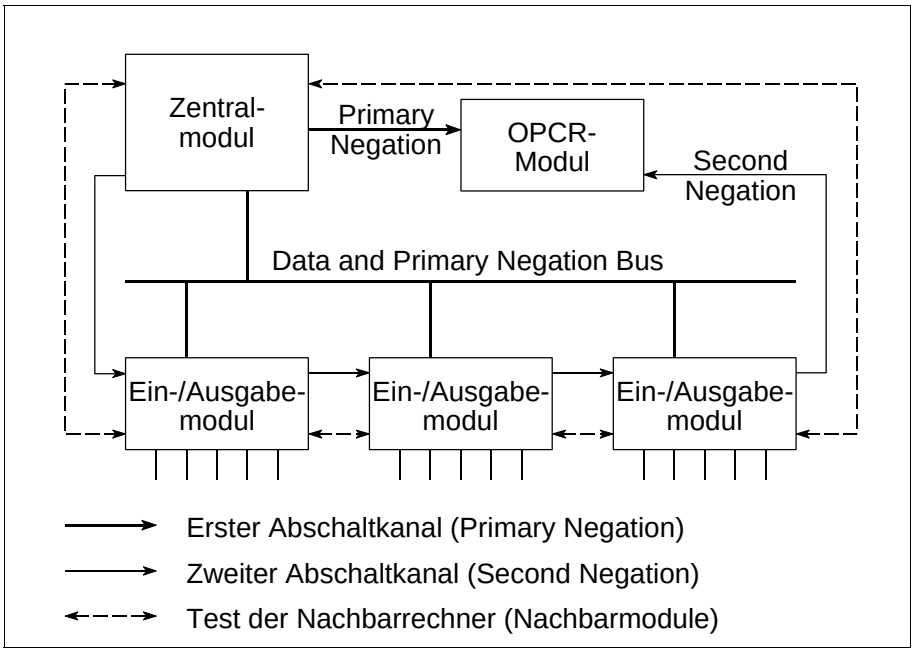


Abbildung 22: Ansteuerung des Output Power Control Relay (OPCR)

Wird in einem Peripheriерechner ein Fehler in einem Ein- oder Ausgang gefunden, so wird zunächst versucht, nur diesen abzuschalten (Graceful Degradation). Erst wenn dieser Versuch scheitert oder weitere Fehler hinzukommen wird das ganze System durch das OPCR abgeschaltet [30].

Der Entwurf der Software erfolgt einkanalig. Erst auf der untersten Übersetzungsebene wird mit zwei verschiedenen Übersetzungsverfahren ein zweikanaliger Programmcode erzeugt (True- und Complement-Logik). Somit beschränkt sich die Diversität der Software auf die Form des Abspeicherns im EPROM. Die Ergebnisse der True- und Complement-Logik werden Prozessorintern

verglichen. Nur bei Gleichheit werden die Ergebnisse zur Weiterverarbeitung bzw. Ausgabe zugelassen [28].

Zur Erhöhung der Verfügbarkeit kann ein „Hot Standby System“ hinzugefügt werden, welches letztlich die Verdopplung der gesamten Anlagensteuerung bedeutet. Diese Möglichkeit wurde in der Literatur nur bei der Beschreibung eines „Large Interlocking“ genannt [30]. Vermutlich ist es auch bei einem „Small Interlocking“ möglich. Westinghouse ist aber so von der Zuverlässigkeit seiner Komponenten überzeugt, daß die redundanten Auslegung eher als „Sonderausstattung“ angesehen wird.

6.1.2 Datenübertragung

Der Datenaustausch erfolgt sowohl durch parallele als auch serielle Verbindungen. Maßnahmen zur Fehlererkennung und Mehrfachübertragung von Daten sorgen für die Sicherheit. Wie dieses im einzelnen realisiert wird, wurde in der verwendeten Literatur nicht näher beschrieben.

6.1.3 Bedienung und Anzeige

An Bedienung und Anzeige werden keine Sicherheitsanforderungen gestellt.

6.2 Systemstruktur

6.2.1 Hardwarearchitektur

Das Hardwarekonzept besteht aus der Zusammenstellung von Funktionsmodulen, die innerhalb der Leistungsgrenzen in beliebiger Kombination um ein Zentralmodul zu einem System konfiguriert werden.

Da WESTRACE eine geringere Leistungsfähigkeit besitzt als alle zuvor beschriebenen ESTW, fallen die Stellbereiche sehr viel kleiner aus. Die kleineren Stellbereiche haben den Vorteil erheblicher Kabelkosteneinsparung, da die einzelnen (kleinen) Stellwerke nur durch ein serielles Datenkabel verbunden werden. Dafür ist die gesamte Steuerlogik über die Bahnanlage verteilt.

Klein- und Kleinststellwerke (**Small Interlocking**) sind das hauptsächliche Anwendungsgebiet von WESTRACE. Meistens bekommt jeder Bahnhofskopf (engl.: end of loops) sein eigenes WESTRACE-Stellwerk. Nur bei Stellbereichen mit sehr wenigen Elementen werden Ein- und Ausgabemodule „ferngesteuert“ (Remote I/O). Abbildung 23 verdeutlicht die Möglichkeiten.

Übersteigt die Anzahl der benötigten Ein- und Ausgaben die Kapazität eines „Small Interlocking“, so wird ein „**Large Interlocking**“ eingesetzt (Abbildung 24). Dabei kommt im VLM ein leistungsstärkerer Prozessor zum Einsatz, der die ausgelagerten Ein- und Ausgabemodule fernsteuert.

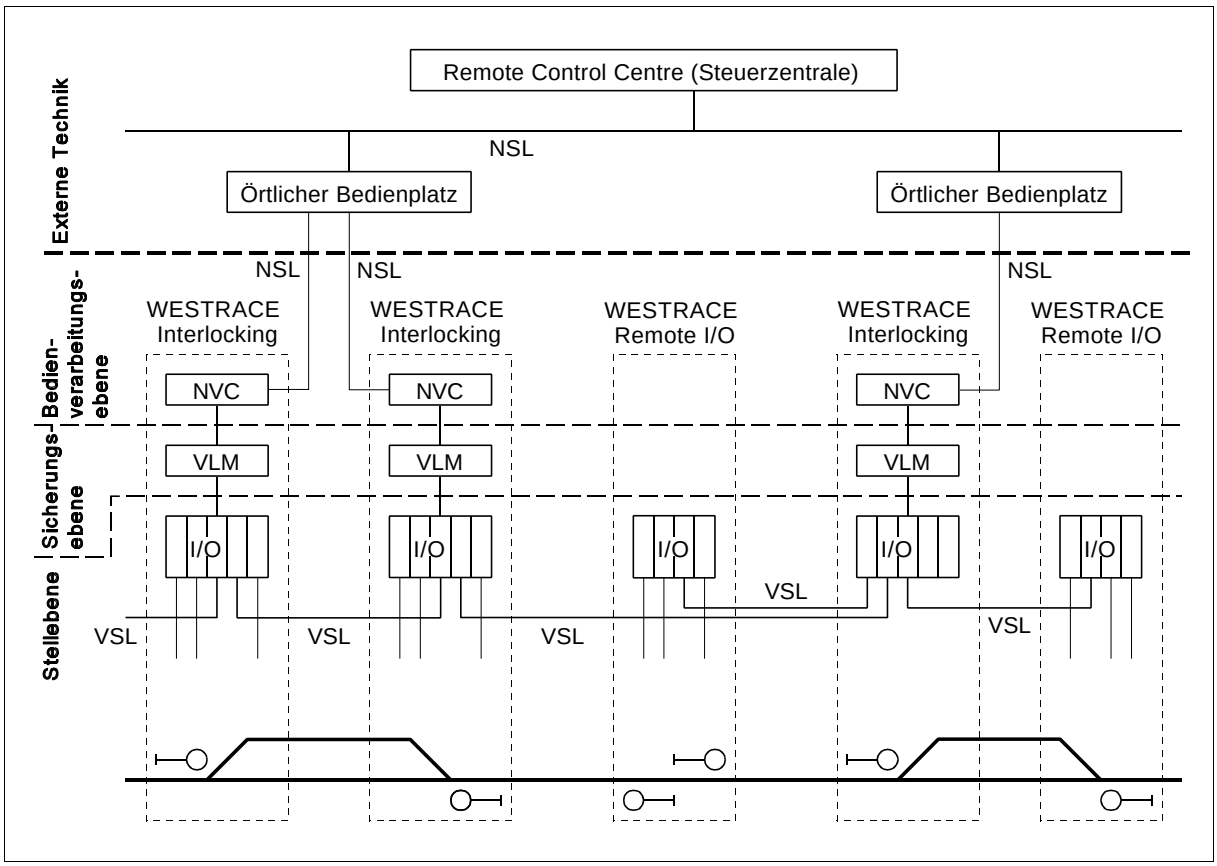


Abbildung 23: Beispielkonfiguration eines WESTRACE Small Interlocking

I/O	Input/Output Modules (Ein- und Ausgabemodule)	NVC	Non-vital Communication Module
NSL	Non-vital Serial Link (Nicht sichere serielle Verbindung)	VLM	Vital Logic Module
		VSL	Vital Serial Link (Sichere serielle Verbindung)

Als Systemkern benötigt WESTRACE das Vital Logic Module (VLM, Sicheres Logik-Modul) für die zentrale Bearbeitung. Dieses Modul ist über Betriebs- und Funktionsüberwachungsbusse mit den Ein- und Ausgangsmodulen verbunden. Folgende Module stehen dafür zur Verfügung:

- Vital Parallel Input Module (VPIM, Sicheres Modul für parallele Eingänge)
- Vital Relay Output Module (VROM, Sicheres Modul für Relais-Ausgänge)
- Vital Lamp Output Module (VLOM, Sicheres Modul für Lampen-Ausgänge)
- Vital Telemetry Modules (verschiedene Module für sicheren Datenaustausch)
- Non-Vital Communications Module (NVC, Nicht sicheres Modul für Datenaustausch)

Die Vital Telemetry Modules ermöglichen die Kommunikation der Stellwerke untereinander. Über das Non-Vital Communications Module erfolgt der Anschluß an die Bedieneinrichtungen. Eine Funk-Zugbeeinflussung (**A**dvanced **T**rain **C**ontrol **S**ystem, **ATCS**) wurde auf Grundlage der WESTRACE-Module von Westinghouse (Australien) entwickelt. Dabei sind drei Systeme

notwendig: Wayside Interface Unit (Ortsfeste Einrichtung), On Board Computer (Fahrzeugeinrichtung) und Central Despatch Computer (Bedieneinrichtung) [29].

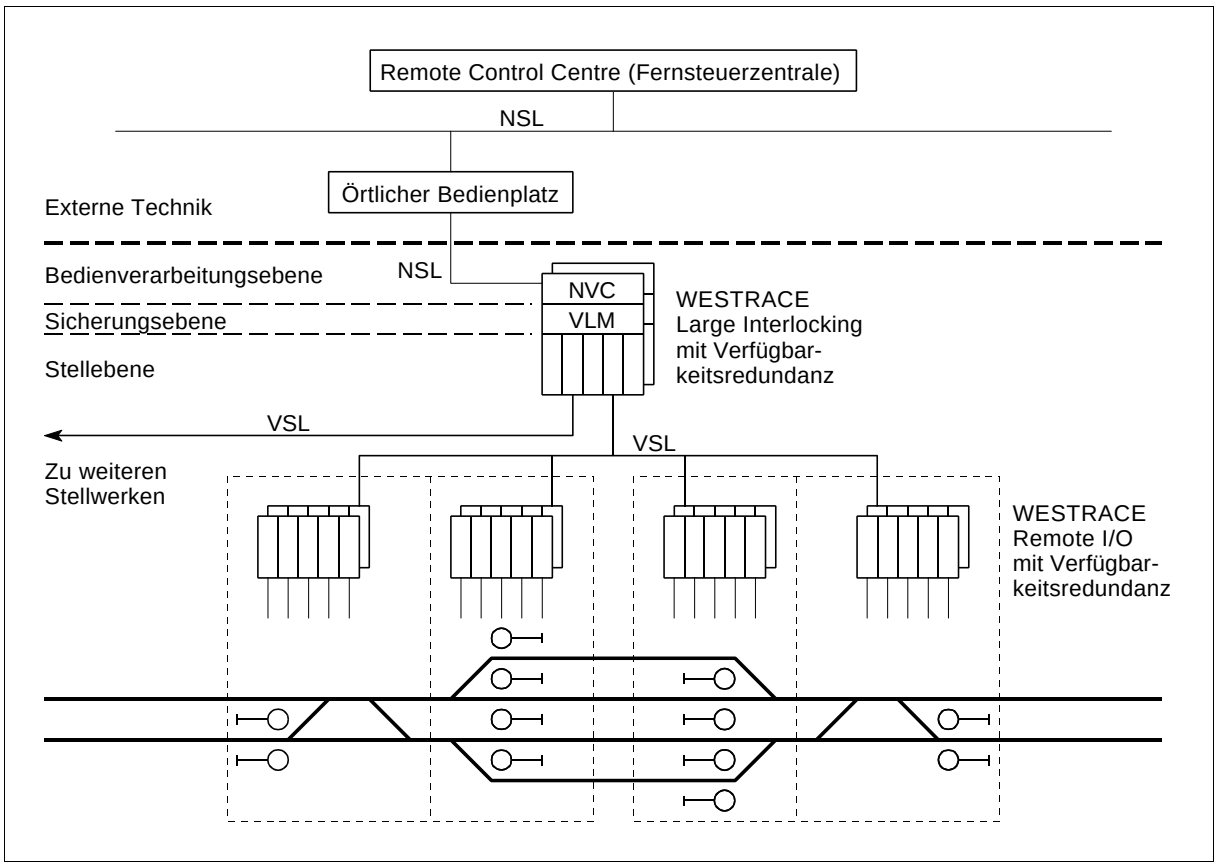


Abbildung 24: Beispielkonfiguration eines WESTRACE Large Interlocking mit Redundanz

NSL	Non-vital Serial Link	VLM	Vital Logic Module
NVC	Non-vital Communication Module	VSL	Vital Serial Link

6.2.2 Rechner und Verstärker

Obwohl Westinghouse von Modulen spricht, entsprechen die Module trotzdem Rechnern im bisher verwendeten Sinn. Es werden darin Prozessoren der Reihe 8088 und 8086 eingesetzt.

6.2.2.1 Bedienrechner

Ein spezieller Bedienrechner ist nicht vorhanden; die Funktionen werden im Zentralrechner realisiert. Die Non-vital I/O-Module können nicht als Bedienrechner angesehen werden, da sie lediglich als Schnittstelle fungieren und in ihnen keine Bearbeitung der Bedienkommandos erfolgt.

6.2.2.2 Zentralrechner

Das Vital Logic Module (VLM) beinhaltet die Gesamtsteuerung des Systems, einschließlich der Kommunikation mit den Ein- und Ausgangsmodulen. Dabei führt das VLM die Verarbeitungen der

Stellwerkslogik aus, steuert die Funktion des Sicherheitsabschalters (OPCR) und ist beteiligt am Sicherheitsmanagement. Folgende Operationen werden zyklisch vom VLM ausgeführt:

- Einlesen der Daten von den Eingangsmodulen
- Bearbeitung der Logik
- Durchführung des Selbsttests, Test der Nachbarmodule
- Übertragen der Daten zu den Ausgangsmodulen.

6.2.2.3 Peripheriерechner

Alle nachfolgend beschriebenen Ein- und Ausgangsmodule enthalten einen eigenen Prozessor, der einen Selbsttest des Moduls und einen Test der Nachbarmodule durchführt [28].

Vital Parallel Input Module (VPIM)

Das VPIM ist ein Schnittstellen-Modul mit zwölf sicheren Eingängen. Diese werden zum Einlesen der aktuellen Zustände von Feldelementen wie z. B. Gleisfreimeldungen oder Weichenüberwachungsmeldungen genutzt. Es sei angemerkt, daß die Weichenüberwachung wie beim SSI durch gesonderte Prüfstromkreise realisiert wird – im Gegensatz zur deutschen Philosophie, bei der die Weichenüberwachung durch Prüfströme in den Stellstrom-Adern erfolgt [28].

Vital Relay Output Module (VROM)

Für die sichere Steuerung von Signalrelais, die ihrerseits die Stellelemente anschalten, steht das VROM zur Verfügung. Ein VROM kann bis zu acht Ausgänge ansteuern [28].

Vital Lamp Output Module (VLOM)

Das VLOM ist ein sicheres Modul für die direkte Ansteuerung von Signallampen und zur Überwachung der Lampenfäden (einschließlich Kaltfadenprüfung). Es kann für Gleich- und Wechselstrom eingesetzt werden sowie für statische und blinkende Signalbilder. Das Modul wird in zwei Größen angeboten; die kleine Version beherrscht sechs, die große zwölf Lampenfäden. Der prinzipielle Aufbau entspricht dem der VPIM und VROM [28].

Damit das Signal im Fehlerfall einen Halt-Begriff zeigt, wird die entsprechende Signallampe zusätzlich durch einen Kontakt des OPCR angesteuert, der dann schließt, wenn das Relais abfällt und damit alle weiteren Ausgaben verhindert [30].

6.2.2.4 Diagnoserechner

Zur Aufzeichnung der Betriebsdaten kann ein „Event Recorder“ angeschlossen werden. Dieser externe Recorder zeichnet alle internen Zustände sowie die Zustände der Ein- und Ausgänge auf.

6.2.2.5 Leistungsschalter

Die Leistungsschalter für Signallampen sind im VLOM integriert. Elektromechanische Elemente, wie Weichen oder Blocktechniken, werden von Signalrelais geschaltet, die durch das VROM gesteuert werden [30].

6.2.3 Interne Kommunikation

6.2.3.1 Aufbau

Die Kommunikation der Module innerhalb eines WESTRACE-Interlocking kann mangels Informationen nicht beschrieben werden. Es ist aber festzustellen, daß die Übertragungswege sehr kurz sind. Sichere Datenübertragung wird außerdem praktiziert, um mit benachbarten Stellwerken (Vital Slotting) und mit ausgelagerten I/O-Modul-Stationen (Vital Remote) zu kommunizieren. Für die beiden Arten der Kommunikation stehen zwei verschiedene Module zur Verfügung.

Vital Serial I/O (Slotting)

Dieses Modul kann acht Bit Ein- und Ausgangsdaten mit einem benachbarten Stellwerk austauschen. Da bis zu drei solcher Module an ein Interlocking angeschlossen werden können, kann mit maximal drei benachbarten Stellwerken kommuniziert werden. Nach Literaturangaben werden die Informationen „im Block“ ausgetauscht [30]. Vermutlich ist damit ein Austausch im Telegrammformat gemeint.

Vital Serial I/O (Remote)

Ein solches Modul kann Daten übertragen, mit denen sechzehn sichere parallele Eingänge und acht sichere parallele Ausgänge von ausgelagerten I/O-Modulen ferngesteuert werden können. In einem Small Interlocking können bis zu drei, in einem Large Interlocking bis zu 32 dieser Module integriert werden [30].

6.2.3.2 Datenübertragung

Die Datenübertragung erfolgt mit 1200 Baud. Dabei wird das standardisierte Protokoll RS422 oder RS232 genutzt [30].

6.2.4 Leistungsparameter

Eine Angabe von beherrschbaren Stell- und Meldeelementen pro Stellwerk ist nur eingeschränkt möglich, da lediglich die Anzahl der sicheren Ein- und Ausgänge bekannt ist. Wie diese verwendet werden, steht dem Anwender frei. Einschließlich der ferngesteuerten I/O-Module besitzt ein ESTW WESTRACE folgende Leistungsgrenzen:

	Small Interlocking	Large Interlocking
Nicht sichere Eingänge	48	150
Nicht sichere Ausgänge	64	200
Sichere Eingänge	48	440
Sichere (Relais-) Ausgänge	48	320
Sichere Lampenansteuerungen	32	keine Angabe

6.3 Software

6.3.1 Struktur und Logikmodell

Das Stellwerkskonzept, flexibel in der Anpassung an Bedingungen verschiedener Bahnverwaltungen zu sein und vorwiegend kleine Anlagen zu steuern, spiegelt sich auch in der Software wieder. Die projektierten Daten sind so einfach gestaltet, daß es keine Verschlußtabellen gibt, sondern die Steuerungsbedingungen direkt in Boolsche Ausdrücke umgesetzt werden [28]. Bei einer überschaubaren Anzahl von Feldelementen ist dies sicherlich die einfachste Methode der Software-Projektierung; ohne geeignete Projektierungswerkzeuge stößt diese Methode aber bei umfangreichen Anlagen schnell an ihre Leistungsgrenzen.

Da alle Steuerungsbedingungen in der projektierten Software enthalten sind, gibt es nur zwei Software-Ebenen: Systemprogramme und projektierte Daten. Gegenüber dem El S bietet dies den Vorteil, daß die Anpassung an bahnverwaltungsspezifische Forderungen nicht von einem Softwarespezialisten vorgenommen werden muß, sondern auch vom Anwender erfolgen kann.

6.3.2 Projektierung

Das Projektierungssystem (Configuration Sub System, CSS) läuft auf einem herkömmlichen, IBM-kompatiblen PC. Die Tools sind so aufbereitet, daß ein Signalingenieur, der mit Relaistechnik vertraut ist, die Projektierung, Programmierung und den Test durchführen kann. Die Steuerungsbedingungen werden den herkömmlichen Relaisschaltungen entnommen und vom Projektant am Projektierungssystem in Boolsche Ausdrücke umgesetzt (Ladder Logic Diagram). Danach wird die Hardware projektiert. Nach der Compilierung werden die Daten auf EPROM gespeichert; im Anschluß daran können sie getestet werden [28].

6.4 Externe Einflußnahme

Zur Bedienung kann ein örtlicher Bedienplatz (Local Control Panel) angeschlossen werden. Die Bedienung des Stellwerks geschieht jedoch in der Regel von einer (Fern-) Steuerzentrale (Remote Control Centre). Diese, mit einer Betriebszentrale vergleichbare Einrichtung, beinhaltet neben rechnerunterstützten Bedienplätzen mit Monitoren zur Anzeige auch eine automatische Fahrplanüberwachung, die mit einer Echtzeit-Anzeige des Bildfahrplans gekoppelt werden kann [30].

7 VPI (GRS)

General Railway Signal (GRS) ist eine traditionsreiche amerikanische Signalbaufirma, dessen Erfahrungen bis zur Jahrhundertwende zurückreichen. GRS gehört heute zur Firma SASIB (Italien), die in Europa für die Vermarktung von VPI zuständig ist. In den Niederlanden wird VPI durch die Firma ASI unter Lizenz von SASIB bzw. GRS vertrieben.

Nach eigenen Angaben hat GRS mehr Strecken mit Sicherungstechnik ausgerüstet als je eine andere Firma. Nicht zuletzt deshalb bezeichnet sie sich als weltweit führenden Entwickler und Hersteller von Verkehrssicherungs- und steuerungstechnik [31]. Diese Behauptung kann aber – wenn überhaupt – nur dann aufrechterhalten werden, wenn man den Bereich der elektronischen Sicherungstechnik auf Systeme mit einkanaliger Hardware begrenzt, da GRS die Entwicklung mehrkanaliger Mikrorechentechnik für sichere Systeme bereits vor Jahren eingestellt hat [32].

VPI (**V**ital **P**rocessor **I**nterlocking) wurde Anfang der achtziger Jahre entwickelt und zeigt große Ähnlichkeit mit dem später von Westinghouse entwickelten System WESTRACE. Es hat bereits eine weite Verbreitung gefunden und wird u.a. in den USA, den Niederlanden, Spanien, Italien, Australien und Asien eingesetzt.

7.1 Sicherheits- und Verfügbarkeitskonzept

7.1.1 Datenverarbeitung

VPI ist ein System mit einkanaliger Hardware. Im Zentralrechner laufen die Programme der „Primary Logic“, die die reine Anwenderlogik enthält, und der „Safety Assurance Logic“ zyklisch nacheinander ab; letzteres ist mit den Online-Prüfprogrammen des El S vergleichbar [33]. Die Safety Assurance Logic (etwa: Algorithmus zur Gewährleistung der Sicherheit) ist eine GRS-eigene Entwicklung, die in allen sicherheitsrelevanten Produkten der Firma zum Einsatz kommt. Um den stellwerksspezifischen Ansprüchen gerecht zu werden, wurde sie zur „Numerically Integrated Safety Assurance Logic“ weiterentwickelt [35].

Während die Primary Logic die eigentlichen Stellwerksfunktionen wahrnimmt, wird durch die Sicherheitslogik die korrekte Ausführung der Programmabläufe und der Zustand der Ausgabebaugruppen überwacht. Die Überwachung geschieht durch Prüfworte, die durch das System zirkulieren und anschließend auf Korrektheit geprüft werden. Somit arbeitet VPI nicht nur mit einkanaliger Hardware, sondern auch mit einkanaliger Software, da die Sicherheitslogik nur Überwachungsfunktionen wahrnimmt. Der einzige zweikanalige Ansatz besteht in der Ablage der Daten im Speicher; darüber hinaus erfolgt die Abspeicherung diversitär.

Der Hauptzyklus, in dem die Bearbeitung der Stellwerkslogik erfolgt, dauert eine Sekunde. Zwanzig mal, also alle 50 ms, wird er durch den Sicherheitszyklus unterbrochen. Dabei werden alle eingeschalteten, sicheren Ausgänge darauf geprüft, ob sie, gemäß des Speichers im Zentralrechner, auch eingeschaltet sein dürfen. Nicht geprüft werden die ausgeschalteten Ausgänge, auch

wenn sie eingeschaltet sein müßten; dieser Fehler wirkt sich jedoch nur hemmend, nicht aber sicherheitskritisch aus.

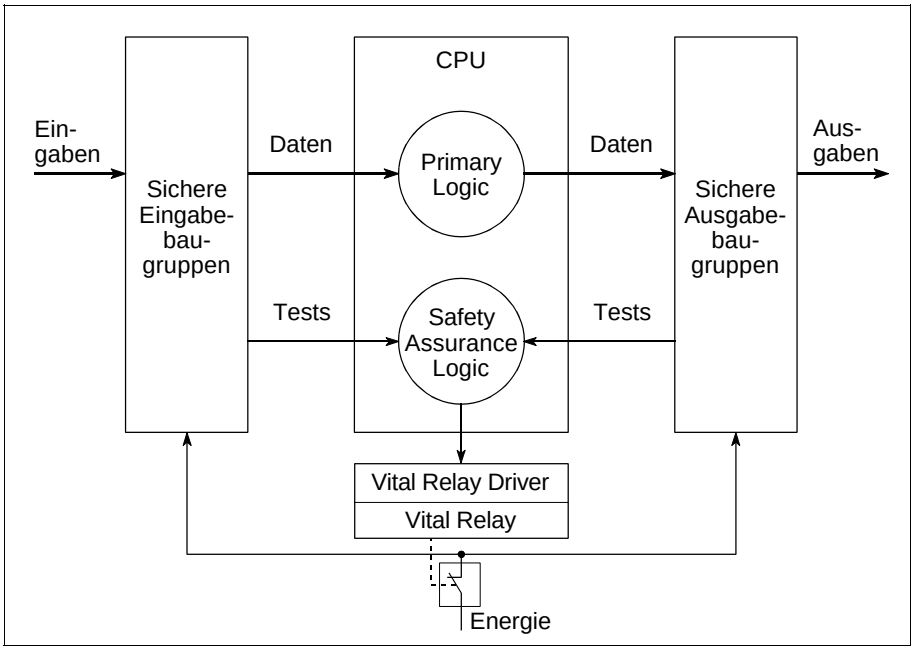


Abbildung 25: Sicherheitsstruktur des ESTW VPI

Wird im Haupt- und Sicherheitszyklus durch die Überwachungslogik kein Fehler erkannt, so wird über die Vital Relay Driver-Baugruppe ein Klasse I-Relais angesteuert. Diese Ansteuerung muß alle 50 ms „aufgefrischt“ werden. Nur wenn das Relais angezogen ist, werden die Ein- und Ausgabebaugruppen mit Energie versorgt. Es ist sichergestellt, daß das Relais spätestens 150 ms nach Erkennen eines Fehlers abfällt [34].

Um die Verfügbarkeit zu erhöhen, kann des System redundant ausgeführt, d. h. komplett verdoppelt werden. Damit im Fehlerfall ohne Verzögerung umgeschaltet werden kann, ist eine Gleichheit der aktuellen Daten in beiden Systemen erforderlich. Beide Systeme sind mit einer seriellen Datenleitung verbunden, um die Konsistenz der Daten zu gewährleisten.

7.1.2 Datenübertragung

Über die Art der Sicherung des Informationsaustauschs liegen keine Erkenntnisse vor. Vermutlich wird die Sicherheit durch Coderedundanz erreicht.

7.1.3 Bedienung und Anzeige

Es werden keine sicherheitsrelevanten Anforderungen an Bedienung und Anzeige gestellt.

7.2 Systemstruktur

Wie bei WESTRACE ist die gesamte Elektronik auf steckbaren Baugruppen realisiert, die je nach Anforderungen zu einem System zusammengefügt werden. Abweichend vom WESTRACE-Konzept wird ein komplettes System (ein ESTW) als „Modul“ bezeichnet.

Kern des ESTW ist ein Prozessor in der zentralen Baugruppe, der die Verknüpfung der Stellwerksdaten vornimmt. Weitere Prozessoren anderer Baugruppen führen untergeordnete Aufgaben aus. An die zentrale Baugruppe können Ein- und Ausgabebaugruppen bis zur Leistungsgrenze des Zentralprozessors angeschlossen werden. Ist die geforderte Kapazität größer, werden mehrere VPI-Stellwerke vorgesehen, die über serielle Datenverbindungen miteinander kommunizieren. Somit werden auch große Anlagen beherrscht, wie z. B. das Grand Central Terminal in New York, bei dem 17 VPI-Systeme zusammenarbeiten [34].

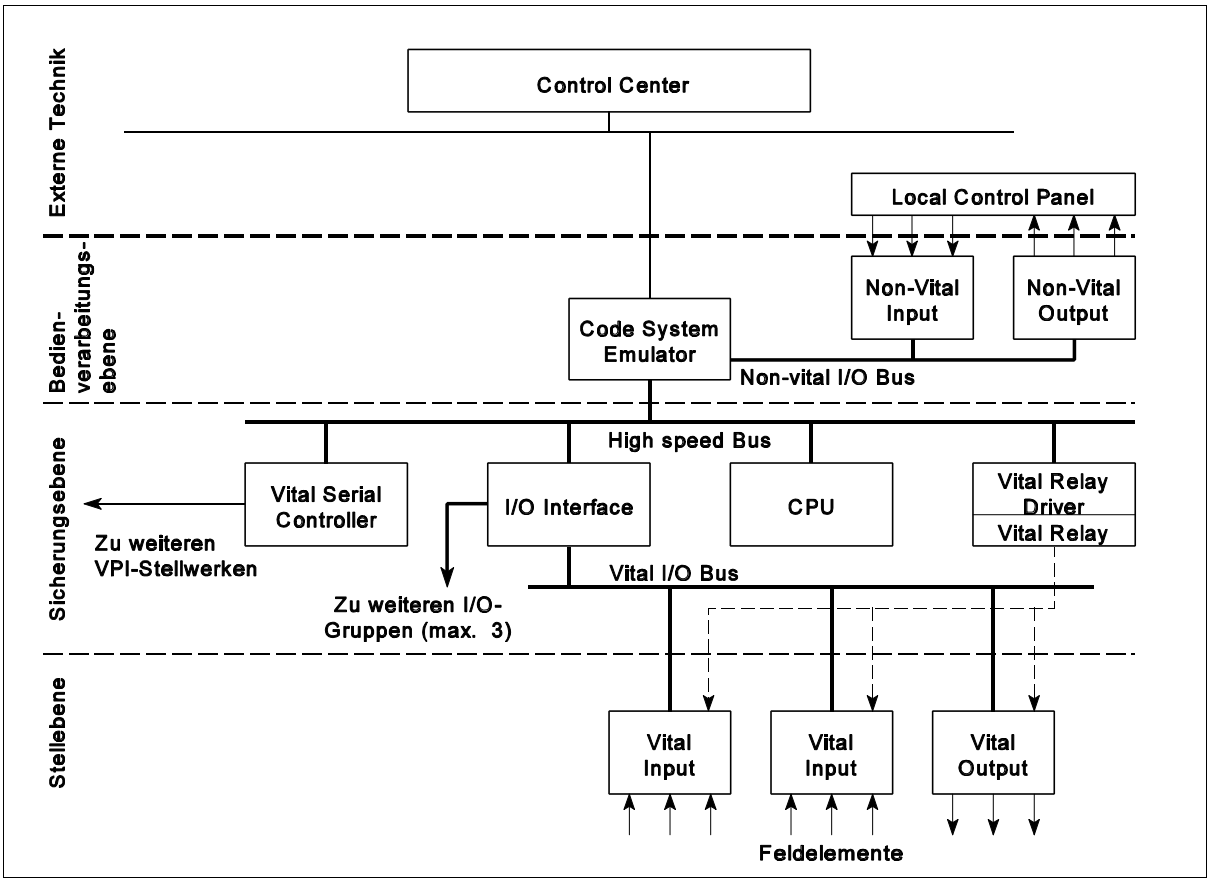


Abbildung 26: Systemstruktur des ESTW VPI

Über eine Steuerung von Relaisstellwerken wurde in der Literatur nichts ausgesagt; bei der relativ geringen Leistung eines einzelnen VPI wäre das auch nicht sinnvoll. Es ist aber anzunehmen, daß von der übergeordneten Steuerzentrale (Control Center) auch Relaisstellwerke ferngesteuert werden können.

7.2.2 Rechner und Verstärker

Obwohl in einem VPI-System mehrere Prozessoren arbeiten, sind nicht alle Baugruppen damit bestückt. Insofern ist es nicht gerechtfertigt, einige Baugruppen als „Rechner“ zu bezeichnen. Um die Einheitlichkeit der Beschreibungen zu wahren, sollen dennoch die bisher genutzten Überschriften verwendet werden.

7.2.2.1 Bedienrechner

Im VPI erfolgt eine strikte Trennung von sicheren („vital“) und nicht sicheren („non-vital“) Steuerungsaufgaben. Für die nicht sicheren Aufgaben ist der Code System Emulator zuständig. Seine wichtigste Aufgabe ist es, die Verbindung mit den lokalen oder zentralen Bedieneinrichtungen zu realisieren. Weiterhin kann er lokale Betriebsleittechniken oder Fahrgastinformationssysteme steuern. Schnittstellen sind dabei die Non-vital Input- und Non-vital Output-Baugruppen, deren parallele Ausgänge wahlfrei beschaltet werden können.

Spezielle Module können für eine „Train-to-Wayside“-Kommunikation eingesetzt werden [35]. Leider ist nicht genau bekannt, welche Informationen dabei ausgetauscht werden. Da diese Module zu den nicht sicheren gehören, liegt die Vermutung nahe, daß hier Informationen vom Fahrzeug an das Stellwerk übertragen werden, die die Einstellung eines gewünschten oder vorprogrammierten Fahrweges auslösen.

7.2.2.2 Zentralrechner

Die zentralen Stellwerksfunktionen werden in der CPU/PD-Baugruppe realisiert. Die Logik des Polynominal Deviders (PD) wurde deshalb hardwaremäßig implementiert, um die durch Polynomdivision entstandenen Sicherungscodes der durch das System zirkulierenden Prüfworte schnell auf Richtigkeit überprüfen zu können.

7.2.2.3 Peripheriерechner

Mehrere Baugruppentypen stehen für die Ausgabe von Stellbefehlen und das Einlesen von Meldungen zur Verfügung. Nachfolgend seien die wichtigsten genannt:

- Direct Input – Einlesen von Meldungen
- Lamp Driver Output – Ansteuerung von Signallampen
- Single Break Output – Ansteuerung von Ausgaberelais (Abschaltung einpolig)
- Double Break Output – Ansteuerung von Ausgaberelais (Abschaltung zweipolig) [35].

7.2.2.4 Diagnoserechner

Für die Diagnose stehen zwei Geräte zur Verfügung. Ein kleines, handliches Gerät, das Handheld Terminal, wird für die Diagnose direkt am Rechner genutzt und mittels eines kurzen Kabels mit diesem verbunden. Auf einem kleinen LCD-Display können verschiedene Daten abgelesen werden.

Als zweite Möglichkeit steht der „Tracker Remote Diagnostic Analyser“ zur Verfügung. Dieses System besteht aus einer speziellen Software, die auf einem IBM-kompatiblen PC installiert ist. Der PC kann an einer zentralen Stelle aufgestellt und über Modem mit einem oder mehreren Stellwerken verbunden sein bzw. bei Nutzung eines Laptops auch direkt im Rechnerraum eingesetzt

werden. Neben der Diagnose kann das System auch ständig Daten aufzeichnen und Alarmmeldungen an das Instandhaltungspersonal ausgeben [35].

7.2.2.5 Leistungsschalter

Für Signallampen sind keine separaten Verstärker notwendig, da diese bereits in der Ausgabebaugruppe für Signale enthalten sind. Für die Ansteuerung anderer Stellelemente werden Relais genutzt, die direkt durch die Ausgabebaugruppe angeschaltet werden [35].

7.2.3 Interne Kommunikation

Zur Realisierung der internen Kommunikation kommen mehrere Busse zum Einsatz. Über deren Aufbau und die Art der Datenübertragung gab es in der verwendeten Literatur keine Angaben.

7.2.4 Leistungsparameter

Wie im ESTW WESTRACE können die Ein- und Ausgänge des VPI wahlfrei beschaltet werden. Insgesamt kann ein VPI 320 sichere Ein- und Ausgänge steuern. Die Kapazität eines VPI wird aber nicht nur durch diese Zahl begrenzt. Auch die Anzahl der maximal adressierbaren Baugruppen, die Anzahl der Kommunikationsbaugruppen und deren Leistungsfähigkeit sowie die Verarbeitungskapazität des Zentralprozessors setzen Grenzen, die in der Gesamtheit betrachtet werden müssen. Als Beispiel sei die Kapazität der CPU herausgegriffen.

Die Bearbeitung der Stellwerkslogik erfolgt durch die Berechnung Boolscher Gleichungen. Abhängig von der Komplexität können in der CPU 2000 bis 3000 solcher Gleichungen verarbeitet werden [35].

7.3 Software

7.3.1 Struktur und Logikmodell

Wie bereits erwähnt, werden die sicherungstechnischen Abhängigkeiten ebenso wie im zuvor vorgestellten System WESTRACE durch die Verknüpfung aller relevanten Daten in Boolschen Gleichungen realisiert. Damit ergeben sich die gleichen Vor- und Nachteile, wie sie bereits beschrieben wurden. Nach [34] sind die Beherrschung großer Anlagen mit dieser Art der Logik schwierig und Änderungen aufwendig. Daß es trotzdem möglich ist, zeigt das bereits angeführte Beispiel Grand Central Terminal.

Angaben über eine hierarchische Struktur der Software lagen nicht vor.

7.3.2 Projektierung

Die Projektierung geschieht durch ein auf PC lauffähiges Softwarepaket mit dem Namen „Computer Aided Assembly (CAA)“. Hier können durch einen Signalingenieur, der mit Relaistechnik

vertraut ist, die Boolschen Gleichungen erstellt werden, die der bisherigen Logik der Relaisschaltungen entsprechen. Das Projektierungssystem stellt außerdem Funktionen bereit, um die erstellten Daten zu prüfen. Weiterhin kann mit dem Projektierungssystem die physikalische Konfiguration der Module erstellt werden.

7.4 Externe Einflußnahme

Das ESTW VPI wird seitens des Herstellers getrennt von den Bedienungsmöglichkeiten betrachtet, was auch der Definition eines ESTW in dieser Arbeit entspricht. Da nur Informationen zum VPI vorlagen, können nur wenige Aussagen über die Einflußnahme auf das Stellwerk getroffen werden. Welche Betriebsleittechniken angewendet werden, ist nicht bekannt.

Für die örtliche Bedienung steht ein Stelltisch bzw. eine Stelltafel zur Verfügung (Local Control Panel). Hauptsächlich werden die ESTW VPI jedoch von (Fern-) Steuerzentralen (Control Centre) bedient. Die Bedienplätze bestehen dabei aus einem rechnergestützten Stellpult und einem Rechnerterminal zur Kommandoeingabe. Über die aktuelle Betriebssituation werden die Bediener durch eine Anzeigetafel informiert.

8. Weitere elektronische Stellwerkssysteme

8.1 SMILE (Nippon, Daydo, Kyosan)

In Zusammenarbeit mit den japanischen Firmen Nippon, Daydo und Kyosan entwickelte die Japanische Eisenbahn (JR) das ESTW SMILE (**S**afe **M**ultiprocessor for **I**nter**l**ocking **E**quipment). Das Know-how wurde unter den Firmen ausgetauscht, so daß die JR mit SMILE über eine Einheitsbauform verfügt. Das erste Stellwerk dieser Art wurde 1987 dem Betrieb übergeben.

SMILE ist für größere Anlagen konzipiert und wird ab einem Steuerungsumfang von etwa 60 Fahrstraßen eingesetzt. Das im Bahnhof Hiroshima eingesetzte SMILE-Stellwerk hat beispielsweise einen Umfang von 587 Fahrstraßen und 174 Stellelementen. Um auch kleinere Bahnhöfe wirtschaftlich mit elektronischer Technik auszurüsten, wurde aus SMILE das System Mikro-SMILE entwickelt, mit dem maximal 80 Fahrstraßen beherrscht werden. Der wichtigste Unterschied zwischen beiden Systemen besteht darin, daß SMILE in 2v3-Rechnerkonfiguration betrieben wird, während in Mikro-SMILE eine 2v2 bzw. 2×(2v2)-Konfiguration zum Einsatz gelangt [39]. Auf Mikro-SMILE soll im folgenden nicht näher eingegangen werden.

8.1.1 Sicherheits- und Verfügbarkeitskonzept

Beim Systemaufbau wurden die Sicherheitsfunktionen von den übrigen Funktionen konsequent getrennt und in einem speziellen Sicherheitsbaustein, dem Fail-Safe Microprocessor (FSM), zusammengefaßt.

Abbildung 27: Der Sicherheitsbaustein FSM

INC Input circuit (Eingabe-Baugruppe)
MVR Majority voting restorer (Mehrheitsentscheider mit Fehlerkorrektur)
OVC Output data voting circuit (Ausgabe-Baugruppe mit Voter)

Auf den Bussen der drei Rechnerkanäle wird ein Vergleicher mit Mehrheitsentscheidung und Fehlerkorrektur (Majority Voting Restorer, MVR) zwischengeschaltet. Die drei Kanäle werden synchron betrieben. Über die bei jedem Speicherzugriff und bei jeder Ein- und Ausgabe auf den Bussen übertragenen Daten wird Bit für Bit abgestimmt. Durch die hohe Abstimmungshäufigkeit wird ein einzelner Fehler sehr schnell entdeckt.

Aufgrund der Korrektur sind die Informationen jeweils hinter dem Vergleicher identisch. Damit Fehler trotz Korrektur offenbart werden, erfolgt eine Überwachung der Daten vor und hinter dem Vergleicher in einer separaten Einrichtung, dem Fail-Safe Comparator (FSC). Darin befinden sich mehrere Hardware-Vergleicher, die die elektrischen Zustände der Busleitungen vor und hinter dem MVR auf Übereinstimmung prüfen. Eine begrenzte Anzahl von Korrekturen innerhalb einer bestimmten Zeit wird toleriert; bei Überschreitung dieser Toleranzgrenze wird die CPU des entsprechenden Kanals abgeschaltet, und die Arbeitsweise des Sicherheitsbausteins geht von 2v3 auf 2v2 über [39].

8.1.2 Systemstruktur

Die Trennung zwischen sicheren und nicht sicheren Aufgaben wird erleichtert durch die Tatsache, daß an Bedienung und Anzeige keine sicherheitsrelevanten Forderungen gestellt werden. Somit genügt der o.g. Sicherheitsbaustein (FSM), um alle sicheren Steuerungsaufgaben zu bewältigen. In den ersten SMILE-Stellwerken wurden die in den FSM integrierten Schnittstellen zur Außen-

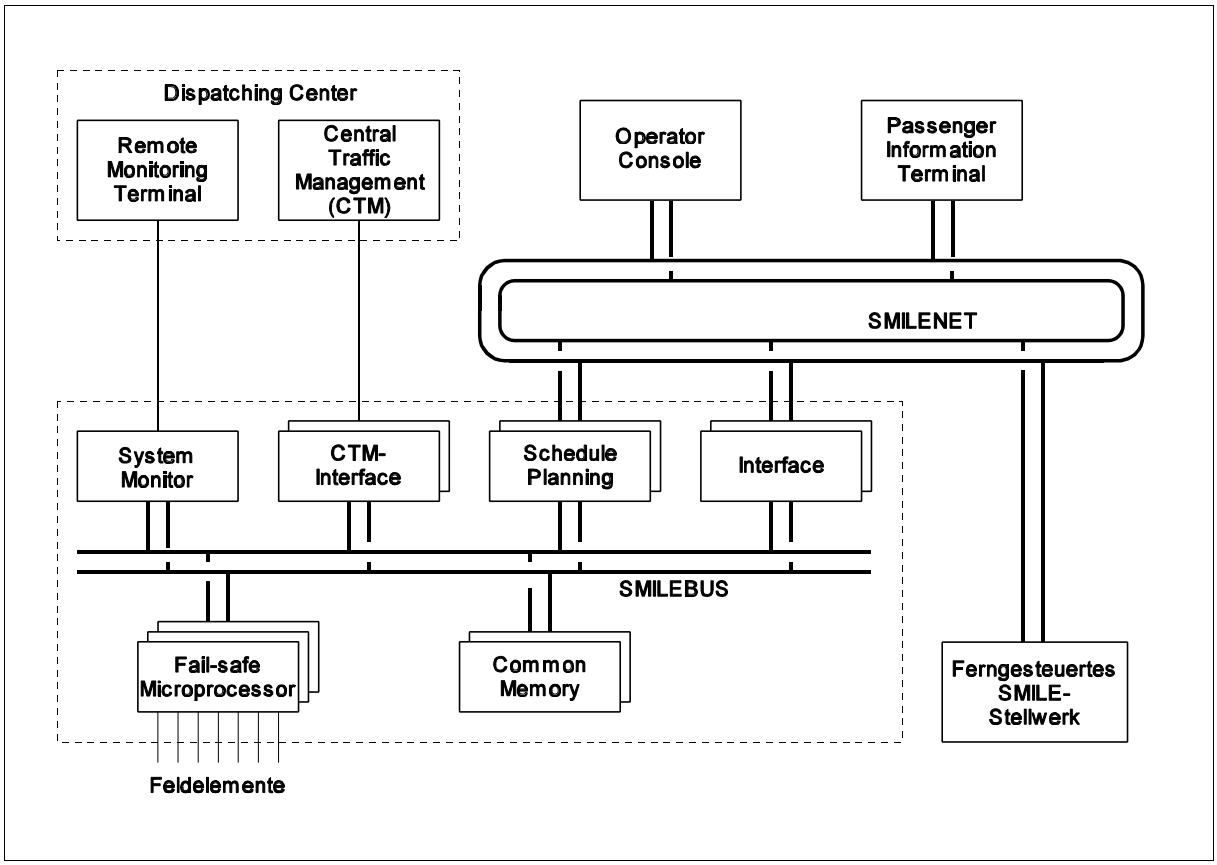


Abbildung 28: Systemstruktur des ESTW SMILE

anlage in Relaistechnik ausgeführt. Die JR beabsichtigte damals, zukünftig eine elektronische Lösung anzustreben. Es ist anzunehmen, daß dies inzwischen erfolgt ist.

Mehrere Komponenten stehen als Schnittstelle für externe Techniken zur Verfügung. Sie kommunizieren untereinander und mit dem FSM über den redundanten SMILEBUS. Bis zu 14 Rechner können daran angeschlossen werden. Interessant ist, daß alle an den SMILEBUS angeschlossenen Komponenten auf einen gemeinsamen Speicher (Common Memory) zugreifen.

Die Bedienung des ESTW erfolgt vom Dispatching Center, das aus dem Central Traffic Management (CTM) und einem Terminal zur Ferndiagnose (Remote Monitoring Terminal) besteht. Mit Ausnahme des Dispatching Centers werden alle peripheren Techniken sowie ausgelagerte Stellbereiche, die eigentlich ferngesteuerte Stellwerke sind, über das SMILENET mit dem ESTW verbunden. Das SMILENET besteht aus einem redundanten Lichtwellenleiter, der alle Komponenten ringförmig miteinander verbindet. Nur der Fahrplanrechner (Schedule Planning Microprocessor) besitzt separate Verbindungen zu SMILENET und SMILEBUS während der sonstige Datenverkehr zwischen beiden Netzen über ein Interface abgewickelt wird.

Konsequenterweise müßten die ferngesteuerten Stellwerke vom Dispatching Center gesteuert werden; dazu lagen jedoch keine Informationen vor. Die an das SMILENET angeschlossene Operator Console dient vermutlich der Einflußnahme auf den Fahrplanrechner und das Fahrgastinformationssystem (Passenger Information Terminal).

8.2 SICAS (SIEMENS)

Das El S ist ein ESTW hoher Komplexität und für die Steuerung umfangreicher Anlagen geeignet. Auch zur Steuerung kleinster Anlagen müssen in einem ESTW El S immer mehrere Rechner eingesetzt werden, was verhältnismäßig hohe Kosten für kleine Anlagen zur Folge hat. Aus diesem Grund setzt beispielsweise die NS neben dem El S für große Bahnhöfe das VPI für kleine Bahnhöfe ein [34].

Die Software des El S bietet wenig Flexibilität bei der Anpassung an bahnverwaltungsspezifische Gegebenheiten; außerdem muß die Anpassung durch Softwarespezialisten vorgenommen werden. Dieser Aufwand ist bei vielen ESTW anderer Bauformen nicht notwendig.

Um ein ESTW für kleinere Anlagen, welches die genannten Nachteile nicht aufweist, anbieten zu können, wurde unter dem Namen SICAS (**SI**EMENS **C**omputer **A**ided **S**ignalling), aufbauend auf den bisherigen umfangreichen Erfahrungen, eine neue Stellwerksbauform entwickelt. Sie soll den Anforderungen möglichst vieler Fern-, Stadt- und Industriebahnen nach hoher Flexibilität, einfacher Umsetzung der kunden- und anlagentypischen Betriebsbedingungen, kurzen Bauzeiten und einfachen Umbaumöglichkeiten gerecht werden. Durch den verstärkten Einsatz handelsüblicher Komponenten und das Anwenden moderner Methoden des Software-Engineerings kann die Realisierung kleiner und mittelgroßer Stellwerksanlagen sowie die Anpassung an unterschiedliche Betriebskonzepte kostengünstiger als mit dem El S durchgeführt werden.

Nach einer Entwicklungszeit von nur zwei Jahren wurde im Mai 1995 mit der ersten Inbetriebnahmephase eines SICAS-ESTW bei der Kölner Verkehrs-Betriebe AG begonnen [40].

8.2.1 Sicherheits- und Verfügbarkeitskonzept

Für die Bearbeitung der zentralen Stellwerkslogikfunktionen wird auf bewährte Rechnerhardware zurückgegriffen; im Kern des ESTW gelangt ein SIMIS 3216-Rechner zum Einsatz. Dieser wird, je nach Verfügbarkeitsanforderungen, in 2v2- oder 2v3-Konfiguration ausgeführt. Da das SIMIS-Konzept bereits bei der Behandlung des El S beschrieben wurde, soll an dieser Stelle nicht weiter darauf eingegangen werden.

Die Bedienung und Anzeige kann sowohl ungesichert als auch verfahrensgesichert realisiert werden [40]. Bei der Verfahrenssicherung wird mit einem Referenzrechner analog des BPS 901 operiert.

8.2.2 Systemstruktur

Aufgrund der Flexibilität des Systems ist die Hardwarearchitektur vielfältig gestaltbar. Kern des Systems ist in jedem Fall ein SIMIS-Rechner, der die sicherungstechnischen Verknüpfungen vornimmt.

Die Realisierung der Bedienung und Anzeige kann lokal oder zentral erfolgen. Sowohl dafür als auch für Diagnosezwecke und als Schnittstelle zu weiteren externen Techniken kommen herkömmliche PC mit 80486- bzw. Pentium-Prozessoren und MS-Windows als Betriebssystem und Bedienoberfläche zum Einsatz. Alternativ zu den PC kann für Bedienung und Anzeige eine Stell- und Meldetafel verwendet werden. Die Informationen werden dann durch eine speicherprogrammierbare Steuerung vom Typ SIMATIC S5 verarbeitet.

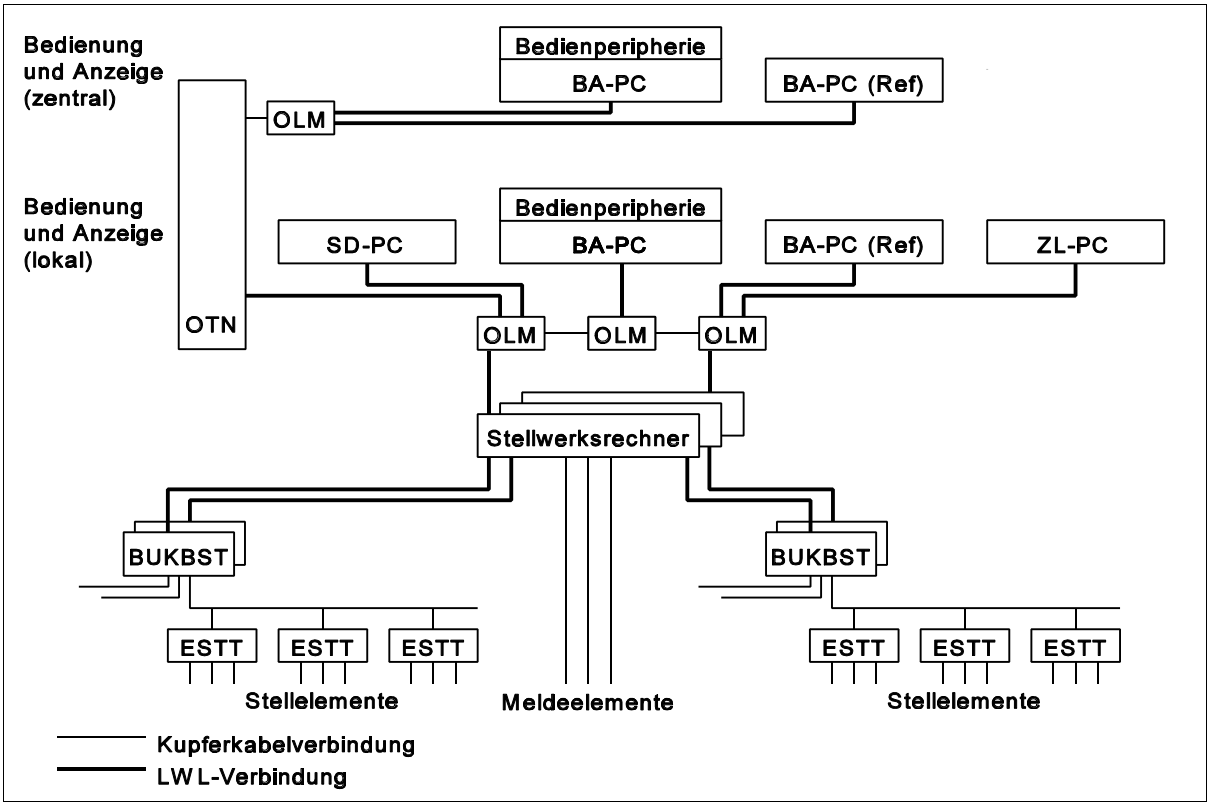


Abbildung 29: Systemstruktur des ESTW SICAS

BA-PC	PC für Bedienung und Anzeige
BA-PC (Ref)	Referenz-PC für Bedienung und Anzeige
BUKBST	Buskoppelbaustein
ESTT	Elektronisches Stellteil
OLM	Optical Link Module
OTN	Open Transport Network
SD-PC	PC für Service und Diagnose
ZL-PC	PC für Kopplung mit Zuglenkung

Eine Neuentwicklung sind die elektronischen Stellteile (ESTT). Sie können, abhängig von der Anlagenkonfiguration, zentral im Stellwerksgebäude oder, bei ausgelagerten Stellbereichen, dezentral angeordnet werden. Stellentfernungen von bis zu 6,5 km sind realisierbar. Das ESTT besteht generell aus einem Rechner- und einem Leistungsteil. Der Rechner des Stellteils, ausgerüstet mit einem 80188-Prozessor, basiert auf dem 2v2-SIMIS-Prinzip und ist in allen Stellteilarten gleich, während sich die Leistungsteile je nach Aufgabe des Stellteils unterscheiden. Es gibt Leistungsteile für folgende Anwendungen:

- Weichenantrieb
- Lichtsignale mit bis zu insgesamt acht Lichtpunkten und Fahrsperre
- Geschwindigkeitsüberwachungseinrichtung

- BÜ-Sicherungsanlage
- frei verwendbare Ein- und Ausgänge.

Bei geringeren Sicherheitsanforderungen können vereinfachte dezentrale Stellteile (DSTT) eingesetzt werden. Neben einer geringeren Anforderungsklasse nach DIN 19250 (ESTT: AK 7; DSTT: AK 6) besitzen sie auch eine kleinere Stellentfernung (1000 m) und eine geringere Leistungsfähigkeit. Die DSTT sind jedoch klimafester und können somit in Schränken der Außenanlage angeordnet werden.

Die Verbindung der Komponenten untereinander erfolgt unter Nutzung handelsüblicher Hardware hauptsächlich auf Basis des Profibus nach DIN 19245, aber auch mit V.24-Schnittstellen [40].

8.2.3 Software

8.2.3.1 Struktur und Logikmodell

Um eine aufwandsarme Anpassungsfähigkeit der Software an kundenspezifische Bedingungen zu erreichen, wurde das Software-Konzept völlig neu gestaltet. Im Gegensatz zum El S erfolgt die Bearbeitung der Stellwerkslogik nach dem Verschlußplanprinzip. Dabei werden die statischen Betriebszustände aller Feldelemente in Tabellenform erfaßt. Die Verknüpfung der Elemente im Rahmen der Fahrstraßenbehandlungen erfolgt über einen für alle Anwendungen einsetzbaren minimalen Software-Kern. Die Anpassung an spezifische Bedingungen erfolgt durch Parametrierung der jeweiligen Anwendung [40].

8.2.3.2 Engineeringprozess

Die Stellwerks- sowie die Stell- und Überwachungslogik wurden nach gleichem Prinzip entworfen und implementiert. Die durchgängige Vorgehensweise erleichtert das Anpassen der Betriebslogik an bahnverwaltungsspezifische Anforderungen.

Zur Realisierung der bahnverwaltungsspezifischen Logik wurde erstmals eine objektorientierte Methode gewählt. Der Signalingenieur, ausgestattet mit dem notwendigen Prozeßwissen, beschreibt zunächst als Modellierer objektorientiert die Struktur der Logik und anschließend als Projektant die betrieblichen Bedingungen, Abhängigkeiten und Projektierungsfälle in der prozeßorientierten Sprache SIL (SIEMENS **I**nterlocking **L**anguage). SIL umfaßt etwa 50 sogenannte Schlüsselsymbole und unterstützt einen objektorientierten und ereignisorientierten Ansatz. Durch den Einsatz von Prüfprogrammen wird die Fehlerträchtigkeit bereits beim Modellentwurf gesenkt. Die Modelle sind nach diesen Prüfungen formal widerspruchsfrei.

Das erstellte Modell wird im nächsten Schritt vom Signalingenieur mittels Testfällen verifiziert; zur Unterstützung dieser Tätigkeit kann das Modell auf einem PC simuliert werden. Die grafische Simulation ermöglicht die Projektierung beliebiger Anlagentopografien, die Anzeige beliebiger Logikzustände und die Simulation von Stör- und Regelverhalten der Feldelemente. Fehler im

Logikmodell und im Projekt können bereits bei der Simulation erkannt werden. Die ermittelten Testfälle werden gespeichert und können jederzeit in Einzelschritten oder im Gesamtlauf wieder eingespielt werden.

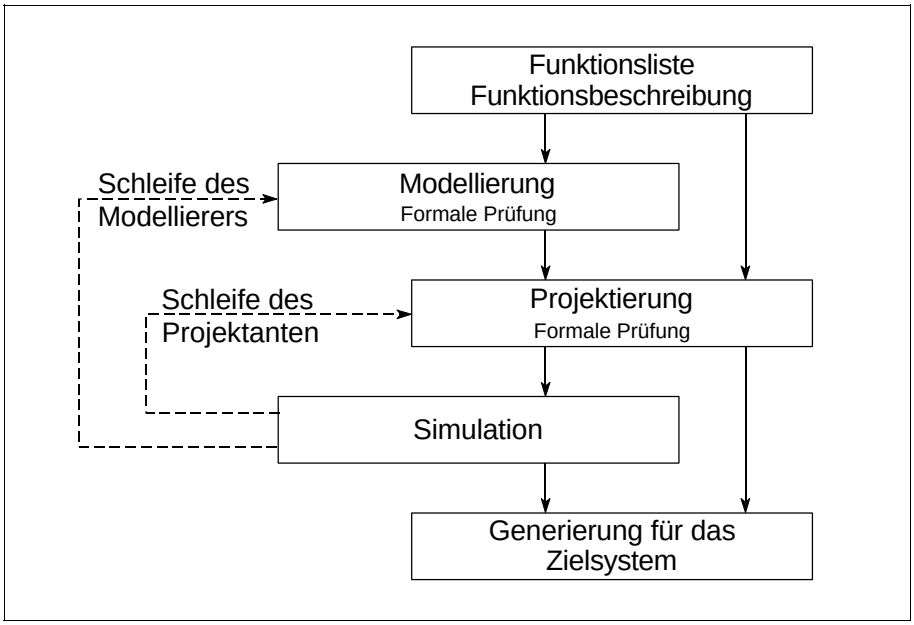


Abbildung 30: Übersicht über den SICAS-Engineeringprozeß

Nachdem die Logik getestet wurde, kann das Modell in eine Datenstruktur überführt werden, die auf dem Zielsystem (dem SIMIS-Rechner) durch einen Automateninterpreter zum Ablauf gebracht wird. Das Verhalten des Automateninterpreters entspricht dem Verhalten in der Simulation.

Ohne Veränderungen können die Modelle auf andere Zielrechner gebracht werden, vorausgesetzt der neue Zielrechner erfüllt die Leistungsanforderungen des Interpreters. So können die gleichen Modelle auch auf der Hardware nächster Generationen eingesetzt werden [40].

8.3 MCDS (IVV)

„Als Beratungsunternehmen und System-Softwarehaus für die Logistik im öffentlichen Verkehr sowie als Entwickler von elektronischen Bahnsteuerungssystemen ist die in Braunschweig ansässige IVV eine weit über die Grenzen des Bundesgebietes hinaus bekannte Ingenieurgesellschaft für Innovation und Technologieführung im Verkehrswesen. Darin bestätigt sich der Erfolg eines Konzeptes, das seit 1970 die ingenieurmäßige Umsetzung wissenschaftlicher Erkenntnisse aus den Bereichen Verkehrstechnik, angewandte Informatik und Systemlogistik in die praktische Anwendung unter marktwirtschaftlichen Kriterien zum Ziel hat. Aus einer Personengesellschaft heraus wurde die IVV Ingenieurgesellschaft für Verkehrsplanung und Verkehrssicherung GmbH im Jahre 1980 von Univ.-Prof. Dr.-Ing. Klaus Pierick und Prof. Dr.-Ing. Klaus-D. Wiegand gegründet.“[45]

Das Ergebnis sind innovative Produkte wie die Softwaretools der „Pro“-Familie und das Microcomputergesteuerte Dezentrale Steuerungssystem (MCDS). Mit MCDS lassen sich komplette ESTW realisieren, die im Verbund mit dem Pro-System eine integrierte Disposition und Betriebsführung ermöglichen [42]. Das MCDS wurde für die Steuerung von Bahnanlagen kleineren und mittlereren Umfangs entwickelt. Anwender sind Industrie-, Stadt- und NE-Bahnen; Bahnverwaltungen also, die auch Zielgruppe von SICAS sind.

Die erste und heute umfangreichste MCDS-Anlage wurde 1989 bei der Eisenbahn und Häfen GmbH, Duisburg in Betrieb genommen. Diese nutzt auch das Dispositionssystems „ProDis“, welches für Industriebahnen besonders geeignet ist, da dort nicht nach Fahrplan gefahren wird, sondern jede einzelne Fahrt „eingelegt“ wird [43]. Neben weiteren Industrie-, Stadt-, Straßen- und NE-Bahnen in Deutschland, wird MCDS derzeitig bei einer schweizer Privatbahn eingesetzt [42, 44].

8.3.1 Sicherheits- und Verfügbarkeitskonzept

Für die sichere Datenverarbeitung wurde ein 2v2-Rechnersystem entwickelt. Nach Literaturangaben erfolgt der Datenvergleich durch Software [42]. Nach Aussage eines IVV-Mitarbeiters werden die Rechenergebnisse durch Soft- und Hardware verglichen. Die Tatsache, daß in den Rechnern pro Kanal eine Vergleicherbaugruppe existiert, erhärtet die Aussage. Eine Verfügbarkeitsredundanz ist nicht vorgesehen.

Die Sicherung der Datenübertragung erfolgt ähnlich wie im El S. Die Telegramme erhalten einen Sicherungsanhang, der eine Hamming-Distanz von d = 6 gewährleistet. Darüber hinaus werden die über einen physikalisch zweikanaligen Bus gesendeten Telegramme im Zielrechner auf Übereinstimmung geprüft. Bei Ausfall eines Buskanals erhalten die Telegramme doppeltes Format.

Bedienung und Anzeige können sicherheitsrelevant ausgelegt werden. Da dafür handelsübliche Hardware zum Einsatz kommt, werden Befehle und Meldungen verfahrensgesichert. Die Sicherung der Anzeige erfolgt durch einen zweikanaligen Bildspeicher, deren Inhalte miteinander verglichen

werden. Um ein sicherheitsrelevantes Kommando abzugeben, muß der Bediener zunächst den Befehl eingeben. Wenn der Befehl durch die Anlage auf Ausführbarkeit geprüft und für zulässig befunden wurde, wird das entsprechende Element auf dem Bildschirm markiert. Der Bediener muß nun den Befehl ein zweites Mal eingeben, damit das Kommando zur Ausführung gelangt.

8.3.2 Systemstruktur

Eine MCDS-Zentrale besteht aus dem Datenkonzentrator (DKZ) sowie einem handelsüblichen PC mit Monitor, Tastatur und Drucker für Bedienung und Anzeige. Der DKZ stellt die Verbindung zwischen dem Bedien-PC und den Dezentralen Rechnern (DZR) her und fungiert als Schnittstellenrechner, durch den der Übergang vom einkanaligen (nicht sicheren) Rechnersystem in der Zentrale auf das zweikanalige (sichere) Rechnersystem des MCDS realisiert wird. Bis zu 10 DZR können an den DKZ angeschlossen werden. Die Verbindung der sicheren Rechner untereinander erfolgt durch ein serielles, zweikanaliges Bussystem.

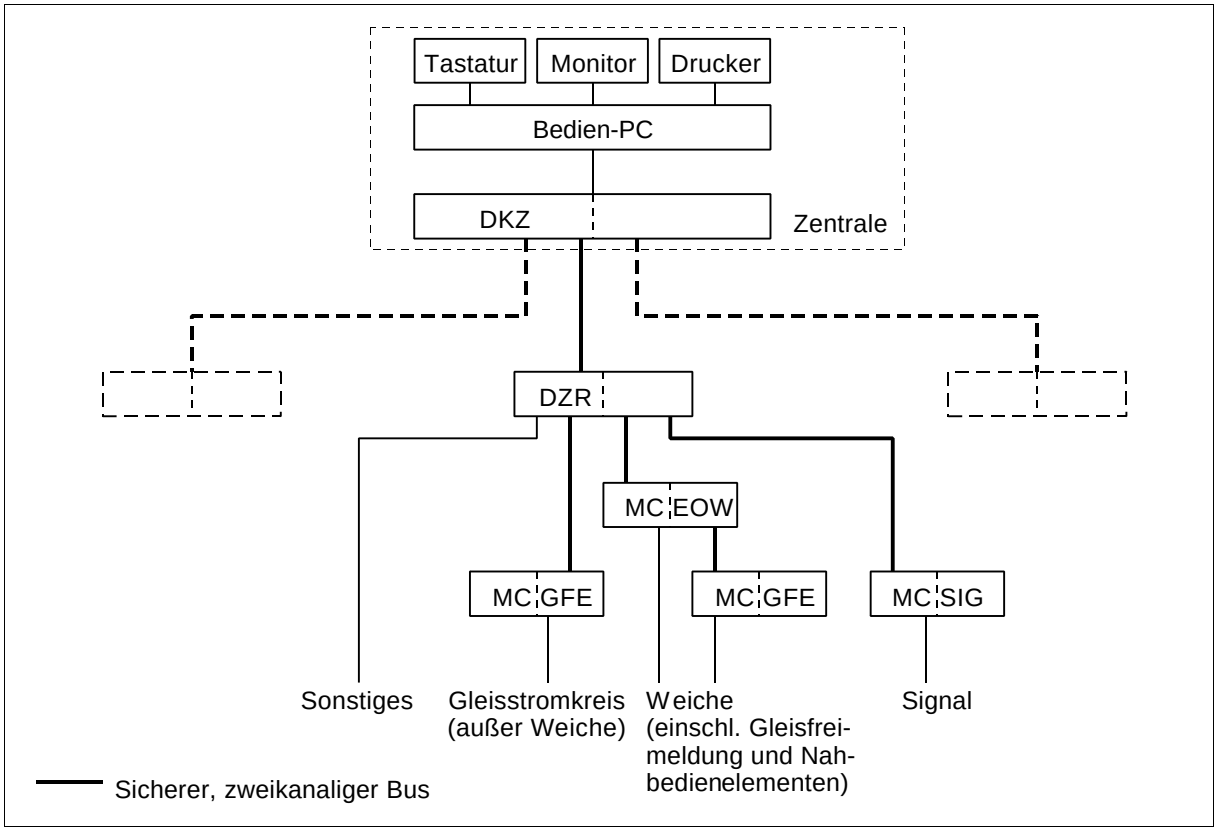


Abbildung 31: Systemstruktur des ESTW der MCDS-Technik

DZR	Dezentraler Rechner	MC GFE	Microcomputergesteuerte Gleisfreimeldeeinrichtung
DKZ	Datenkonzentrator		
MC EOW	Microcomputergesteuerte, elektrisch ortsbedienbare Weiche	MC SIG	Microcomputergesteuerte Signalsteuerung

„Ein Grundprinzip des System besteht darin, die für die technische Realisierung der Fahrwegsicherung nötigen Anlagen möglichst dezentral (in geographischer Nähe zur Gleisanlage)

anzuordnen.“[42] Die in anderen Systemen „Stellbereich“ genannten Areale werden in der MCDS-Technik als „dezentraler Bereich“ bezeichnet. Die Steuerung und Überwachung der Feldelemente eines solchen Bereichs wird von der zugehörigen Rechnereinheit, dem Dezentralen Rechner (DZR), durchgeführt. Die Aufgaben des DZR sind mit denen des BSTR aus dem El S vergleichbar. Der DZR enthält die für seinen Bereich gültige Fahrstraßenlogik und trägt die Sicherheitsverantwortung bei der Verknüpfung der Elemente.

Signale, Weichen und Gleisfreimeldeanlagen werden durch eigene, dem DZR untergeordnete Rechner gesteuert und überwacht. Das Einlesen von Kontakten (Schlüsselschalter, Schienenkontakte etc.), die nicht der direkten Weichensteuerung dienen, sowie die Kommunikation mit Block- und BÜ-Techniken werden vom DZR wahrgenommen.

Die Sicherheitsverantwortung für die Steuerung von Weichen übernimmt die Weichensteuerung MC EOW (Microcomputergesteuerte, elektrisch ortsbedienbare Weiche). Eine komplette Steuerungseinheit MC EOW kann zwei Weichen steuern und einschließlich Gleisbesetztmeldung überwachen. Die Weichen können sowohl als ortsbediente Weichen betrieben als auch über einen DZR fernbedient werden. Umschaltungen zwischen den beiden Betriebsarten sind möglich.

Für die Steuerung und Überwachung von Lichtsignalen steht die Signalsteuerung MC SIG zur Verfügung. Sie wird am Signalmast montiert oder zusammen mit den anderen Rechnern im Schalthaus untergebracht.

Die Gleisfreimeldeeinrichtung MC GFE basiert auf einem hochfrequenten Gleisstromkreis. Die Auswertung der Frei-/Besetztmeldung wird vom jeweils übergeordneten Rechner vorgenommen. Dies kann ein DZR sein oder der Rechner einer MC EOW.

8.3.3 Externe Einflußnahmemöglichkeiten

Neben der Möglichkeit, das System durch einen PC zu bedienen (in der MCDS-Technik auch „Zentralrechner“ genannt), gibt es eine ganze Reihe weiterer Möglichkeiten. Da die MCDS-Technik vor allem auf Bahnen mit einfachem Betriebsablauf zum Einsatz gelangt, können die meisten Steuerungsaufgaben durch im DZR programmierten Selbststellbetrieb realisiert werden. Somit muß die zentrale Bedienstelle nicht immer besetzt sein. Während der Anstoß zur Einstellung einer Einfahrstraße zugbewirkt erfolgen kann, ist die Anforderung einer Ausfahrstraße durch Taster in Bedienkästen möglich, die vom Triebfahrzeugführer betätigt werden [44].

Für den Rangierbetrieb können die Weichen ortsbedient oder von der stumpfen Seite mit Schienenkontakten angesteuert werden. Rangieren in Nahbedienbereichen ist ebenso möglich, wie auf gesicherten Rangierfahrstraßen.

8.3.4 Dezentralität des Systems und zukünftige Entwicklungsrichtungen

Seitens der IVV wird großer Wert auf die Eigenschaft der Dezentralität gelegt, was sich nicht nur im Namen des Systems, sondern auch in allen Publikationen widerspiegelt. Der Begriff der Dezentralität kann aber verschieden interpretiert werden. Mögliche Auslegungen sind folgende:

1. Bei Ausfall der Zentrale bleibt der dezentrale Bereich (Stellbereich) arbeitsfähig; es können weiterhin vollständig gesicherte Fahrstraßen eingestellt werden.

2. Während die Fahrstraßenlogik eines Bereiches zentral realisiert wird (DZR), werden die Peripheriерechner (MC EOW, MC SIG, MC GFE) in geografischer Nähe zu den Feldelementen angeordnet.

3. Die Fahrstraßenlogik wird nicht mehr zentral realisiert, sondern durch Kommunikation der Peripheriерechner untereinander (Spurplanprinzip).

Zur Zeit wird durch MCDS nur der erste Punkt uneingeschränkt erfüllt. Der zweiten Auslegungsmöglichkeit der Dezentralität wird meistens nicht entsprochen, da durch MCDS-Anlagen in der Regel ältere elektrische Stellwerke ersetzt werden, bei denen bereits Kabel für Stell- und Überwachungsleitungen von einer Zentrale zu den Feldelementen vorhanden sind. Um aufwendige Erdarbeiten zu vermeiden, werden die vorhandenen Kabel genutzt und somit die Peripherierechner zentral im Bahnhof angeordnet.

Die dritte Auslegungsmöglichkeit ist derzeitig noch nicht realisiert, befindet sich aber in der Entwicklung. Dabei soll ein System zur Selbstkonfiguration der Anlage entstehen, die die aufwendigen Projektierungs-, Prüf- und Abnahmeaufgaben erleichtert. *„Das Arbeitsprinzip dieses Systems beruht darauf, daß jedes Logikelement die Grundklasse seines Fahrwegelementes kennt und aus den Nachbarschaftsbeziehungen zu den Logikeinheiten eindeutig ableiten kann, in welcher Programmierart seiner Klasse es im Gleisfeld tätig werden soll.“*[43] Dieses Verfahren erinnert an das Spurplanprinzip. So, wie jedem Element im Spurplanrelaisstellwerk eine eigene Relaisgruppe und im El S ein Softwareelement zugeordnet wird, hat im selbstkonfigurierenden MCDS jedes Element seinen eigenen Rechner. Die Nachbarschaftsbeziehungen, im Spurplanrelaisstellwerk durch Spurkabel realisiert, erhält der Rechner – wie im El S – durch projektierte Daten.

Teil III:

Vergleich ausgewählter Eigenschaften der Stellwerkssysteme

1 Sicherheitskonzepte

1.1 Nachweis der Sicherheit

1.1.1 Nachweismethoden

Jedes System besitzt einen gewissen Grad an Sicherheit. Die Frage „Wie sicher ist ein System?“ ist jedoch schwer zu beantworten. Um eine Antwort darauf zu finden, können qualitative oder quantitative Methoden angewendet werden.

1.1.1.1 Quantitativer Nachweis

Die Sicherheit ist das Komplement zu eins der Gefährdungsrate, zumeist als Gefährdungswahrscheinlichkeit pro Betriebsstunde (h^{-1}) ausgedrückt. *„So soll z. B. ‚London Underground Limited‘ 1983 für das erste ESTW zur Steuerung eines Depots eine Gefährdungsrate # 10^{-7} h^{-1} gefordert haben, und heute # 10^{-9} h^{-1} fordern . Bei der Deutschen Bundesbahn waren in früheren Jahren # 10^{-11} h^{-1} im Gespräch.“*[38]

Sind die partiellen Ausfallraten der verwendeten Elemente oder Baugruppen z. B. durch langjährige Aufzeichnungen bekannt, so kann die Sicherheit eines Stellwerks tatsächlich mit ausreichender Genauigkeit berechnet werden. Die Sicherheit muß allerdings vor Inbetriebnahme nachgewiesen werden, wenn noch keine oder nur unzureichende Angaben über die verwendete Hardware vorliegen. Oft besteht dann das Ergebnis einer solchen Berechnung aus dem Produkt vieler geschätzter Parameter. Durch geringfügiges Ändern der Parameter lassen sich sehr unterschiedliche Gefährdungsraten errechnen. Vielfach wird diese Methode abgelehnt, da sich die Parameter nicht beweisen lassen [38]. Bei der Innovationsfreudigkeit der Industrie lohnt sich diese Methode heute meines Erachtens auch nicht für den Nachweis der Sicherheit im Nachhinein, da zu dem Zeitpunkt, an dem ausreichend statistisches Material zur Verfügung steht, die betreffenden Baugruppen oder -elemente längst durch neue ersetzt wurden.

1.1.1.2 Qualitativer Nachweis

Dem Mangel des quantitativen Nachweises kann durch Anwendung qualitativer Methoden begegnet werden. Dabei ist ein schriftlicher Nachweis nach verbindlichen Regelwerken (z. B. Mü 8004) anzufertigen, in dem nachgewiesen wird, daß das System alle geforderten Eigenschaften besitzt. Der Nachweis beruht dann nicht mehr auf Annahme von (geschätzten) Parametern sondern auf Annahme konkreter Fakten, wie z. B. der sicherungstechnischen Unabhängigkeit zweier Rechnerkanäle. Durch die vorgeschriebene Gliederung des Sicherheitsnachweises soll die Vollständigkeit der Betrachtungen gewährleistet werden.

1.1.2 Praktische Durchführung

Viele europäische Bahnverwaltungen (z. B. DB AG, SBB, DSB) fordern nachprüfbare Sicherheitsnachweise und prüfen diese sehr genau. Diese Vorgehensweise ist aber nicht bei allen Bahnverwaltungen üblich. Ob es für ein Stellwerk einen Sicherheitsnachweis gibt, hängt im wesentlichen davon ab, für wen es erstmals hergestellt wurde. So existieren für das El S und das El L Sicherheitsnachweise, da sie erstmals in Deutschland eingesetzt wurden. Für SSI dagegen existieren keine Sicherheitsnachweise, da BR als Hauptentwickler das System sehr genau kennt und es auf dieser Basis akzeptiert. Offensichtlich sind auch andere Kunden bereit, SSI ohne Sicherheitsnachweis einzusetzen. BR vergibt an die Herstellerfirmen ein Zertifikat darüber, daß das von diesem Hersteller gefertigte ESTW bei BR für die Steuerung von Bahnanlagen mit Personenverkehr zugelassen ist. *„Ansätze für ein solches Zertifikat-Verfahren sind sowohl in Deutschland als auch im europäischen Ausland erkennbar... Hierbei spielt möglicherweise die neue EU-Gesetzgebung zur Produzentenhaftung eine bedeutende Rolle.“*[38]

Die Produzentenhaftung als Sicherheitsgarant wird bei ESTW amerikanischen Ursprungs angewendet. Darüber hinaus bietet das VPI als einziges ESTW einen quantitativen Sicherheitsnachweis. Die Richtigkeit der Gefährdungsratenberechnungen wird in [33] bezweifelt: *„Wahrscheinlichkeits-theoretische Berechnungen der Gefährdung basieren auf Modellen, deren Gültigkeiten nicht bewiesen werden können.“*

Die Gesetzgebung zur Produzentenhaftung verpflichtet die Hersteller zu besonderer Sorgfalt, die gegebenenfalls vor Gericht nachweisbar sein muß. Dabei werden nachvollziehbare Sicherheitsnachweise das Urteil maßgeblich beeinflussen. In dem Zusammenhang ist es dann doch wieder von wesentlicher Bedeutung, in welchem Maße und wie die einschlägigen Vorschriften eingehalten wurden [38].

1.2 Systematisierung der Sicherheitskonzepte

Als **zweikanalige Strukturen** werden in diesem Teil der Arbeit alle mehrkanaligen Rechnersysteme bezeichnet, in denen mindestens zwei Kanäle bei der Ausgabe zu einem übereinstimmenden Ergebnis kommen müssen (mvn, m = 2, n $ 2). Bei allen betrachteten Systemen arbeiten maximal drei Kanäle in einem Rechnersystem. Im Rahmen der Arbeit kommen also 2v2 und 2v3-Konfigurationen für zweikanalige Rechnersysteme zum Einsatz. Der Vergleich kann durch Hardware (z. B. SIMIS) oder Software (z. B. SELMIS, SSI) erfolgen. Zumeist sind die Kanäle identisch programmiert. Eine Sonderstellung nimmt ELEKTRA ein. Hier wird auf zweikanaliger Hardware diversitäre Software eingesetzt. Außerdem erfolgt der Vergleich der Ergebnisse aus beiden Kanälen sowohl durch Software als auch durch Hardware.

Das entscheidende Merkmal **einkanaliger Systeme** ist, daß die Datenverarbeitung auch bei Nutzung anderer Redundanzen auf einem einkanaligen Rechner erfolgt. Zumeist kommt dabei

zweikanalige Software zum Einsatz (EBILOCK, WESTRACE). Eine vollständige Diversität ist dabei nicht immer gegeben! Im VPI wird auch die Software einkanalig verwendet.

1.3 Vergleich der Sicherheitskonzepte

Um die Sicherheit in den ESTW der einzelnen Hersteller objektiv zu vergleichen, wären quantitative Methoden, basierend auf seriösem Zahlenmaterial, gut geeignet. Aus mehreren Gründen kann diese Methode hier nicht angewendet werden:

- Die Berechnung ist umfangreich, sehr kompliziert und verlangt detaillierte Hardwarekenntnisse.
- Es liegen keine Zahlenangaben vor.
- Wie bereits erläutert, würden viele Zahlen auf Schätzungen beruhen.

Aus den genannten Gründen werden die folgenden Vergleiche auf qualitativer Basis erfolgen. Dabei wird davon ausgegangen, daß auf einen erkannten, zufälligen Fehler hinreichend schnell reagiert wird, die Fehlerreaktionszeit also im Verhältnis zur Fehleroffenbarungszeit vernachlässigt werden kann.

Systematische Fehler sollen nicht betrachtet werden, da diese von der angewendeten Sorgfalt bei Entwicklung, Produktion, Projektierung und Montage abhängig sind. Dazu können keine Angaben gemacht werden, weil dafür ein umfangreiches Studium der Entwicklungs- und Produktionsbedingungen der einzelnen ESTW notwendig wäre.

1.3.1 Gegenüberstellung ein- und zweikanaliger Hardwarestrukturen

1.3.1.1 Behandlung zufälliger Einfachfehler

In einkanaligen Hardwarestrukturen kann auch bei Nutzung von Softwareredundanz die Ungefährlichkeit eines zufälligen Einfachfehlers nicht nachgewiesen werden, da die Zahl der möglichen Ausfälle unüberschaubar ist [41]. Somit können solche Systeme einem qualitativen Sicherheitsnachweis nach Mü 8004 nicht standhalten. Nach [6] ist nicht beweisbar, daß ein einkanaliger Rechner nicht so ausfallen kann, daß er trotzdem die externe Zusatzhardware (z. B. OPCR einschließlich dessen Ansteuerung bei WESTRACE) mit den richtigen Signalen zur Aufrechterhaltung der Funktion versorgt.

Bei einer konsequent zweikanaligen Hardwarestruktur ist ein zufälliger Einfachfehler garantiert ungefährlich. Wichtig dabei ist, daß die beiden Kanäle sicherungstechnisch unabhängig voneinander arbeiten. Die Effektivität des Prüfprogramms spielt für den Schutz gegen den Einfachfehler keine Rolle. Dagegen müssen Prüfprogramme in einkanaligen Systemen sehr viel umfangreicher sein, da keine automatische und vor allem unabhängige Fehleroffenbarung durch einen Vergleich in einem anderen Rechnerkanal (Softwarevergleich) oder in einer Zusatzhardware (Hardwarever-

gleich) stattfindet. Eine vollständige Prüfung selbst eines einfachen Prozessors ist aufgrund seiner Komplexität ausgeschlossen [6].

1.3.1.2 Behandlung zufälliger Mehrfachfehler

Kritisch sind einkanalige Systeme erst recht bei Annahme von zufälligen Mehrfachfehlern. Tritt ein Fehler im Rechner auf, findet kein Vergleich von Rechenergebnissen mehr statt, und unkontrollierte Ausgaben können die Folge sein. Bei Annahme eines weiteren, noch nicht offenbarten Fehlers in der Abschalt-Hardware kann keine Sicherheitsabschaltung erfolgen.

Zufälligen Mehrfachfehlern wird durch die hinreichend schnelle Offenbarung des ersten Fehlers begegnet. In zweikanaligen Systemen wird der erste Fehler meist durch den Vergleich der Ergebnisse beider Kanäle offenbart. Nur durch diesen Vergleich nicht erkennbare Fehler (verdeckte Fehler) müssen durch ein Prüfprogramm offenbart werden. Dagegen spielen Prüfprogramme in einkanaligen Systemen eine wesentlich größere Rolle, da wegen der nicht gegebenen Unabhängigkeit der Softwarekanäle nicht davon ausgegangen werden kann, daß der erste Fehler durch einen prozessorinternen Vergleich entdeckt wird. Eine hinreichend kurze Fehleroffenbarungszeit des ersten Fehlers müßte schon durch ein Prüfprogramm sichergestellt werden!

1.3.1.3 Praktische Bedeutung von einkanaligen Hardwarestrukturen

Trotz der sicherheitstechnischen Unterlegenheit einkanaliger Systeme werden sie von vielen Bahnverwaltungen eingesetzt. Dabei wird seitens der Anwender wesentlich größeres Augenmerk auf die Verfügbarkeit der Systeme gelegt, da die meisten Unfälle auf Eingriffe des Menschen bei Ausfall des Systems zurückzuführen sind.

1.3.2 Gegenüberstellung von Hard- und Softwarevergleichern

Der Vergleich der in zwei Rechnerkanälen ermittelten Ergebnisse findet bei Einsatz eines Hardwarevergleichers in einer Zusatzhardware, also außerhalb des Rechners statt. Erfolgt der Vergleich durch Software (z. B. SELMIS, Abbildung 8), werden die Ergebnisse in den jeweils anderen Rechner übertragen und mit dessen Ergebnis verglichen. Tritt dabei in einem Kanal ein Fehler auf, so kann nicht mehr davon ausgegangen werden, daß der Vergleich in diesem Kanal noch ordnungsgemäß durchgeführt wird. Hier muß die Diskrepanz der Ergebnisse durch den anderen Rechner offenbart werden.

Bei Einsatz eines Hardwarevergleichers pro Kanal (z. B. SIMIS, Abbildung 4) werden trotz eines fehlerhaften Rechnerkerns noch zwei unabhängige Vergleiche durchgeführt. Das gewährleistet zweifellos eine höhere Sicherheit im Rechnersystem; notwendig ist diese aber selbst nach den strengen deutschen Vorschriften nicht.

Vorteile von Hardwarevergleichern im SIMIS-System sind, daß die Verarbeitungsergebnisse ohne Belastung der Rechnerleistung verglichen werden und der Vergleich automatisch erfolgt; eine

Koordination der Rechner ist nicht erforderlich, da sie taktsynchron betrieben werden. Deshalb verhält sich ein solcher Rechner wie ein einkanaliger.

Ein Softwarevergleich dagegen erfordert, daß Rechnerleistung für den Vergleich bereitgestellt wird und bei der Programmierung entsprechende Synchronisationsstellen zur Rechnerkoordinierung für den Vergleich der Verarbeitungsergebnisse berücksichtigt werden. Problematisch kann die programmgesteuerte Koordination dann werden, wenn in sehr kurzer Zeit auf anstehende Prozeßanforderungen reagiert werden muß [6].

Nachteilig bei einem Hardwarevergleich wirkt sich aus, daß dafür eine gesonderte Hardware bereitgestellt werden muß, die darüber hinaus an jede neue Rechnergeneration angepaßt werden muß. SIEMENS argumentiert dazu: *„Der Hardwarevergleich erfordert nur sehr wenig Aufwand (2 ICs) und ist z. B. im SIMIS-C deshalb mit in die Prozessorkarte integriert. Eine gesonderte Baugruppe, allein für die Überwachung, ist bei Anwendung moderner Technologie nicht erforderlich.*“[6]

Vielfach ist es Ansicht der Entwickler, ob Hard- oder Softwarevergleicher eingesetzt werden. Der Einsatz eines Hardwarevergleichers scheint nur dann sinnvoll, wenn Rechner aus eigener Entwicklung zum Einsatz gelangen, da dann der zusätzliche Aufwand für den Vergleicher gering ausfällt. Kosten- und andere Analysen, die eine Entscheidung über den Einsatz von Hard- oder Softwarevergleichern herbeiführen sollen, sind aber hauptsächlich nur im Vorfeld der Entwicklung eines ESTW von Bedeutung, da eine einmal gewählte Philosophie nahezu unumstößlich ist.

2 Logikmodelle

Beim Bilden von Fahrstraßen wird in den ESTW nach drei verschiedenen Logikmodellen verfahren. Jedes dieser Modelle kann seine Vorzüge bei bestimmten Stellwerksgrößen ausspielen.

2.1 Verknüpfung durch Boolsche Gleichungen

Die Verknüpfung der Elemente in Boolschen Gleichungen ist das einfachste Logikmodell. Dabei werden alle Elemente durch jeweils eine Variable repräsentiert, der ein logischer Wert (true/false) zugewiesen wird. Eine zur Verdeutlichung hier stark vereinfachte Gleichung kann folgendermaßen lauten:

$$S = X \cdot G1 \cdot G3 \cdot /W1$$

In Worten ausgedrückt bedeutet diese Gleichung folgendes:

Das Signal S zeigt Fahrt (S = true), wenn das Bedienungsereignis X eintritt (X = true), die Gleisabschnitte G1 und G3 frei sind (G1 = G3 = true), und sich die Weiche W1 in Minusstellung befindet (W1 = false).

Dieses Verfahren zeigt Ähnlichkeit mit dem Verschlußplanprinzip, in dem der Zustand der Elemente für jede Fahrstraße bei der Projektierung festgelegt wird. Eine Verschlußtabelle besitzt jedoch eine weitaus höhere Transparenz. Auch Änderungen der anlagenspezifischen Daten lassen sich nur mit großem Aufwand in die Gleichungen einarbeiten. Vorteile zeigt das Modell bei der Anpassung an bahnverwaltungsspezifische Bedingungen, da diese allein durch die Boolschen Gleichungen beschrieben werden. Darüber hinaus sind die Gleichungen der bisherigen (Klasse I-) Relaislogik entnommen und so für den damit vertrauten Signalingenieur leicht nachvollziehbar. Aufgrund der oben genannten Nachteile eignet sich das Verfahren nur für kleine bis maximal mittelgroße Anlagen.

2.2 Verschlußplanprinzip

Wird für das Bilden von Fahrstraßen das Verschlußplanprinzip angewendet, so werden die einzelnen Elemente über eine Tabelle (Verschlußtabelle, Verschlußplan oder Verschlußtafel genannt) mit den Fahrstraßen verknüpft. Die Übersichtlichkeit, die eine solche Tabelle in gedruckter Form bietet, geht jedoch bei großen Bahnhöfen und dementsprechend großen Tabellen verloren. Wenn die Projektierung rechnergestützt erfolgt, ist das Problem der Komplexität beherrschbar. Das Projektierungssystem für das El L beispielsweise generiert zunächst gemäß dem Elementverbindungsplan alle Fahrstraßen, die nach der Gleislage möglich sind. Da allerdings nur die von der Bahnverwaltung geforderten Fahrstraßen implementiert sein dürfen, müssen anschließend alle nicht gewünschten Fahrstraßen aus der Tabelle entfernt werden. Bei großen Bahnhöfen kann die Anzahl der Fahrtmöglichkeiten mehr als doppelt so hoch sein wie die Anzahl der geforderten Fahrstraßen [3].

Vorteile bietet das Verschlußplanprinzip bei der Anpassung der Logik an bahnverwaltungsspezifische Bedingungen, da diese durch die Eintragungen in der Verschlußtabelle realisiert werden können. Die Eigenschaften des Verschlußplanprinzips können am besten bei Anlagen kleiner und mittlerer Größe ausgenutzt werden.

2.3 Spurplanprinzip

Viele Vorteile, die die Anwendung des Spurplanprinzips in Relaisstellwerken mit sich bringt, wie beispielsweise Standardisierung und einfache Montage der Relaisgruppen, sind in elektronischen Stellwerken nicht mehr relevant. Trotzdem wird dieses Logikmodell auch in elektronischen Stellwerken genutzt.

Das im El S angewandte Spurplanprinzip besitzt allerdings einen bedeutenden Unterschied zum Prinzip im Spurplanrelaisstellwerk: Die Spursuche, die im Relaisstellwerk mit Such- und Echostrom erfolgte, ist hier nicht mehr notwendig. Neben dem Elementverbindungsplan werden die von der Bahnverwaltung geforderten Fahrstraßen einschließlich ihres Weges durch die Elemente als projektierte Daten im Speicher der Rechner abgelegt. Bei Aktivierung einer Fahrstraße laufen zwar verschiedenartige Telegramme von Element zu Element, wie die Ströme durch die Spuradern in Spurplanrelaisstellwerken, der Weg der Telegramme ist jedoch von vornherein festgelegt [3]. Die aktivierten Elemente arbeiten nun ihre Algorithmen ab und senden ihre, für die weitere Bearbeitung der Fahrstraße relevanten Meldungen durch Telegramme an ihre Nachbarelemente. Jede dabei auftretende Telegrammart ist mit einer Spurader im Spurplanrelaisstellwerk zu vergleichen.

Wenig Flexibilität zeigt dieses Logikmodell bei der Implementation von spezifischen Bedingungen der Anwender. Auch die Einarbeitung zusätzlicher Funktionen in bestehende, bahnverwaltungsspezifische Software ist mit hohem Aufwand verbunden. Hierzu werden Softwarespezialisten benötigt, die die speziellen Anforderungen in den Algorithmus zur Abarbeitung der Spurplanlogik einarbeiten. Somit ist zunächst ein hoher Aufwand notwendig, um die Betriebslogik einer Bahnverwaltung softwaremäßig zu beschreiben. Ist dieser Schritt erst einmal getan, so zahlt sich die Arbeit durch eine leichte Änderbarkeit der projektierten Daten aus. Auch komplizierte Funktionen wie z. B. Ersatzschutzsuche, sind mittels Spurplanlogik zu realisieren. Besonders geeignet ist die Spurplanlogik zur Sicherung umfangreicher Bahnanlagen, für deren Steuerung eine hohe Funktionalität gefordert wird.

3 Einordnung der ESTW nach Komplexität

Die behandelten ESTW lassen sich in drei Kategorien einteilen, die im wesentlichen von der Größe der zu steuernden Bahnanlagen und der Sicherungsphilosophie der jeweiligen Anwender abhängen. Jedes ESTW ist für eine bestimmte Kategorie prädestiniert, was jedoch nicht bedeutet, daß es außerhalb dieser nicht eingesetzt wird. Für jeden der drei Einsatzzwecke sind bestimmte Merkmale prägend, die ein ESTW jedoch nicht immer vollständig erfüllt. Eine scharfe Abgrenzung ist daher nicht möglich.

3.1 Hohe Komplexität

Das dichte mitteleuropäische Eisenbahnnetz mit seinen komplexen Knotenbahnhöfen verlangt nach ESTW, die einerseits in der Lage sind, große Bahnhöfe zu steuern, und andererseits die hohen Anforderungen nach Funktionalität erfüllen. An solche Stellwerke werden höchste Sicherheitsanforderungen gestellt, die sich beispielsweise auf dem Gebiet der BRD in der Mü 8004 niederschlagen. Um die geforderte Sicherheit zu erreichen, ist der Einsatz zweikanaliger Hardwarestrukturen unumgänglich. Umfangreiche und gesicherte Hilfsbedienungen sowie eine gesicherte Zustandsanzeige der Außenanlage für den Bediener gehören zum Standardumfang dieser ESTW. Bahnverwaltungen, die solche Anforderungen stellen, sind u. a. DB AG, SBB und ÖBB. Das El S, das El L und das ESTW ELEKTRA sind den hohen Ansprüchen gewachsen. Je nach Hersteller kommt dabei Spurplan- oder Verschlußplanlogik zum Einsatz.

3.2 Mittlere Komplexität

Typische Anwendungsgebiete dieser ESTW sind Fernbahnen der SNCF, BR, FS und RENFE sowie Stadtbahnen. Die funktionellen Anforderungen sind nicht so hoch wie bei der vorangegangenen Kategorie, dennoch müssen sich mittelgroße Anlagen mit den eingesetzten ESTW realisieren lassen. Obwohl an die Sicherheit in der Informationsverarbeitung, bei der meist eine zweikanalige Hardwarestruktur zum Einsatz gelangt, hohe Anforderungen gestellt werden, bleiben diese auf die Stellwerksfunktionen beschränkt. Bedienung und Anzeige unterliegen zumeist keiner Sicherheitsrelevanz; auch Hilfsbedienungen sind nicht üblich. SSI, EBILOCK, SICAS und MCDS sind typische Vertreter dieser Gattung. Als Logikmodell wird meistens die Verschlußplanlogik angewendet.

3.3 Geringe Komplexität

Im Gegensatz zum teilweise sehr dichten europäischen Eisenbahnnetz zeigen die außereuropäischen Netze eine wesentlich geringere Vermaschung und die Bahnhöfe eine weitaus geringere Komplexität. Auch viele Industrie- und einfache Stadtbahnen stellen nicht so hohe Ansprüche, wie es bei stark belasteten Fernbahnen der Fall ist. Da in den ESTW für diese Einsatzzwecke vornehmlich einkanalige Hardware genutzt wird, kann das Sicherheitsniveau von vornherein als geringer eingestuft werden. Sicherheit in Bedienung und Anzeige wird nicht gefordert. Eine Verknü-

pfung der Elemente durch Boolsche Gleichungen ist üblich und durch die meist bestehende Einfachheit der Bahnanlagen möglich. Typische Vertreter sind WESTRACE und VPI sowie das in dieser Arbeit nicht behandelte Microlock, das dem VPI sehr stark ähnelt und ebenfalls amerikanischen Ursprungs ist.

Schlußbetrachtungen

Die vorliegende Arbeit dient dem Zweck, einen Überblick über die derzeit international eingesetzten ESTW zu geben. Dieser Aufgabenstellung ist im zweiten Teil entsprochen worden. Dabei erfolgte die Beschreibung aufgrund der zugänglichen Literatur. Die durchaus vorhandenen Lücken zu schließen und in die ESTW tiefer einzudringen, kann Aufgabe weiterer Studien- oder Diplomarbeiten sein. Dazu scheint es angebracht, die Signalbaufirmen und deren im Einsatz befindliche ESTW zu besuchen und diese vor Ort, im Gespräch mit den Spezialisten zu analysieren. Die Bearbeitung dieser Aufgabe könnte beispielsweise im Rahmen eines Praxissemesters o. ä. erfolgen; ein Auslandsaufenthalt wird dabei meist erforderlich sein. Außerdem können die Sicherungsphilosophien der Anwender, die bahnverwaltungsspezifischen Bedingungen, vor Ort besser studiert werden.

Die im dritten Teil angestellten, vergleichenden Betrachtungen dienen dem Zweck, das im zweiten Teil gezeichnete Bild der ESTW abzurunden und die Systeme einordnen zu können. Hierbei wurden ausgewählte Eigenschaften verglichen; es kann ebenfalls Aufgabe weiterer Arbeiten sein, diese Betrachtungen zu vertiefen und weitere anzustellen. Beispielsweise könnte dabei untersucht werden, wie sich die Stellwerkssysteme in die Sicherheitsstufen „Safety Integrity Level“ (SIL) nach CENELEC-Norm 50126 ff einordnen lassen.

Die wichtigste Erkenntnis der vorliegenden Arbeit ist die Tatsache, daß elektronische Eisenbahnsicherungstechnik durchaus auf anderen Wegen als den in Deutschland beschrittenen – wenn auch auf unterschiedlichem Niveau – realisierbar ist. Einkanalige Hardwarestrukturen ohne Sicherheitsnachweis, fehlende Sicherheit in Bedienung und Anzeige – auf mitteleuropäischen Hauptbahnen undenkbar, in anderen Teilen der Welt alltäglich. Es bleibt abzuwarten, ob und inwiefern die europäische Harmonisierung mit einer Abrüstung des historisch gewachsenen hohen deutschen Sicherheitsniveaus einhergehen. Eine bedeutende Rolle wird dabei das EBA spielen, das als staatlich autorisierte Aufsichtsbehörde der deutschen Eisenbahnen über die Höhe der Sicherheitsanforderungen zu befinden hat. Darüber hinaus bringt die Privatisierung der Eisenbahnen ein verstärktes Kostendenken mit sich, welches auch vor der in Fragestellung des derzeitigen Sicherheitsniveaus nicht haltmachen wird.

Ein Zuviel an Sicherheit schließt zwar gefährliches Versagen der Technik nahezu aus, auch schränken hochverfügbare Systeme den gefährlichen Eingriff des Menschen ein, doch Sicherheit muß bezahlbar bleiben, und bezahlbare Sicherungstechnik bedeutet konkurrenzfähige Bahnen.

Anhang

I Zusammenstellung der wichtigsten Eigenschaften aller ausführlich behandelten ESTW

Name	**El S**	**El L (L90)**	**ELEKTRA**	**EBILOCK**	**SSI**	**WESTRACE**	**VPI**
Hersteller	SIEMENS	SEL	Alcatel Austria	ABB (ADTRANZ)	Westinghouse, GEC ALSTHOM	Westinghouse	GRS
1. Allgemeines							
Standards	VDE/DIN, IEC, Herstellerintern		UIC, Hersteller-intern	UIC	BS	BR, AAR	AAR
Gewährleistung der Sicherheit	qualitativer Sicher-heitsnachweis (Mü 8004)	qualitativer Sicher-heitsnachweis (Mü 8004)	qualitativer Sicher-heitsnachweis ÖBB	Vorschriften der SJ	Zertifikat von BR	k. A.	quantitativer Si-cherheitsnachweis
Entwicklungsinitia-tive durch	Hersteller	Hersteller	Hersteller und Kunden	Hersteller und Kunden	Kunden (BR)	Hersteller und Weltmarkt	Hersteller
Qualitätsanforde-rungen	DIN ISO 9001-9003	DIN ISO 9001-9003	k. A.	DIN ISO 9001-9003 BS 5750	BS 5750	BS 5750	k. A.
Komplexität	hoch	hoch	hoch	mittel	mittel	gering	gering
Einsatzländer (Aus-wahl)	Deutschland, Schweiz, Öster-reich, Niederlande, Finnland	Deutschland, Spa-nien	Österreich, Schweiz, Ungarn	Schweden, Finn-land, Dänemark, Bulgarien	Großbritannien, USA , Spanien, Australien	Großbritannien, Spanien, Australien	USA, Niederlande, Spanien, Italien, Asien, Australien

2. Hardware 2.1 Allgemeines							
Stellentfernung (max. Länge der leistungsführenden Kabeladern)	6,5 km	6,5 km	6,5 km	< 1km*	0,7 km	0,7 km	k. A.
Aufstellung des Peripherierechners in der Außenanlage	nein	nein	nein	ja	ja	möglich	keine örtliche Trennung von Zentral- und Peripherierechner
Einsatz des Zentralrechners in nicht klimatisierter Umgebung	nein	nein	nein*	ja	ja	ja	ja
2.2 Bedienrechner							
Name	BAR 16	Melde- und Eingabemodul	Video Control Computer	Bestandteil des Zentralrechners	Panel Processor Module	Bestandteil des Zentralrechners	Code System Emulator
Sicher durch	2v3 mit Hardwarevergleich	2v3 mit Softwarevergleich	Safety-Bag-Verfahren		nicht sicher		nicht sicher
Konfiguration	2v3	2v3	2v2		1v2		1v1
Baugruppensystem	eigen	kommerziell	eigen		eigen		eigen
CPU-Typ	80486	Firma Digital	80286/80486		M 6802		k. A.
2.3 Zentralrechner							
Name	EKIR	Sicherungsmodul	Central Control Computer	Zentraler Sicherheitsbaustein	Interlocking Multiprocessor Module	VLM-Baugruppe	CPU/PD-Baugruppe
Konfiguration	2×(2v2)	2v3	2v3	1v2	2v3	1v1	1v1

Sicher durch	2v2 mit Hardware-vergleich	2v3 mit Software-vergleich	Safety-Bag-Verfahren	Zweikanalige Software	2v3 mit Software-vergleich	Zweikanalige Software	Prüfprogramm
Baugruppen	eigen	kommerziell	eigen	eigen und kommerziell	eigen	eigen	eigen
CPU-Typ	8085	Firma Digital	80268/80486	M 68030 (EBILOCK 950)	M 6802	8086/8088	k. A.
2.4 Peripherierechner							
Name	BSTR	Elementansteuermodul	Peripheral Control Computer	Objektsteuergerät	Trackside Functional Module	VPIM/VROM/ VLOM	diverse Baugruppen
Sicher durch	2v2 mit Hardware-vergleich	2v3 mit Software-vergleich	2v2 mit Hardware-vergleich	Zweikanalige Software	2v2 mit Software-vergleich	Zweikanalige Software	Prüfprogramm
Konfiguration	2×(2v2)	2v3	1v2	1v1	2v2	1v1	1v1
Baugruppen	eigen	kommerziell	eigen	eigen	eigen	eigen	eigen
CPU-Typ	8085	Firma Digital	8085	8085	M 6802	k. A.	k. A.
2.5 Interne Kommunikation							
Konfiguration	1v2	1v2	1v2, 2v2	1v2 durch Schleife	1v2	1v1	1v1
Struktur	Stern	Punkt-Punkt	Stern, Punkt-Punkt	Schleife	Linie	Stern	k. A.
Format	parallel	seriell	seriell	seriell	seriell	seriell	k. A.
Übertragungsprotokoll	spezial	standard	standard	standard	spezial	spezial	spezial

3. Software							
Fahrstraßenlogik	Spurplan	Verschlußplan	Verschlußplan	Verschlußplan	Verschlußplan	Boolsche Gleichungen	Boolsche Gleichungen
Aufwand für Bahnhofsänderung	klein	klein-mittel	mittel*	mittel*	mittel*	groß	groß
Aufwand für Anpassung an andere Bahnverwaltung	groß	mittel-groß	mittel-groß*	klein-mittel*	klein-mittel*	klein	klein
Sicher durch	Fehlerfreiheit	Fehlerfreiheit	Diversität	Diversität	Fehlerfreiheit	Diversität	Prüfprogramm
4. Bedienung und Anzeige							
Sichere Eingabegeräte	KF-Taste	KF-Taste	Ausführungstaste (KF-Taste)	Keine	Keine	Keine	Keine
Weitere Eingabegeräte	Keyboard, Tablett	Keyboard, Tablett	Keyboard, Maus	Keyboard	Keyboard, Stelltisch, Trackball	Keyboard, Stelltisch	Keyboard, Stelltisch
Sichere Ausgabegeräte	Monitor, Meldetafel, Videoprojektion	Monitor, Meldetafel, Videoprojektion	Monitor	Keine	Keine	Keine	Keine
Weitere Ausgabegeräte	Monitor, Drucker, Videoprojektion	Monitor, Drucker, Videoprojektion	Monitor	Monitor, Meldetafel, Videoprojektion	Monitor, Meldetafel	Monitor, Meldetafel, Videoprojektion*	Monitor, Meldetafel, Videoprojektion*

* Angaben nach eigener Einschätzung

k. A. Keine Angaben verfügbar

II Systematisierung der ESTW nach Komplexität

Komplexität	gering	mittel	hoch
Anforderungen an Funktionalität (bezogen auf das Spektrum der ESTW)	gering	mittel	hoch
Mögliche Größe der zu steuernden Anlagen mit einem ESTW	klein	mittel	groß
Sicherheitsanforderungen (bezogen auf das Spektrum der ESTW)	gering	mittel	sehr hoch
Sicherheit entspricht Anforderungsklasse nach DIN 19250	# 6*	6* und 7	7
Hardwarestruktur zur Gewährleistung der Sicherheit	einkanalig	ein- und zwei-kanalig	zweikanalig
Gesicherte Hilfsbedienungen	nicht möglich	teilweise mög-lich	möglich
Verwendete Logikmodelle	Boolsche Glei-chungen	Verschlußplan	Verschlußplan, Spurplan
Typische Vertreter (Auswahl)	WESTRACE, VPI	SSI, EBILOCK, SICAS, MCDS	El S, El L, ELEK-TRA
Anwender in Deutschland	keine*	Industrie-, Stadt-, Straßen- und NE-Bahnen	DB AG, Industrie- und Stadtbahnen
Anwender außerhalb Deutschlands (Auswahl)	NS, Stadtbahnen, außereuropäische Fernbahnen	SNCF, SNCB, SJ BR, FS, RENFE, DSB, Stadtbahnen	ÖBB, SBB, NS, VR, RENFE, CFL

* Angaben nach eigener Einschätzung

III Abkürzungsverzeichnis

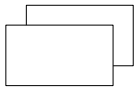
AAR	Association of American Railways
ABB	Asea Brown Boveri
ADTRANZ	ABB und Daimler bieten Transporttechnik von A bis Z
AK	Anforderungsklasse
ANSR	Anzeige- und Schnittstellenrechner
ARS	Automatic Route Setting
ATC	Automatic Train Control
ATP	Automatic Train Protection
AWS	Automatic Warning System
BAnpR	Bedien-Anpaßrechner
BAR 16	Bedien- und Anzeigerechner (16 Bit)
BERÜ	Bereichsübersicht
BFS	Betriebsführungssystem
BIS	Betriebsinformationssystem
BLT	Betriebsleitbus
BM	Bildschirmmodul
BOS	Betriebsoperationssystem
BPR	Bedienplatzrechner
BPS	Bedienplatzsystem
BR	British Railways (Britische Eisenbahnen)
BS	British Standards
BSTR	Bereichsstellrechner
BT	Bedientablett
BÜ	Bahnübergang
BUREP	Busanschlußbaugruppe für Rechner (parallel)
BUVER	Bus-Verstärkerbaugruppe
BZ	Betriebszentrale
BZA	Bundesbahnzentralamt
CAA	Computer Aided Assembly
CC	Central Control Computer
CENELEC	Comite Europeen De Normalisation Electrotechnique
CFL	Chemins de Fer Luxembourg (Luxemburgische Eisenbahnen)
COM-Server	Kommunikations-Server
CPU	Central Processing Unit
CSS	Configuration Sub System
DAG	Datenanschlußgerät
DB AG	Deutsche Bahn AG
DB	Deutsche Bundesbahn
DET	Dateneingabetastatur
DGP	Diagnostic Processor
Diag MPM	Diagnostic Multi-Processor Module
DIN	Deutsche Industrie Norm
DLM	Data Link Module
DMC	Disposition Management Computer
DOS	Disk Operating System
DSB	Danske Statsbaner (Dänische Staatsbahn)
DSTT	Dezentrales Stellteil
EAM	Elementansteuer-Modul
EBA	Eisenbahnbundesamt

EBO	Eisenbahn-Bau- und Betriebsordnung (Deutschland)
EBO	Einheitliche Bedienoberfläche (ÖBB)
EKIR	Eingabe- Kontroll- und Interpretationsrechner
El S	Elektronisches Stellwerk Bauart Siemens
El L	Elektronisches Stellwerk Bauart Lorenz (SEL)
EPROM	Erasable Programmable Read-Only Memory
ESTT	Elektronisches Stellteil
ESTW	Elektronisches Stellwerk
ESU	Element-Steuerung und -Überwachung
EVP	Elementverbindungsplan
FS	Ferrovie dello Stato Italiane (Italienische Staatsbahnen)
FSC	Fail-Safe Comparator
FSM	Fail-Safe Microprocessor
GRS	General Railway Signal
I/L MPM	Interlocking Multi-Processor Module
I/O	Input/Output
IC	Integrated Circuit
IEC	International Electrotechnical Comission
IECC	Integrated Electronic Control Centre
ILP	Interlocking Processor
ISO	International Organization for Standardization
JR	Japanese Railways (Japanische Eisenbahnen)
KA	Kontrollanzeige
KF	Kommando-Freigabe
Ks	Kombinationssignal
LAN	Local Area Network
LCD	Liquid Crystal Display
LDT	Long Distance Terminal
LWL	Lichtwellenleiter
LZB	Linienförmige Zugbeeinflussung
LZB-Kop	LZB-Koppelbaustein
MEM	Melde- und Eingabe-Modul
METARE	Meldetafelrechner
MVR	Majority Voting Restorer
NE-Bahn	Nicht bundeseigene Eisenbahn
NS	Nederlandsche Spoorwegen (Niederländische Eisenbahnen)
NVC	Non-Vital Serial Link
ÖBB	Österreichische Bundesbahn
OHR2	Overheadrechner 2
OPCR	Output Power Control Relay
OSG	Objektsteuergerät
PC	Peripheral Control Computer (nur in Verbindung mit -A oder -B und nur im System ELEKTRA)
PC	Personalcomputer
PD	Polynominal Devider
PPM	Panel Processor Module
PSD	Protokoll- und Störungsdrucker
RAM	Random Access Memory
RENFE	Red National de los ferrocariles Espanoles (Nationales Netz der Eisenbahnen Spaniens)
ResR	Reserverechner
ROM	Read-Only Memory

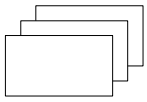
RR	Referenzrechner
RSTW	Relaisstellwerk
RZÜ	Rechnergestützte Zugüberwachung
SBB	Schweizerische Bundesbahn
SBP	Safety Bag Processor
SD	Störungsdrucker
SDS	Signalman’s Display System
SEL	Standard Elektrik Lorenz
SICAS	SIEMENS Computer Aided Signalling
SIDOS	Sichtgeräte-Doppelsteuerung
SIL	SIEMENS Interlocking Language
SIMIS	Sicheres Microcomputersystem von SIEMENS (ab 1983)
SIMIS	Sicheres Microcomputersystem (bis 1983)
SJ	Statens Järnvägar (Schwedische Staatsbahn)
SM	Sicherungsmodul
SMILE	Safe Multiprocessor for Interlocking Equipment
SNCB	Société Nationale des Chemins de Fer Belges (Nationale Gesellschaft der belgischen Eisenbahnen)
SNCF	Société Nationale des Chemins de Fer Francais (Nationale Gesellschaft der französischen Eisenbahnen)
SOPP	SIMIS Online Prüfprogramm
SPC	Serial Peripheral Controller
SSI	Solid State Interlocking
TFM	Trackside Functional Module
UIC	Union internationale des chemins de fer (Internationaler Eisenbahnverband)
VC	Video Control Computer
VDE	Verein Deutscher Elektrotechniker
VLM	Vital Logic Module
VLOM	Vital Lamp Output Module
VOTRICS	Voting Triple Modular Redundant Computing System
VPI	Vital Processor Interlocking
VPIM	Vital Parallel Input Module
VR	Valtionrautatiet (Finnische Staatsbahnen)
VROM	Vital Parallel Output Module
WESTRACE	Westinghouse Train Radio and Advanced Control Equipment
WSSB	Werk für Signal- und Sicherungstechnik Berlin
ZEBER	Zentrale Bus-Erweiterungsbaugruppe
ZEBUS	Zentrale Bus-Steuerbaugruppe
ZL	Zuglenkung
ZN	Zugnummernmeldung

IV Symbolverzeichnis

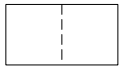
Die nachstehend aufgeführten Symbole gelten für die Konfigurationen von Baugruppen (auch Rechner) in den Abbildungen der Systemstrukturen und nur, sofern nichts anderes angegeben ist.



1v2



2v3



2v2

V Quellenangaben

[1] *o.V.:* Sicherheit für die Bahnen – Das elektronische Stellwerk.
Firmendruckschrift SIEMENS AG, Bereich Verkehrstechnik, Bestell-Nr. A19100-V100-B412-V1

[2] *Kipping, H.; Günther, C.; Kaiser, C.:* Elektronische Stellwerkstechnik.
Ingenieurarbeit, SIEMENS AG, Bereich Verkehrstechnik, Braunschweig, 1991

[3] Mündliche Aussagen von Dipl.-Ing. H.-J. Petersen, SIEMENS AG, Bereich Verkehrstechnik, Braunschweig

[4] *Schnieder, E.:* Elektronische Stellwerke als Automatisierungskomponenten bei Bahnen.
Studie, 1992, S. 10

[5] *Schnieder, E.:* Elektronische Stellwerke als Automatisierungskomponenten bei Bahnen.
Kurzfassung der Studie, 1993, S. 4

[6] *o.V.:* SIMIS im Vergleich.
Siemens-Schulungsunterlage der Schule für Verkehrstechnik, Braunschweig, 1994

[7] *Forstreuter, H.; Weitner von Pein, A.:* Verfahrensgesicherte Meldebildanzeige für den Fdl-Arbeitsplatz bei der Deutschen Bahn AG.
SIGNAL+DRAHT, 86 (1994), Heft 10, S. 320 – 324

[8] *Wehner, L.:* Das ESTW der Bauform SEL.
SIGNAL+DRAHT, 76 (1984), Heft 5, S. 83 – 88

[9] *Krehle, H.-J.:* Das elektronische Stellwerk der Bauform SEL-einschließlich Erfahrungen in Magstadt und Neufahrn.
SIGNAL+DRAHT, 79 (1987), Heft 10, S. 217 – 222

[10] *Krehle, H.-J.:* Stand der ESTW L90-Technik und Ausblick.
SIGNAL+DRAHT, 84 (1992), Heft 9, S. 254 – 259

[11] *Kehrer, J.:* Elektronische Element-Steuerung und -Überwachung im Elektronischen Stellwerk ESTW L90.
Eisenbahntechnische Rundschau, 39 (1990), Heft 4, S. 237 – 240

[12] *o.V.:* Das elektronische Stellwerk ESTW L90.
Firmendruckschrift SEL, Geschäftsbereich Bahnen, Bestell-Nr. 2524 7862.5 Be

[13] *Steinbrecher, H.; Böhm, W.:* Das Elektronische Stellwerk ELEKTRA.
Elektrotechnik und Informationstechnik, 109 (1992), Heft 3, S. 125 – 131

[14] *Berger, J.; Helmwein, J.:* Die Projektierung des Systems ELEKTRA.
SIGNAL+DRAHT, 86 (1994), Heft 4, S. 109 – 112

[15] *Krehle, H.-J.; Lennartz, K.:* Fahrdienstleiterarbeitsplatz am El L-Stellwerk.
SIGNAL+DRAHT, 81 (1989), Heft 11, S.227 – 232

[16] *Nikolaizik, J.; Nikolov, B.; Warlitz, J.:* Fehlertolerante Mikrocomputersysteme.
Berlin, 1990, S. 96 ff.

[17] *o.V.:* ESTW L90 Maximalkonfiguration pro Anschaltbereich.
Folie von Alcatel SEL

[18] *Erb, A.; Wirthumer, G.:* Zeitgemäße Basistechnologie für Fahrwegsicherung und operative Betriebsführung.
SIGNAL+DRAHT, 84 (1992), Heft 10, S. 309 – 312

[19] *Steinbrecher, H.; Fuss, G.:* Das Betriebsoperationssystem ELEKTRA.
Elektrotechnik und Informationstechnik, 109 (1992), Heft 3, S. 131 – 135

[20] *Kirsche, H.-J. (Hrsg.):* Lexikon Eisenbahn.
Berlin, 1973

[21] *Nordenfors, D.; Sjöberg, A.:* Computer-Controlled Electronic Interlocking System, ERILOCK 850.
Ericsson Review, 1986, Heft 1

[22] *o.V.:* EBILOCK 950.
Firmendruckschrift ABB Henschel AG, DEAHE-F 9500 D

[23] *o.V.:* EBICOS 900.
Firmendruckschrift ABB Signal

[24] *Blomqvist, L.; Lind, H.:* Automatische Zugsteuerung mit schneller Signalübertragung.
ABB Technik, 1994, Heft 8, S. 28 – 35

[25] *o.V.:* EBILOCK 850, fully electronic interlocking.
Firmendruckschrift ABB Signal

[26] *Backes, H.:* Rechnerunterstütztes Projektieren von Elektronischen Stellwerken.
SIGNAL+DRAHT, 82 (1990), Heft 11, S. 212 – 219

[27] *o.V.:* EBICOS 900.
Firmendruckschrift ABB Signal

[28] *McDougall, B.:* Launching second generation safe processor systems.

[29] *McDonald, W.:* WESTRACE: Second Generation Solid State Signalling.

[30] *o.V.:* WESTRACE Data Sheets.
Firmendruckschrift Westinghouse Brake & Signal Company

[31] *o.V.:* GRS: Helping to move rail transit into the future.
Firmendruckschrift

[32] *Shook, C. G.:* Microprocessors in fail-safe systems.
Vortrag auf dem IRSE Meeting, 1986

[33] *Strelow, H.:* Beurteilung des VPI-Stellwerk-Rechners von GRS.

Siemens-interner Aufsatz, 1989

[34] *o.V.:* VPI.
od de Rails, 1995, Heft 3

[35] *o.V.:* Vital Processor Interlocking Control System Application.
Firmendruckschrift General Railway Signal, 1994

[36] *Barnard, R.:* SSI-An international electronic interlocking product range.
GEC ALSTHOM Technical Review, 1994, Heft 15, S. 1 – 11

[37] *Leach:* Railway Control Systems.
London, 1991

[38] *Strelow, H.:* Besprechung über WESTRACE bei Westinghouse Brake and Signal.
Siemens-interner Aktenvermerk, 1990

[39] *Suwe, K.-H.:* Signaltechnik in Japan.
SIGNAL+DRAHT, 80 (1988), Heft 6, S. 132 – 139

[40] *Finke, W.; Ganswindt, T.:* Vereinheitlichte Stellwerksbauform von Siemens für Fernbahn, Stadtbahn und Industriebahn.
SIGNAL+DRAHT, 87 (1995), Heft 10, S. 350 – 354

[41] *Reschke, E.:* Vergleichende Untersuchungen zur Sicherheit in elektronischen Stellwerken.
Diplomarbeit an der Hochschule für Verkehrswesen „Friedrich List“, Dresden, 1990, S. 13

[42] *o.V.:* MCDS.
Firmendruckschrift IVV GmbH, Braunschweig, 1994

[43] *Pierick, K.; Wiegand, K.-D.:* Die MCDS-Technik als Basismodul einer rechnerintegrierten Prozeßregelung für Bahnen.
Eisenbahntechnische Rundschau, 43 (1994), Heft 11, S. 731 – 737

[44] *Gaillard, P.; Thies, H.:* Einsatz vereinfachter elektronischer Signaltechnik bei schweizerischen Privatbahnen.
SIGNAL+DRAHT, 87 (1995), Heft 11, S. 381 – 388

[45] *o. V.:* IVV.
Firmendruckschrift IVV GmbH, Braunschweig, 1996

Erklärung

Hiermit erkläre ich, daß die vorliegende Diplomarbeit von mir allein und nur unter Verwendung der angegebenen Hilfsmittel erstellt wurde.

Magdeburg, 3. Juni 1996

Thesen

1. Der Begriff des Elektronischen Stellwerks (ESTW) wird derzeitig international unterschiedlich gehandhabt. Wichtigste Frage dabei ist, ob die Bedieneinrichtungen und weitere, das Stellwerk beeinflussende Techniken zum ESTW gehören. In der Arbeit wird eine Definition vorgeschlagen und verwendet, die die Techniken der externen Einflußnahme vom ESTW abtrennt.

2. Bei Verwendung der o. g. Definition, lassen sich die betrachteten ESTW in Bedienverarbeitungs-, Sicherungs- und Stellebene untergliedern. Die Ebenen lassen sich nicht immer scharf voneinander abgrenzen, trotzdem hilft diese Einteilung bei einer Systematisierung der Stellwerkssysteme.

3. Viele weltweit eingesetzte ESTW bieten ein weitaus geringeres Sicherheitsniveau als es in Deutschland vorgeschrieben ist. Einkanalige Hardwarestrukturen, keine Sicherheit in Bedienung und Anzeige sowie der Einsatz ohne Sicherheitsnachweis sind durchaus üblich.

4. Die bei der DB AG eingesetzten ESTW genügen höchsten Sicherheitsanforderungen und bieten eine hohe Funktionalität. Dies führt jedoch zu einem hohen Preis, der für die Hersteller und Betreiber einen Wettbewerbsnachteil gegenüber anderen Anbietern bedeutet.

5. Die betrachteten ESTW lassen sich in drei Kategorien einteilen:

Komplexität	gering	mittel	hoch
Sicherheitsanforderungen (bezogen auf das Spektrum der ESTW)	gering	mittel	sehr hoch
Gesicherte Hilfsbedienungen	nicht möglich	teilweise möglich	möglich
Anforderungen an Funktionalität (bezogen auf das Spektrum der ESTW)	gering	mittel	hoch
Mögliche Größe der zu steuernden Anlagen mit einem ESTW	klein	mittel	groß
Verwendete Logikmodelle	Boolsche Gleichungen	Verschlußplan	Verschlußplan, Spurplan
Anwender (Auswahl)	außereuropäische Fernbahnen, Stadtbahnen	west- und nordeuropäische Fernbahnen, Stadtbahnen	mitteleuropäische Fernbahnen, deutsche Stadtbahnen

TECHNISCHE UNIVERSITÄT DRESDEN
FAKULTÄT FÜR VERKEHRSWISSENSCHAFTEN „FRIEDRICH LIST“
PROFESSUR VERKEHRSSICHERUNGSTECHNIK

Diplomarbeit

zum Thema:

Analyse zur Gestaltung elektronischer Stellwerke

vorgelegt am 5. Juni 1996 durch

Ulrich Maschek

geboren am 17.12.1970
Mat.-Nr. 2262792

Betreuer: Dr.-Ing. P. Naumann (TU Dresden)
Dipl.-Ing. H.-J. Petersen (SIEMENS AG, Bereich Verkehrstechnik, Braunschweig)

Inhaltsverzeichnis

Vorwort zur Diplomarbeit nach drei Jahren

Vor nunmehr drei Jahren schrieb ich die Arbeit „Analyse zur Gestaltung elektronischer Stellwerke“. Wie damals schon vermutet, war dies nur eine Momentaufnahme der innovationsfreudigen Industrie. Inzwischen haben sich viele Details geändert, grundlegende Änderungen gab es jedoch bei den beschriebenen Systemen nicht.

Nach drei Jahren Arbeit und Weiterbildung als Ingenieur muss ich aber auch einige Aussagen revidieren. So ist der damals von mir - in Einklang mit der Lehrmeinung an der Universität - vertretene Standpunkt, quantitative Sicherheitsnachweise seien nicht geeignet für den Nachweis der Sicherheit, heute nicht mehr haltbar. Gleichwohl kann ich meine Bedenken gegen Nachweise solcher Art aufgrund der vielen Abschätzungen nicht ganz verdrängen.

Auch die Privatisierung der Deutschen Bahn ist vorangeschritten und hat das Kostenbewusstsein weiter verstärkt. Auf die Sicherheit der Stellwerke hat dies keinen Einfluss gehabt, wohl aber auf die Sicherheit in der Betriebsführung. Es bleibt zu hoffen, dass man auch weiterhin mit gutem Gefühl im sichersten Landverkehrsmittel reisen kann.

Magdeburg, im August 1999 U. Maschek