TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Verkehrswissenschaften „Friedrich List“ Professur für Verkehrssicherungstechnik

Diplomarbeit

Untersuchungen zum Einsatz vereinfachter Bedienplätze

eingereicht von Florian Wieland

Prüfer:

Prof. Dr.-Ing. Jochen Trinckauf

Dr.-Ing. Ulrich Maschek

Betreuer:

Dipl.-Ing Carsten Weber

Dr.-Ing. Ulrich Maschek

Dipl.-Ing Klaus Bartnicki/Fa. Thales RSS GmbH

Autorenreferat

Diese Arbeit beschäftigt sich mit der Vereinfachung von Bedienplatzsicherungen für Stellwerke. Der Grund sind die strengen Anforderungen an Fahrdienstleiterbedienplätze im Bereich der Anzeigesicherheit. Das in Deutschland zu Grunde liegende Betriebsverfahren beruht darauf, dass der Bediener des Stellwerks immer den Zustand der Außenanlage sicher kennt.

Ziel war es, ein vereinfachtes Bedienplatzsystem zu finden, das gleichzeitig zulassungsfähig ist. Mangels Felddaten ist dieses Ziel nicht erreicht worden. Hingegen liegt eine fundierte Annäherung an das Thema vor. Die Arbeit zeigt aktuelle Anstrengungen zur Vereinfachung von Bedienplätzen auf und führt diese in Gedankenexperimenten fort. Neben dem Studium einschlägiger Fachliteratur wurden Fachleute auf Herstellerseite und auf Betreiberseite befragt, außerdem wurde der Blick zu ausländischen Bahnen gewagt.

Es werden verschiedene Ansätze zu Vereinfachung der Bedienplatzsysteme diskutiert. Zum einen wird mit der Forderung nach einer Vereinfachung der Definition einer sicheren Anzeige vor allem auf eine Vereinfachung des Zulassungsprozesses hingewirkt. Zum anderen wird auf die Anzeigensicherung verzichtet und der Einfluss auf die Rückfallebenen diskutiert. In weiteren Kapiteln werden einfache Sicherungsmaßnahmen wieder eingeführt um den Einfluss auf die Rückfallebene zu begrenzen und die Einführung verfahrensbasierter Anzeigesicherungen diskutiert.

Um die Empfehlung, die Verfahrenssicherung nach dem Vorbild EBO 2 zu übernehmen, zu realisieren, ist das Erstellen einer Risikoanalyse für Regionalnetze erforderlich. Weiterhin werden zusätzliche Untersuchungen zur menschlichen Fehlerwahrscheinlichkeit für notwendig erachtet.

Abstract

This report engages in the simplification of the rather complex safety measurements for German solid state interlocking operations control centres. The reason for the complexity is high requirements in indication solutions, being necessary because of the underlined German operations procedure as it is based on the signaller's precise knowledge of the actual state of the safety equipment at any time.

Being an expense factor, technically based indication safety is challenged when lines with less traffic are considered. The omitting goes with the current diversification process at solid state interlockings in Germany, offering exactly the necessary amount of safety equipment depending on the lines traffic situation.

Acceptable simplification possibilities were searched but not sufficiently found due to lack of field data. Nevertheless an approach to the topic has been achieved and ongoing developments have been identified and explained. The topic of safety and availability has been introduced as basis for the following research of requirements for operations control centres.

Different approaches for simplification have been conducted. First of all the definition of a safe indication has been discussed. The basis of the criticism is the requirement of SIL 4 for Indications whilst a human with its high failure rate has to interpret it. It has been suggested to lower the requirement and lower the human failure rate instead procedure based. That would actually raise the over all safety.

By means of a gedankenexperiment the safety measurements of indications have been omitted and studied how the fall back policies in operations procedures would need to bee changed to insure safe traffic. In a second step different simple safety procedures have been introduced and discussed.

The recommendation to adapt the procedure based safety of Austrian railways to use for ESTW-R necessitates a risk analysis for railway operation in rural areas as well as further inquiries concerning human failure rates.

Annahmen und Thesen

Inhaltsverzeichnis

1 Einleitung

1.1 Zielsetzung

Vor dem Hintergrund des zunehmenden Modernisierungsbedarfs der Leit- und Sicherungstechnik (LST) für Strecken mit schwachem bis mäßigem Verkehr bedarf es einer angepassten und dadurch preiswerten Technik. Es wird in dieser Arbeit untersucht, wie eine Vereinfachung von Bedienplätzen für elektronische Stellwerke (ESTW) realisiert werden kann. Betrieblichen Rückfallebenen werden im Kontext von Sicherheit und betrieblicher Verfügbarkeit für die unterschiedlichen Realisierungsvarianten betrachtet und die Durchführbarkeit in einer knappen Marktbetrachtung diskutiert.

Was die Arbeit nicht bietet sind direkt umsetzbare Ergebnisse. Dies liegt an dem Mangel an Felddaten der sich wie ein roter Faden durch die Abhandlung zieht. Hingegen liegt eine fundierte Annäherung an das Thema vor. Die Arbeit zeigt aktuelle Anstrengungen zur Vereinfachung von Bedienplätzen auf und führt diese in Gedankenexperimenten fort. Neben dem Studium einschlägiger Fachliteratur wurden Fachleute auf Herstellerseite und auf Betreiberseite befragt außerdem der Blick zu ausländischen Bahnen gewagt.

1.2 Einordnung des Themas

Das **Durchschnittsalter** der Sicherungstechnischen Anlagen der DB-Netz AG **steigt**. Die Ursache sind die nicht in hinreichendem Umfang durchgeführten Ersatzinvestitionen, was mit begrenzten zur Verfügung stehenden finanziellen Mitteln begründet werden kann. Laut Bormet (1) müssten, um das Durchschnittsalter konstant zu halten, von den 250 000 Schalteinheiten[1] der DB-Netz AG jährlich 5700 erneuert werden, im Gegensatz zu tatsächlichen 3000 Schalteinheiten.

[1] Schalteinheiten sind die Summe der Weichen mit Gleissperren und Signale mit Zusatzanzeiger. Sie sind nicht zu verwechseln mit den Anschlusseinheiten (ASE) Siehe hierzu auch (1).

Bormet beschreibt eine **Life-Cycle Strategie zur Kostenreduktion** im LST Bereich. Vorgeschlagene Maßnahmen sind unter anderem:

- Die Optimierung und Modularisierung der ESTW und Schaffung von einheitlichen Schnittstellen innerhalb des Systems, z.B. zwischen Sicherungskern und Bedienebene um auch anderen Herstellern das Anbieten eines Bedienplatzes zu ermöglichen und dadurch Wettbewerb und Innovation zu steigern.
- Schaffung einer generischen Blockschnittstelle auf ESTW-Seite.
- Reduzierung der Verkabelung durch ISDN- oder BUS-Anbindung der Elemente.
- Durchgängige Datenhaltung soll Effizienz von Investitionen und Instandhaltung steigern
- Anforderungsstandard in Abhängigkeit von der Streckenkategorie.

Der letzte Punkt soll hier näher betrachtet werden. Die DB-Netz AG hat in der Konzernrichtlinie (Koril) 413 **Streckenstandards definiert** (2). In diesen werden die Strecken nach ihrer verkehrlichen Bedeutung eingeteilt und entsprechend dem Standard ausgerüstet. Auch die LST-Ausrüstung ist in Anlehnung an diese Standards diversifiziert worden. Abbildung 1 zeigt die verschiedenen Abstufungen. Die Grenzen zwischen den Bauformen sind nicht scharf und die zugeordneten Streckenkategorien stellen nur Anhaltspunkte dar.

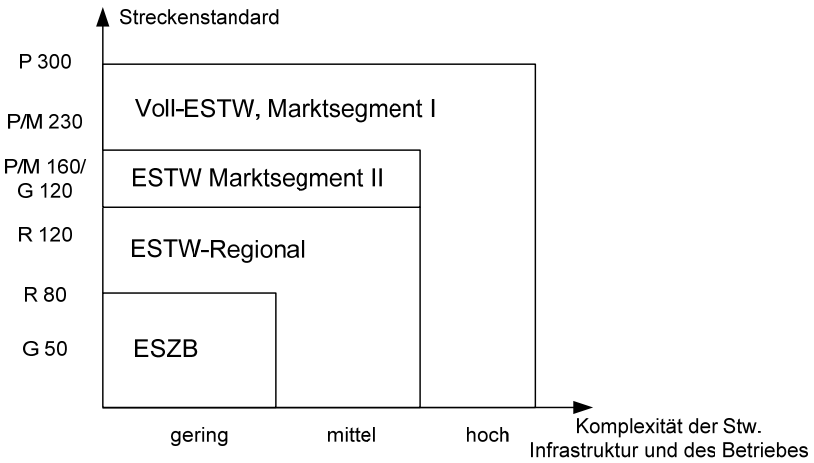

Abbildung 1 Diversifizierung der Stellwerke

Das Voll-ESTW ist mit allen ESTW Funktionalitäten ausgestattet und erfüllt höchste Ansprüche an Verfügbarkeit und Sicherheit. Es gilt für den Betrieb die Koril 408, Züge fahren und Rangieren (3).

Das ESTW Marktsegment (MS) II unterscheidet sich vom ESTW nach MS I nur durch Funktionen, auf die verzichtet wurde. Dies sind unter anderem Mittelweichenfunktion, Zuglenkung und die BZ-Fähigkeit, aber auch sicherheitserhöhende Funktionen wie die Fahrstraßen Prüfung und Überwachung (FPÜ) auf die später noch eingegangen wird. Insgesamt wird auf 20 Funktionen verzichtet (4). Da aber die Funktionen nur gesperrt werden, jedoch nach wie vor vorhanden sind, haben etablierte Hersteller dadurch keine Vorteile. Dieses ESTW wird nur sehr selten bestellt, da dies vertraglich nur möglich ist, wenn tatsächlich alle 20 Funktionen nicht benötigt werden (5).

Ein eigenes Lastenheft wurde für das **ESTW-Regional (ESTW-R)** herausgegeben[2] (6). Ausrüstung und Funktion werden gegenüber dem Voll ESTW (nach Systemvertrag) reduziert. Dabei wird das ESTW-R als Untermenge des Voll-ESTW bezeichnet. Dies soll zum Ausdruck bringen, dass keine zusätzlichen Funktionen gefordert werden.

Den Herstellern der Voll-ESTW's soll dadurch das Anbieten von **ESTW-R allein durch Weglassen von Funktionen** ermöglicht werden. Am Beispiel des **Verzichts auf Zugdeckungssignale** wird deutlich, dass dem nicht so ist (7). Das Einfahren in teilweise besetzte Gleise soll nämlich weiterhin möglich sein. In der ESTW-Logik ist das Einstellen von Zugfahrstraßen in besetzte Gleise jedoch nicht möglich. Aufwendige Programmierarbeiten sind die Folge.

Weiter soll auf Ersatzsignale verzichtet werden. Das Zulassen einer Fahrt ohne Hauptsignal erfolgt mittels schriftlichen Befehls, der jedoch derart in das Bediensystem integriert wird, dass anstelle der Ersatzsignal-Bedienungen EE1 und EE2 die Bedienungen BEFEHLA und BEFEHLB aufgenommen werden und unter den gleichen Voraussetzungen bedienbar sind.

---

[2] Sowohl beim ESTW MS II als auch für das ESTW-R wird teilweise vom Regio-ESTW gesprochen. In dieser Arbeit wird der Begriff ESTW-R ausschließlich für das ESTW nach Lastenheft ESTW-R verwendet.

Grundsätzlich kann festgestellt werden, dass auch hier **vor allem funktionale Abstriche** gemacht wurden. In Ansätzen sind auch nonfunktionale Erleichterungen erkennbar:

- Ein sicheres Meldebild wird für die Lupen gefordert. Für die Bereichsübersichten soll dies jedoch optional möglich sein.
- Der Einsatz weiterer vom EBA zugelassener Verfahren zur sicheren Meldebildanzeige ist unter Beachtung der Rahmenbedingungen (z.B. Einsatz in einer Regionalen Bedienzentrale) zulässig.

Ziel dieser Festlegung ist es, auch andere Verfahren nicht auszuschließen als die bisher gängigen. Ziel dieser Arbeit ist es ein solches System zu entwickeln.

Das ESZB ist ein Betrieb mit ESTW der auf dem Zugleitbetrieb (Zlb) basiert (8). Der Betrieb unterscheidet sich im Regelbetrieb nicht notwendigerweise von dem des mit normalen ESTW. Durch den **Zugleitbetrieb als** Basis kann in der **Rückfallebene** auf diesen zurückgegriffen werden. Die entscheidende Konsequenz daraus ist die Einbeziehung des Lokführers in die Rückfallebene, eine Möglichkeit, die sonst kategorisch ausgeschlossen wird und die **Verwendung eines nicht gesicherten Bedienplatzes** ermöglicht. Dies stellt eine entscheidende nonfunktionale Erleichterung dar.

Hilfsbedienungen werden in Hilfsumgehungen und Hilfshandlungen unterschieden und müssen unter **Mitwirkung des Zugleiters und des Lokführers**[3] durchgeführt werden. Erstere identifiziert den Grund warum eine Fahrstraße nicht eingestellt werden kann. Unter Umgehung des gestörten Elements kann die Fahrstraße dann gesichert werden. Für das gestörte Element müssen nun Hilfshandlungen durchgeführt werden (9). Die funktionalen Abstriche gehen hier noch über die des ESTW-R hinaus. Eine Einführung in die Thematik des Zugleitbetriebs bietet (10).

[3] Im reinen Zugleitbetrieb werden oft die Aufgaben des Zugführers durch den Lokführer wahrgenommen, im SZB-E ist dies grundsätzlich der Fall.

Tabelle 1 Funktionale und Nonfunktionale Abstufungen der ESTW

	ESTW MS II	ESTW-R	ESZB
Max. Weichen /Bf	unbegrenzt	32	8[4]
Max. Hauptsignale/Bf	unbegrenzt	22	12[5]
Bsp. Zug-deckungssignale	Ja	Nein	Ja
Bsp. Zust. zur Fahrt ohne Hauptsignal	Ersatzsignal	Befehl (mit Kf-Bedienung)	Ersatzsignal
Bsp. FPÜ/Hilfs-umgehung	Nein	Nein	Ja
Gesichertes Meldebild	Ja, volle Ausrüs-tung	Ja, Sonderformen u.u. zugelassen	Nein
Hilfsbedienung	Durch Fdl autonom	Durch Fdl autonom	Unter Einbeziehung des Tf.

Tabelle 1 listet eine Auswahl von zum Teil widersprüchlichen Forderungen für verschiedene ESTW auf. In den weiteren Betrachtungen sollen vor allem das ESTW-R betrachtet werden und mögliche Formen des sicheren Meldebilds untersucht werden. Als **Referenz-Strecke wird die Definition des Streckenstandards R 120 aus** (2) **verwendet**. Zu Vergleichszwecken wird auch auf das ESZB immer wieder eingegangen. Um eine einheitliche Basis zu schaffen, soll im nächsten Kapitel auf die Grundstrukturen von ESTW eingegangen werden.

These 1: Durch eine anforderungsgerechte Gestaltung von LST können Kosten gesenkt werden und das Steigen des Durchschnittsalters gebremst werden.

1.3 ESTW Prinzipien

Der prinzipielle **Aufbau der ESTW** wird üblicherweise mit dem **Ebenenmodell** beschrieben (11) und (12), siehe Abbildung 2. Hier unterscheidet man drei Ebenen der Funktionalität:

[4] Quelle: (9): Es ist jedoch unklar ob sich die Angaben auf eine Beschränkung der möglichen Elemente beziehen oder ob lediglich der größte realisierte Bf. vorgestellt wird.
[5] Quelle: (9): Es ist jedoch unklar ob sich die Angaben auf eine Beschränkung der möglichen Elemente beziehen oder ob lediglich der größte realisierte Bf. vorgestellt wird.

- **Die Bedienebene**: hierzu zählen Bedienplätze ebenso aber dispositive Systeme wie die Zuglenkung. Auf dieser Ebene werden die Stellbefehle generiert.
- **Die Sicherungsebene**: hier werden die eingegebenen Befehle auf ihre Durchführbarkeit hinsichtlich der Sicherheit geprüft. Im Regelfall interagieren die Elemente der Bedienebene mit der Sicherungsebene.
- **Die Feldebene** besteht aus den Aktoren und Sensoren sowie den Schnittstellen zur Sicherungsebene. Aus den Meldungen der Sensoren der Feldebene kann die Sicherungsebene die Zulässigkeit von Eingaben des Bedieners prüfen und zulassen. Diese werden dann durch die Sicherungsebene veranlasst und an die Feldebene weitergegeben.
- **Die Ein-/Ausgabeebene** ist das Bindeglied zwischen Bedien- und Sicherungsebene, **die Stellebene** ist das Bindeglied zwischen Sicherungs- und Feldebene.

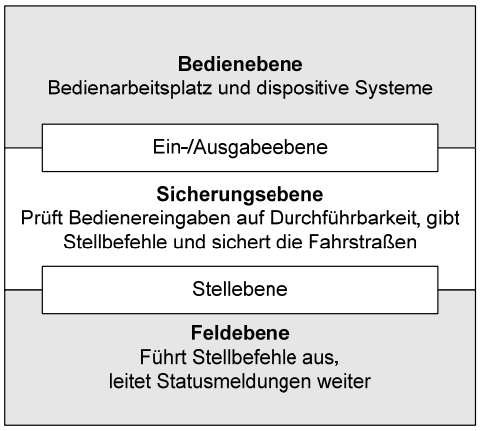

Abbildung 2 Ebenenmodell für ESTW

Prinzipiell wurden für die ESTW die Sicherungslogik der Spurplanstellwerke übernommen und die Schaltungen in Computerlogik programmiert. Die große Herausforderung bestand jedoch darin, die Sicherheit der Stellwerke nachzuweisen. Bei Relais-Technologie sind die Schaltungen offensichtlich. Die möglichen Fehler konnten erkannt werden und konstruktive Maßnahmen verhinderten den gefährlichen Zustand oder sorgten für eine hinreichend kleine Fehleroffenbarungszeit.

Softwarefehler können nicht vorausgesehen werden. Bei dieser Fehlerart handelt es sich um systematische Fehler also Programmierfehler. Solche Fehler sind bei umfangreichen Quelltexten unvermeidbar und finden sich überall und können sich daher in beliebiger Form äußern. Verschiedene Maßnahmen aus

der Informatik, die in Kapitel 2.3 beschrieben werden, sollen dieser Problematik begegnen und das System fehlertolerant machen.

Der modulare Aufbau eines ESTW ist in Abbildung 3 am Beispiel des ESTW L90 dargestellt. Den Kern bildet die ESTW-Zentrale (ESTW-Z) oder die ESTW-Unterzentrale (ESTW-Uz). Diese sind vollständige Stellwerke mit allen Bestandteilen. Weitere Betriebsstellen die eine maximale Entfernung vom ESTW-Z/Uz haben dürfen, können über Anschluss-ESTW (ESTW-A) an das ESTW-Z/Uz angebunden werden. Die ESTW-A enthalten ausschließlich die Schnittstellen zu den Feldelementen, die Fahrstraßensicherung erfolgt von dem zugehörigen ESTW-Z/Uz. Eine Unterzentrale (ESTW-Uz) wird von einer Betriebszentrale (Bz) fernbedient, eine Zentrale (ESTW-Z) wird vor Ort bedient.

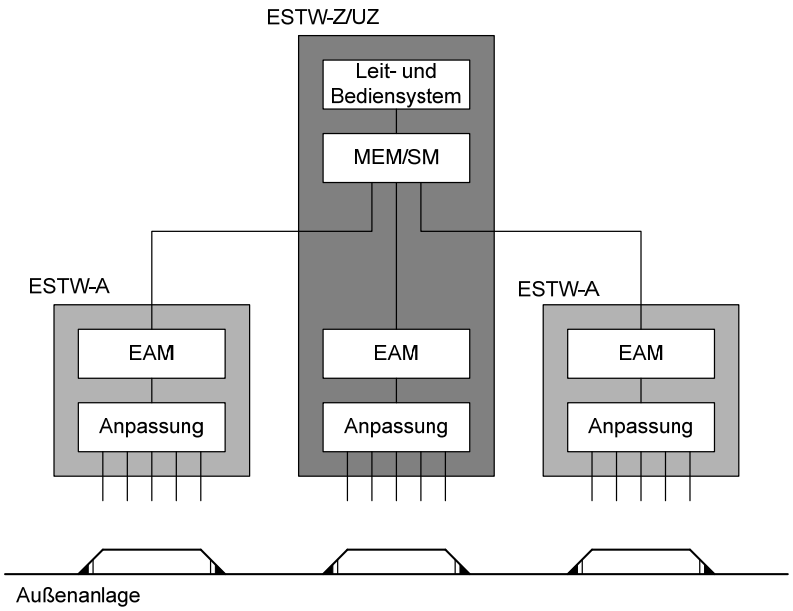

Abbildung 3 Prinzip ESTW L90

Die Sicherungsebene des ESTW L 90 wird durch das Sicherungsmodul (SM) und das Melde- und Eingabemodul (MEM) gebildet. Im MEM werden die Eingaben des Bedieners auf Konsistenz und Syntax geprüft, das vom SM ausgegebene Meldebild wird für die Bedienebene aufgearbeitet. Das MEM repräsentiert die Ein-/Ausgabeebene aus Abbildung 2.

Im SM sind alle Elementverknüpfungen und Fahrstraßen gespeichert. Fahrstraßenwünsche werden auf Zulässigkeit geprüft und Stellbefehle an die Feldebene gesendet. Die SM angrenzender Stellbezirke sind seriell miteinander zum Austausch von Fahrstraßeninformationen verbunden. Über diese Schnittstelle werden auch benachbarte ESTW angebunden. Die Verbindung zum MEM erfolgt ebenfalls seriell. Das SM stellt die Sicherungsebene dar.

Das Element-Ansteuer-Modul (EAM) als Modul der Stellebene überwacht die Elemente der Außenanlage und gibt deren Lage bei Veränderung oder auf Anfrage an die Sicherungsebene. Außerdem werden Stellbefehle der Sicherungsebene ausgeführt. Das EAM kann im ESTW-Z/Uz installiert werden oder abgesetzt an Standorten. Dadurch lassen sich große Stellbereiche verwirklichen.

Die vorgestellte Einteilung in Feldebene, Sicherungsebene und Bedienebene gilt für alle ESTW. Die Unterteilung in Module wurde am Beispiel des ESTW L 90 erläutert. Das Ebenenmodell ermöglicht die folgende Annahme.

Annahme 1: Die Sicherungsebene wird im Sinne dieser Arbeit als „unfehlbar" angesehen.

2 Sicherheit und Verfügbarkeit

Diskutiert man über die Vereinfachung von Bestandteilen der Sicherungstechnik, ist das Thema von Sicherheit und Verfügbarkeit essenziell. Es wird daher in diesem Kapitel ausführlich besprochen.

2.1 Definitionen

Alle Definitionen stammen soweit nicht anders angegeben aus (13).

Zuverlässigkeit *ist die Wahrscheinlichkeit, dass eine Einheit ihre Funktion unter der gegebenen Zeitspanne (t_1, t_2) erfüllen kann.*

Die Einheit erfüllt ihre Funktion nicht, wenn es sich um einen sicherheitsrelevanten Ausfall oder um einen verfügbarkeitsrelevanten Ausfall handelt. Dabei ist nur die Tatsache relevant, dass ein Ausfall stattfindet – die Dauer ist nicht maßgebend. Die Zuverlässigkeit strebt bei ausfallfreiem Betrieb gegen null, da ein Ausfall im Intervall (t1, t2) immer wahrscheinlicher wird.

Verfügbarkeit *ist die Fähigkeit eines Produkts, in einem Zustand zu sein, in dem es unter vorgegebenen Bedingungen zu einem vorgegebenen Zeitpunkt oder während einer vorgegebenen Zeitspanne eine geforderte Funktion erfüllen kann unter der Voraussetzung, dass die geforderten äußeren Hilfsmittel bereitstehen.*

Während die Zuverlässigkeit nur bis zum nächsten Ausfall definiert ist, also Einheiten ohne Erneuerung betrachtet, ist die Verfügbarkeit eine Erweiterung für Einheiten mit Erneuerung, d.h. mit Reparatur. Es wird das Verhältnis der Zeit angegeben, in der das Gerät seine Aufgaben erfüllt, zum Betrachtungszeitraum. Grundsätzlich ist davon auszugehen, dass Sicherungstechnik im Falle eines sicherheitskritischen Fehlers eine der geforderten Funktionen nicht erfüllen kann.

Es ist jedoch im Eisenbahnbereich **zwischen technischer und betrieblicher Verfügbarkeit zu unterscheiden**. Letztere wird meist in Verspätungsminuten

erfasst. Ein sicherheitsrelevanter Fehler erzeugt jedoch keine Verspätungsminuten und wird somit nicht in Verfügbarkeitsstatistiken aufgeführt. Erst wenn der Fehler offenbar ist und betriebliche Maßnahmen getroffen werden entstehen Verspätungsminuten. Dann ist aber die Sicherheit wieder voll gegeben. Es wird daher angenommen, dass sicherheitsrelevante Fehler die betriebliche Verfügbarkeit nicht einschränken. Ist künftig nur **von Verfügbarkeit die Rede**, ist immer die **betriebliche Verfügbarkeit gemeint**.

Sicherheit *ist das Nichtvorhandensein eines unzulässigen Schadensrisikos.*

Risiko ist *die Wahrscheinlichkeit des Auftretens einer Gefahr, die einen Schaden verursacht, sowie der Schweregrad eines Schadens.*

Gefahr *ist eine Sachlage, bei der das Risiko größer als das Grenzrisiko ist. (VDE 31000/VDE 1987).*

Grenzrisiko *ist das größte noch vertretbare Risiko eines bestimmten technischen Vorganges oder Zustands. Im Allgemeinen lässt sich das Grenzrisiko nicht quantitativ erfassen (VDE 31000/VDV 1987).*

Abbildung 4 soll diese Definitionen veranschaulichen. Dabei geht von einer technischen Anordnung grundsätzlich eine Gefährdung aus. Diese Gefährdung wird in ihrer quantifizierten Form Gefährdungsrate bezeichnet. Das Produkt aus Gefährdungsrate und Schadensausmaß bezeichnet man als Risiko. Das Grenzrisiko ist dabei ein festgelegtes tolerierbares Maximum des Risikos. Wird dies überschritten, spricht man von Gefahr.

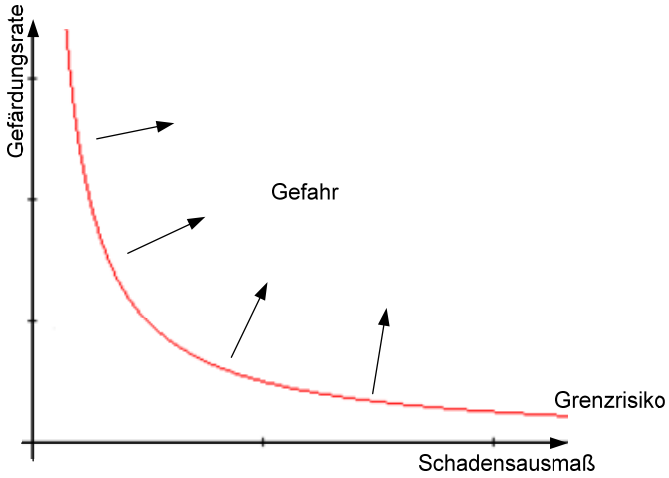

Abbildung 4 Risiko, Grenzrisiko und Gefahr

2.2 Zusammenhang zwischen Sicherheit und Verfügbarkeit

Der Zusammenhang zwischen Sicherheit und (betrieblicher) Verfügbarkeit (14) lässt sich an einem Gedankenexperiment verdeutlichen. Ein stillgelegtes Fahrzeug ist sicher aber nicht verfügbar. Ein Fahrzeug, das ohne Sicherheitsfunktionen fährt und somit nicht aufgrund eines Fehlers gestoppt wird ist hoch verfügbar aber nicht sicher. Verfügbarkeit und Sicherheit sind voneinander gemäß Abbildung 5 abhängig.

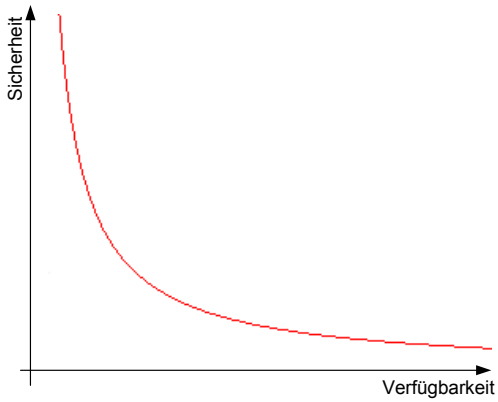

Abbildung 5 Zuverlässigkeitsdiagramm

Bei gleicher Zuverlässigkeit kann die Sicherheit zu Kosten der Verfügbarkeit maximiert werden oder die Verfügbarkeit zu Kosten der Sicherheit maximiert

werden. Die Zuverlässigkeit erhöht sich wenn Sicherheit und Verfügbarkeit erhöht werden. Die Abhängigkeit der Aufwendungen bei Erhöhung der Zuverlässigkeit ist qualitativ in Abbildung 6 dargestellt. Der Grenznutzen einer Aufwandseinheit nimmt mit zunehmender Zuverlässigkeit ab.

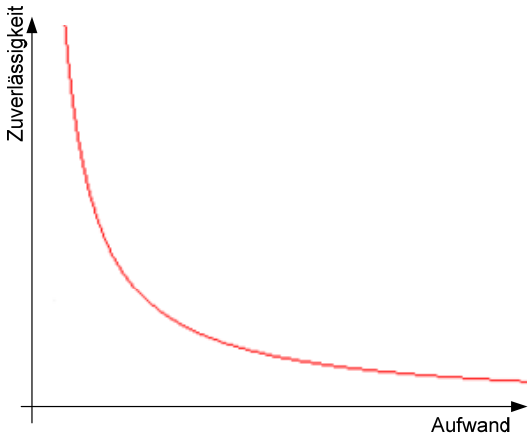

Abbildung 6 Zuverlässigkeits-Aufwands-Diagramm

Es wird die These vertreten, dass jeder Fehler in Sicherheitsverantwortung tragenden Bauteilen der LST auch ein sicherheitskritischer Fehler ist. Nach der Fehleroffenbarung und der Fehlerreaktion geht das System in einen sicheren Zustand über, der Fehler wird verfügbarkeitsrelevant. Dies teilt sich auf in logistische Wartezeiten und die Fehlerbehebung. Der Lebenslauf eines Fehlers (15) ist in Abbildung 7 dargestellt.

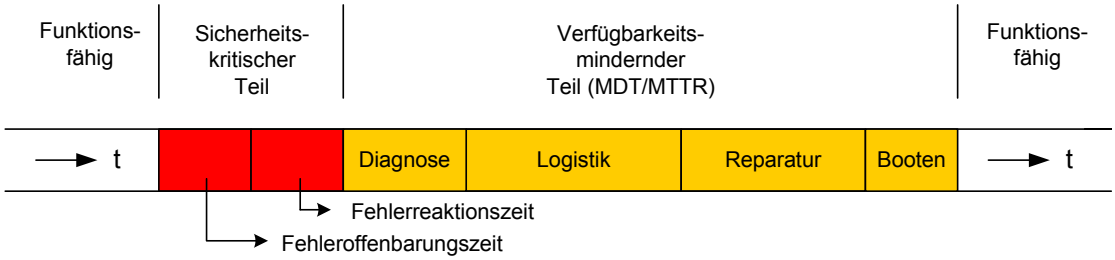

Abbildung 7 Lebenslauf eines Fehlers

Es wurden die Zusammenhänge zwischen Sicherheit und Verfügbarkeit aufgezeigt. Fehler lassen sich in ein Sicherheits-Verfügbarkeits-Diagramm einordnen. Im Folgenden sollen Möglichkeiten besprochen werden, Sicherheit und Verfügbarkeit zu manipulieren.

2.2.1 Redundanz für Verfügbarkeit und Sicherheit

Redundanz ist das zentrale Mittel zur **Herstellung von Zuverlässigkeit**. Je nach Verwendung kann durch Redundanz das Sicherheitsverhalten oder die Verfügbarkeit beeinflusst werden.

Unter Redundanz versteht (16) das *Vorhandensein von überflüssigen, für die Information nicht notwendigen Elementen in einer Nachricht.* Dies kann jedoch beabsichtigt oder unbeabsichtigt sein, insofern ist sie nicht in jedem Fall überflüssig. (17) definiert Redundanz als *alle unter Fehlerfreiheit entbehrlichen Mittel*. Eine Einführung in das Thema der Redundanz liefern (17) und (18).

Man kann **verschiedene Arten von Redundanzen** unterscheiden (19):

- Hardwareredundanz (strukturelle Redundanz)
- Informationsredundanz
- Zeitredundanz
- Softwareredundanz (funktionelle Redundanz)
    - Zusatzfunktion
    - Diversität

Bei **Hardwareredundanz** sind **Hardwarekomponenten mehrfach vorhanden** wie z.B. bei 2 von 3 oder 2 von 2 Systemen. Man unterscheidet dabei zwischen heißer und kalter Redundanz je nach dem ob die redundanten Komponenten während des Normalbetriebs arbeiten oder nicht. Bei kalter Redundanz muss ein Verfahren gefunden werden, das Ersatzsystem im Fehlerfall in Betrieb zu nehmen.

Funktionelle Redundanz bezeichnet die Erweiterung eines Systems um für den Regelbetrieb entbehrliche **Funktionen wie z.B. Testfunktionen** (19). Hierunter fällt auch die Diversität (Softwarediversität), welche ein Mittel darstellt um das gleichzeitige Ausfallen redundanter Komponenten aufgrund von Softwarefehlern zu verhindern. (19) führt als Alltagsbeispiel das Einholen einer zweiten Ärztemeinung an.

Mit **Informationsredundanz** sind **Anhänge an Datentelegramme** gemeint wie sie durch das Hinzufügen einer Prüfsumme entstehen. Diese Anhänge können mit übertragen werden oder mit gespeichert werden.

Zeitredundanz bezeichnet die über den Zeitbedarf des Normalbetriebs hinausgehende Zeit, die einem funktionell redundanten System zur Funktionsausführung zur Verfügung steht (19). Ein Beispiel ist das nochmalige Versenden eines verlorengegangenen Telegramms nach Ablauf eines Timers.

Redundanz wird entweder nur zur **Fehlererkennung** (Sicherheitsaspekte) **oder** auch zur **Fehlerkorrektur** (Verfügbarkeitsaspekte) genutzt. Dabei können jeweils verschiedene Arten von Redundanz zur Anwendung kommen. **Möglichkeiten zur Fehlererkennung** sind laut (19):

- Die Zeitschrankenüberwachung
- Absoluttests: z.B. muss die Anzahl von Datensätzen vor und nach der Sortierung übereinstimmen
- Relativtests: Zwei redundant berechnete Ergebnisse werden verglichen.
- Nutzung von Informationsredundanz wie CRC Codes.

Fehlerkorrekturen werden i.a. über Mehrheitsentscheidungen herbeigeführt. So gilt bei einem 2 von 3 System das Ergebnis, das bei mindestens zwei Rechnern übereinstimmt. Im Eisenbahnbereich war die Fehlerkorrektur im Bereich der Informationsredundanz nicht zulässig[6].

These 2: Zuverlässigkeit, die über die dem System immanente Zuverlässigkeit hinaus geht kann nur über Redundanz erreicht werden.

Nachdem nun die praktischen Mittel gegeben sind, Sicherheit und Verfügbarkeit zu beeinflussen sollen die Umsetzbarkeit solcher Maßnahmen diskutiert werden.

[6] Nach der inzwischen ungültigen Mü 8004.

2.2.2 Variation der Sicherheit

Das **Kalkulieren mit Sicherheit** ist in Deutschland mit einem negativen Beigeschmack verbunden. Es wird oft der Vorwurf geäußert, es gelte der Grundsatz „so sicher wie möglich", der Deutschland eines der sichersten aber auch teuersten Eisenbahnsysteme eingebracht habe.

Variation der Sicherheit ist in diesem Fall jedoch so zu verstehen, dass eine **stark belastete Hauptstrecke zurzeit den gleichen Anforderungen** genügen muss **wie eine wesentlich schwächer ausgelastete Strecke** im Regionalverkehr. Da die Sicherheit als Kehrwehrt des Risikos berechnet wird und dieses sich aus Schadenshäufigkeit multipliziert mit dem zu erwartenden Schadensausmaß ergibt, erhält man große Sicherheitsunterschiede. Geringer belastete Strecken weisen **geringeren Verkehr** auf und mindern somit die Schadenshäufigkeit bei gleichzeitig **geringerer Höchstgeschwindigkeit**, was das zu erwartende Schadensausmaß reduziert.

Die einzige Möglichkeit, diese Missstände anzupassen **ist eine Risikoanalyse nach EN 50126**, die durch den Betreiber zu erbringen ist und speziell auf die Verhältnisse für Strecken mit schwachem bis mäßigem Verkehr zugeschnitten sein muss oder die die gleiche Sicherheit wie im Fern- und Ballungsnetz nachweist. In Anbetracht der Tatsache, dass selbst die Risikoanalysen für den normalen Betrieb noch nicht verfügbar sind, sollte man in den nächsten Jahren hier noch keine Fortschritte erwarten. Siehe hierzu auch Kapitel 3.3.1.

These 3: Die Anforderungen an die Sicherheit signaltechnischer Anlagen sind auf Strecken mit schwachem bis mäßigem Verkehr zu hoch. Um diesen Zustand zu korrigieren muss eine Risikoanalyse für den Betrieb auf diesen Strecken erstellt werden

2.2.3 Variation der Verfügbarkeit

Mit einem Angleichen der Sicherheit ist in den nächsten Jahren nicht zu rechnen (trotzdem wird in Kapitel 4.1 ein Vorschlag dazu unterbreitet). Dagegen kann **bei gleicher Sicherheit die Verfügbarkeit variiert werden**. Die Argu-

mentation entspricht der des vorherigen Kapitels, in dem es um die Sicherheit ging.

Das Messen der Verfügbarkeit erfolgt im Bahnbereich üblicherweise in Verspätungsminuten. Erweitert man diese Definition auf **Fahrgast-Verspätungsminuten** oder entsprechendes bei Güterzügen so kommt man zu dem Ergebnis, dass auf hochbelasteten Strecken die Verspätung minimiert werden muss, da viele Fahrgäste davon betroffen sind.

$$Verfügbarkeit = \frac{Verspätung}{Zug} * \frac{Fahrgäste\ oder\ Nutzlast}{Zug} * Anzahl\ Züge$$

Bei **Strecken mit geringerem Fahrgastaufkommen** sind weniger Fahrgäste durch die Verspätung eines Zuges betroffen. Der **Nutzen einer hohen Verfügbarkeit ist somit geringer**, er sollte nicht überproportional durch hochverfügbare Technik bezahlt werden. Es ist ein Gleichgewicht zu finden zwischen Produktattraktivität, die im wesentlichen Maß durch Pünktlichkeit bestimmt wird, und der Wirtschaftlichkeit einer Strecke.

Es wird vorgeschlagen, einen **Vergleichswert auf Basis von tolerierbaren Verspätungsminuten** zu berechnen. Berücksichtigt werden müssen der Streckenwirkungsgrad als Maßstab der Möglichkeit, Verspätungen zu reduzieren, die Anzahl der Streckengleise als wesentliches Kriterium der Abhängigkeit einer Zugfahrt von Fahrten in die Gegenrichtung sowie die Einfallverspätung, die als Maß für die Verkettung der Fahrten in den nicht betrachteten Anschlussbereichen dient. Von diesen Verspätungsminuten kann dann auf die benötigte Verfügbarkeit des Systems geschlossen werden. Diese muss in geeigneter Weise auf die verschiedenen Systembestandteile, darunter die LST, aufgeteilt werden.

Um die tolerierbare Verspätung zu Berechnen und diese auf die LST aufzuteilen müssen Daten über Verspätungen bekannt sein. Ebenfalls werden Verfügbarkeitsaussagen zur verwendeten Technik benötigt. Es war im Zuge dieser Arbeit nicht möglich, Felddaten dieser Art zu bekommen, daher wird der Verfügbarkeitseinbruch nicht qualifiziert.

These 4: Die mögliche Minderung der Verfügbarkeit von LST kann anhand von tolerierbaren Verspätungsminuten ermittelt werden. Dazu werden Felddaten benötigt.

2.3 Funktionale Sicherheit

Mit der funktionalen Sicherheit soll hier ein Kapitel angesprochen werden, dem oft mit Unverständnis begegnet wird. Es soll daher versucht werden auch dem diesbezüglich Fachfremden das nötige Wissen zu vermitteln um dem weiteren Verlauf der Arbeit folgen zu können. Dabei wird der Begriff selbst erläutert um anschließend seine Einordnung in den Themenkomplex der Risikoanalysen aufzuzeigen.

Funktionale Sicherheit ist der Teil der Gesamtsicherheit, der von der konkreten Funktion eines sicherheitsbezogenen Systems abhängt (20). Das Beispiel eines Elektromotors und Abbildung 8 sollen den Begriff verdeutlichen. Elektromotoren können durch Überlastung oder einen Defekt überhitzen. Den Schutz der Umgebung kann man einerseits durch das Aufstellen des Motors in einem geschützten Raum erreichen, was keine funktionale Sicherheit darstellt. Andererseits kann man einen **Wärmesensor (Sensor) installieren**, der bei Überhitzung eine Abschaltung (Actor) des Motors (EUC) initiiert. **Dies ist eine Sicherheitsfunktion**, die erreichte Sicherheit ist somit **eine funktionale Sicherheit**. Es ist wichtig, dass diese Funktion auch zuverlässig funktioniert. Wie zuverlässig, hängt einerseits von dem Risiko ab, das vom EUC ausgeht und andererseits vom tolerierbaren Risiko.

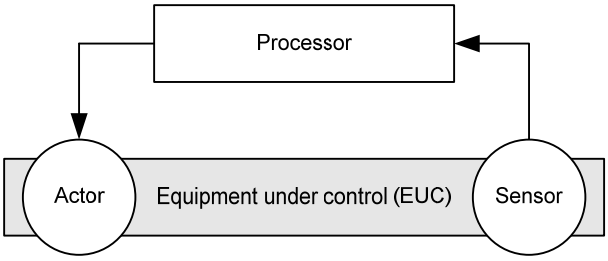

Abbildung 8 Funktionssicherheitssystem

Steht der Motor in dem angesprochenen separaten Gebäude, kann kein großer Schaden entstehen, es wird ein niedriges Safety Integrity Level gefordert, z.B. SIL 1. Ist der zu erwartende Schaden größer wird ein entsprechendes höheres SIL gewählt. Dies wird **mittels einer Risikoanalyse ermittelt**. Wie eine solche Überhitzung entstehen kann und wie man das geforderte SIL erreichen kann wird durch den Hersteller **in einer Ursachenanalyse (oder Gefährdungsanalyse) ermittelt**.

(20) beschreibt ein sicherheitsbezogenes System nach IEC/EN 61508 *als ein System das alles (Hardware, Software, menschliche Faktoren) einschließt was zur Ausführung eines oder mehrerer Sicherheitsfunktionen benötigt wird*. Der **Ausfall eines sicherheitsbezogenen Systems** würde eine **signifikante Zunahme des Sicherheitsrisikos** für Mensch und Umwelt bedeuten.

Für eine bestimmte sicherheitsrelevante Funktion wird das **geforderte SIL** bestimmt. Es dürfen dann nur Systeme zur Erfüllung dieser Funktion herangezogen werden, die **mindestens dieses SIL erfüllen**. Dabei gilt die geforderte Safety Integrety für das gesamte sicherheitsbezogene System. Die Bestandteile müssen entsprechend ausgelegt sein.

Für Hardware ist das Ausfallverhalten charakterisiert durch **Alterserscheinungen wie Verschleiß**. Es werden ausschließlich zufällige Fehler angenommen. Sind die Ausfallcharakteristika der verwendeten Komponenten hinreichend bekannt, kann die Ausfallwahrscheinlichkeit der Hardware ermittelt werden.

Software hingegen altert nicht. Zufällige Fehler treten nicht auf. **Programmierfehler** sind in einem Softwareprojekt ab einer bestimmten Größe unvermeid-

bar. Diese Fehler werden systematische Fehler genannt und sie treten bei gleichen Voraussetzungen immer auf. Diese Fehler **können mit stochastischen Mitteln nicht erfasst werden**. Man gibt für ein bestimmtes SIL qualitätssichernde Verfahren vor. Werden diese korrekt umgesetzt so kann mit hinreichendem Vertrauen davon ausgegangen werden, dass ein entsprechendes SIL erfüllt wird. Die Aussage SILn-Software ist nach (20) eine Kurzform für: „*Software entwickelt unter Verwendung angemessener Techniken und Maßnahmen, die sicherstellen, dass die Software die Anforderungen an systematische Ausfälle einer bestimmten Sicherheitsfunktion X für SILn erfüllt*"

Weiterhin **müssen die Menschen mit betrachtet werden, die in dem betreffenden Funktionssicherheitssystem mitwirken**. Der Mensch kann hier eindeutig als **Schwachstelle mit hoher Fehlerrate** identifiziert werden und sollte an sicherheitsrelevanten Funktionen nicht beteiligt sein. Manchmal ist dies jedoch unvermeidlich. Es müssen dann Maßnahmen zur Fehlerreduktion getroffen werden. Ein Beispiel ist das Kf-Verfahren zur Durchführung von sicherheitsrelevanten Bedienungen bei ESTW, worauf im nächsten Kapitel eingegangen wird.

Ebenfalls in (20) heißt es: „***Das SIL eines Teilsystems bestimmt das höchste SIL das für eine Sicherheitsfunktion*** *unter Verwendung dieses Teilsystems verwendet werden kann.*" Was aber nicht den Umkehrschluss zulässt: ein System hat nicht automatisch SILn weil alle Komponenten für die Verwendung in SILn zugelassen sind.

2.4 Menschen unter Sicherheitsverantwortung

Es wurde festgestellt, dass die unsichersten unter Sicherheitsverantwortung stehenden Subsysteme für die Gesamtsicherheit maßgebend sind. Dass der unter Sicherheitsverantwortung stehende Mensch hier eine Schwachstelle darstellt soll nun diskutiert werden. Es steht dabei die Vermutung im Vordergrund, dass die Sicherheit des Kf-Verfahrens bei der Eingabesicherung überschätzt wird.

Die **Zuverlässigkeit des Menschen** unter Sicherheitsverantwortung sei laut (21) **äußerst begrenzt**. Es kann nach (21) sogar festgestellt werden, dass völlig fehlerfreie Handlungen praktisch nicht auftreten und hohe Sicherheitsanforderungen (Zuverlässigkeit des Gesamtsystems) nur durch **fehlertolerante Gestaltung des Mensch-Maschine Systems** erreicht werden können. Oft wird auf die Berücksichtigung des menschlichen Faktors aufgrund der schwierigen Quantifizierbarkeit des Problems verzichtet. Dabei wird unter bestimmten Bedingungen **die berechnete technische Zuverlässigkeit praktisch bedeutungslos** (21). Für eine Betrachtung über Bedienplatzsysteme im Eisenbahnbereich ist eine Betrachtung des Menschen unter Sicherheitsverantwortung unerlässlich.

Maßgeblich beeinflussen die Arbeitsbedingungen und das Aktivierungspotential (Stress) der entsprechenden Person die Fehlerwahrscheinlichkeit. Jedoch sind auch unter idealen Bedingungen menschliche Fehler derart häufig, dass Sicherheitsverantwortung möglichst vermieden werden sollte, was nicht immer möglich aber auch nicht immer gewollt ist, da **bei Betriebsstörungen der Mensch die Verfügbarkeit des Systems positiv beeinflussen kann**. Tabelle 2 listet Fehlerwahrscheinlichkeiten auf, wie sie vom Eisenbahnbundesamt zugrunde gelegt werden (22).

Tabelle 2 Fehlerwahrscheinlichkeit nach Hinzen

Handlungsebene	Fehlerwahrscheinlichkeit/ Bedienhandlung
Fertigkeitsbasiert	$1 * 10^{-3}$
Regelbasiert	$1 * 10^{-2}$
Wissensbasiert	$1 * 10^{-1}$

Es wird in Handlungsebenen unterschieden. Eine Einführung in die Handlungsebenen des Menschen unter Sicherheitsverantwortung bieten ebenfalls (22) sowie Anders in (23). Auf der **fertigkeitsbasierten Ebene ist mit Leichtsinnsfehlern** zu rechnen. Die Handlungen des Bedieners sind automatisiert, ein aktives Nachdenken ist nicht nötig. Die Fehler werden als Schnitzer (Gedächtnisfehler) und Patzer (Aufmerksamkeitsfehler) bezeichnet.

Bei regel- und wissensbasierten Fehlern handelt es sich vor allem um falsche Schlussfolgerungen. In der regelbasierten Ebene wird unter Anwendung von Regeln gearbeitet. Dabei kann eine **gute Regel falsch angewendet** werden oder eine **schlechte Regel richtig angewendet** werden. Fehler in der wissensbasierten Ebene sind vielfältig. Es wird angenommen, dass die wissensbasierte Ebene im Bereich der Stellwerksbedienung aufgrund guter Ausbildung des Personals nicht vorkommt. Ebenfalls werden Verstöße aus der Betrachtung ausgeklammert.

Annahme 2: Der Bediener eines ESTW für regionale Strecken arbeitet überwiegend in der fertigkeitsbasierten Ebene. In die regelbasierte Ebene fällt er nur in Ausnahmefällen, die wissensbasierte Ebene wird ausgeschlossen.

Der Ablauf einer Bedienhandlung im Störungsfall soll im Folgenden näher betrachtet werden. Abbildung 9 zeigt das Modell für Mensch-Technik Interaktion aus (21) in abgewandelter Form. Dabei wurden jeweils zwei Ebenen zusammengefasst und an den Fall der Hilfshandlung bei ESTW angepasst.

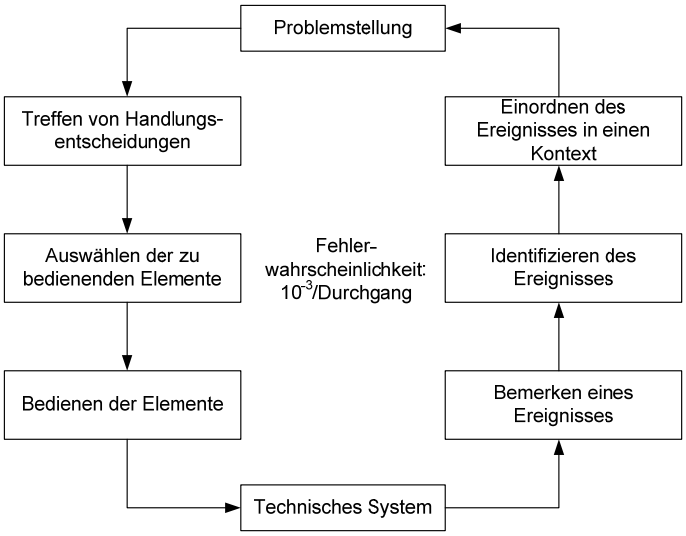

Abbildung 9 Ebenenmodell für Mensch-Technik Interaktion

Jeder der Einzelschritte ist mit einer Fehlerwahrscheinlichkeit derart behaftet, dass der Gesamtprozess die Hinzensche Fehlerwahrscheinlichkeit von 10^{-3} ergibt: $10^{-3}/6$.

- Das **Bemerken eines Ereignisses,** das auf dem Meldebild zur Anzeige kommt, also beispielsweise das Auftreten einer Störung, soll derart definiert sein, dass es bemerkt wird bevor eine aufgrund des Fehlers unzulässige Bedienung durchgeführt wird. (Störungsmeldung: Weiche erreicht keine Endlage, unzulässige Bedienung: Fahrstraße einstellen.)
- Die **Identifikation des Ereignisses** ist die korrekte Zuordnung eines Anzeigezustands zu dessen Bedeutung. (Stellungsmelder blinkt rot, der Weichenlaufmelder ist dunkel: Die Weiche hat die Endlage nicht erreicht.)
- Durch das **Einordnen in den Kontext** wird sich der Bediener der Tragweite und der betrieblichen Bedeutung des Ereignisses bewusst. (Die gestörte Weiche kann nicht mehr befahren werden.)
- **Handlungsentscheidungen** können betrieblicher Art oder Bedienungshandlungen am Stellwerk sein, meistens eine Kombination davon. (Durch einen erneuten Umstellversuch kann der Grundzustand wieder hergestellt werden, wenn die Fehlerursache nur vorübergehend bestand)
- Das **Auswählen der zu bedienenden Elemente** bezieht sich auf eine Stellwerksbedienung, gilt aber auch für betriebliche Handlungen. (Das Kontextmenü muss geöffnet werden und der Weichenstellbefehl WU ausgewählt werden.)
- Beim **Bedienen der Elemente** werden die entsprechend geplanten Aktionen durchgeführt.

- **Die Ergebniskontrolle** resultiert in einem erneuten Durchlauf des Prozesses (z.B. Störung nicht beseitigt).

Es sollen im Folgenden die **Regeln der Redundanz** aus Kapitel 2.2.1 herangezogen werden um Betrachtungen zur Steigerung der Toleranz gegenüber menschlichen Fehlhandlungen anzustellen.

Systematische Redundanz (Hardwareredundanz) entspricht dem Einbinden von zwei Personen. Diese müssen den Prozess unabhängig voneinander durchführen. Man könnte sich das **Einbeziehen eines zweiten Bedieners** vorstellen, der für einen anderen Bereich zuständig ist und dem bei Vorliegen einer Fehlermeldung das Bild aufgeschaltet wird. Er muss nun zum gleichen Ergebnis kommen wie der eigentliche Bediener. Sind die beiden Bediener auch räumlich getrennt, so kann von einer völligen Unabhängigkeit ausgegangen werden. Mit Abstrichen ist dies auch durch Einbeziehung des betreffenden Lokführers möglich. Dieser verfügt weder über das gleiche Fachwissen noch kann er über die Umstände eines Ereignisses in vollem Maße in Kenntnis gesetzt werden. Aber es ist immerhin eine Entscheidungskontrolle möglich.

Einer **Informationsredundanz** würde das wiederholte Durchlaufen der **Entscheidungsfindung durch denselben Bediener** entsprechen. Die zweite Entscheidungsfindung muss jedoch diversitär ablaufen, da die erste Entscheidungsfindung noch präsent ist und automatisch herangezogen werden würde. Um auch den Verarbeitungsprozess in die Redundanz mit einzubeziehen, muss diese spätestens mit dem Erkennen der Störung einsetzen, d.h. alle Schritte müssen ab da ein zweites Mal durchlaufen werden. Bei gängigen Verfahren werden jedoch nur die nachgelagerten Schritte redundant ausgeführt.

Es sollen nun die **vorhandenen Redundanzen identifiziert werden**, wie sie beim bei der DBAG üblichen Bedienplatz unter Anwendung des Kf-Verfahrens[7] vorhanden sind.

[7] Das Kf-Verfahren wird in Kapitel 3.2.1 erklärt

- Beim **Erkennen des Fehlers**: Fehlerminderungsfaktor ist hier ein **akustisches Signal** das den Bediener auf das Vorliegen eines Fehlers aufmerksam macht. (Faktor 0,01)
- Beim **Identifizieren des Fehlers**: Ein Fehlerminderungsfaktor ist hier der **Störungssammelmelder**, der anzeigt in welcher Elementgruppe der Fehler vorliegt, außerdem die alphanumerische Fehleranzeige. Da es sich bei beiden um optische Anzeigen handelt, wird die Wirkung als relativ gering eingeschätzt. (Faktor 0,5)
- **Einordnen des Fehlers** und **Treffen von Handlungsentscheidungen**: Für diese Schritte wurden **keine eigenen Fehlerminderungsfaktoren** identifiziert. Jedoch wirkt sich das selektiv eingeschränkte Anbieten von Befehlen fehlermindernd aus. Dies wirkt sich jedoch auf alle Fehler aus so, so dass der Faktor erst zur Gesamtfehlerrate multipliziert wird.
- **Handlungsschritte planen und durchführen**: Hier greift das Kf-Verfahren. Der eingegebene Befehl gelangt erst zur Ausführung wenn die Kf 1 Taste, gefolgt von der Kf 2 Taste betätigt wurde. Aufgrund des oben beschriebenen Automatismus der dem Verfahren zueigen ist, kann keine stochastische Unabhängigkeit angenommen werden. (Faktor 0,01)
- Der Fehlerwahrscheinlichkeit des Gesamtprozesses wird ein Fehlerreduktionsfaktor von 0,5 multipliziert um die Fehleroffenbarung durch selektives Anbieten von Befehlen zu berücksichtigen.

Die Einbeziehung der Reduktionsfaktoren ist in Tabelle 3 dargestellt.

Tabelle 3 Fehlerwahrscheinlichkeit Mensch-Technik Interaktion mit dem Kf-Verfahren

Ebene	Fehler-wkt.	Minderungsgründe beim Kf-Verfahren	Minderungs-faktor	Ges. Fehlerwkt.
Erkennen	$1{,}7*10^{-4}$	Gleichzeitig Akustischer Alarm	0,01	$1{,}7*10^{-6}$
Identifizieren	$1{,}7*10^{-4}$	Gleichzeitig Störungssammelmelder	0,5	$8{,}3*10^{-5}$
Einordnen	$1{,}7*10^{-4}$	Keine	1	$1{,}7*10^{-4}$
Handlungsentscheidungen	$1{,}7*10^{-4}$	Keine	1	$1{,}7*10^{-4}$
Handlungsschritte	$1{,}7*10^{-4}$	Befehl muss über Kf1 und Kf2 bestätigt werden	0,01	$1{,}7*10^{-6}$
Handlungsdurchführung	$1{,}7*10^{-4}$	Befehl muss über Kf1 und Kf2 bestätigt werden	0,01	$1{,}7*10^{-6}$
Zwischensumme:				$4{,}2*10^{-4}$
Fehlerreduktion durch situativ eingeschränkten Befehlsvorrat:				0,5

Gesamt:	**$1{,}0*10^{-3}$**	**$2{,}1*10^{-4}$**

Es ist zu beachten, dass die gewählten Fehlerreduktionsfaktoren **als absolute Zahlenwerte keinerlei Aussagewert** besitzen, da sie einer Schätzung des Autors entstammen. Vielmehr sollen sie die Schwachpunkte des Kf-Verfahrens aufdecken und das Vorschlagen von Verbesserungen ermöglichen.

Bei der in Tabelle 2 aufgeführten Fehlerwahrscheinlichkeit von $\frac{10^{-3}}{Bedienung}$ wird von optimalen Arbeitsbedingungen ausgegangen. Nach den Regeln der Wahrscheinlichkeitsrechnung, kann man **unabhängige Ereignisse multiplizieren**. Zwei unabhängige Eingaben mit gleichem Ziel würde also zu einer Fehlerwahrscheinlichkeit von $\frac{10^{-3}}{Bedienung} * \frac{10^{-3}}{Bedienung} = \frac{10^{-6}}{Bedienung}$ führen. **Beim üblichen Kf-Verfahren ist dies jedoch eindeutig nicht der Fall**. Zum einen da das Verfahren nicht alle Prozessschritte abdeckt, zum anderen, da das Verfahren bei den Teilprozessen bei denen es greift ebenfalls keine stochastische Unabhängigkeit aufweist. Letzteres soll an folgendem Beispiel verdeutlicht werden.

Bei Anwendungen des Betriebssystems Windows wird vor dem Schließen einer Anwendung noch einmal nachgefragt, ob die Anwendung wirklich geschlossen werden soll. Dies stellt ein Verfahren dar, durch welches Fehler durch ein erneutes Treffen der Entscheidung verringert werden sollen. Es kann oft beobachtet werden, dass **das Geben dieser Bestätigung zum Automatismus geworden ist**. Nach Abschluss des Verfahrens merkt der Benutzer, dass er das Programm fälschlicherweise geschlossen hat.

Diese automatischen Handlungsabläufe sind eine typische Beobachtung bei Handlungen auf der Fertigkeitsebene. Es wird daher angenommen, dass Handlungen, die automatische Handlungsabläufe ermöglichen, nicht stochastisch unabhängig sind. **Ein Fehler bei der Initialen Handlung erhöht die Fehlerwahrscheinlichkeit der Folgebedienungen**.

Nicht abgedeckt durch das Verfahren werden die beiden Punkte, die man auch als **Verarbeitungsprozess im menschlichen Gehirn** ansehen könnte, das Einordnen des Fehlers in den Gesamtzusammenhang und das Ableiten von

Maßnahmen. Die Fehlerwahrscheinlichkeit könnte also wesentlich gesenkt werden, wenn diese beiden Punkte eine Redundanz erfahren. Der Grund für die geringe Kontrolle des Verarbeitungsprozess liegt daran, dass der Prozess ausschließlich im menschlichen Gehirn stattfindet. Eine **technische Kontrolle ist daher nicht ohne weiteres möglich**. Die Redundanz des Verarbeitungsprozesses kann durch eine **zweite eingebundene Person** erreicht werden, die idealerweise die Entscheidung unabhängig trifft, zumindest jedoch die Entscheidung des Bedieners verifiziert.

These 5: Bei Anwendung des Kf-Verfahren werden wesentliche Teile der Entscheidungsfindung nicht mit Redundanz versehen. Von einer unabhängigen zweiten Entscheidungsfindung kann daher nicht ausgegangen werden.

Als Konsequenz werden Fehlerwahrscheinlichkeiten nach Tabelle 4 für Kombinierte Bedienungen angenommen.

Annahme 3: Die Fehlerwahrscheinlichkeit des Menschen beträgt unter idealen Bedingungen 10-3/ Bedienung. Beim Kf Verfahren mindestens 10-4/ Bedienung.

Tabelle 4 Annahmen zu Fehlerwahrscheinlichkeiten kombinierter Bedienungen

Verknüpfung von zwei Bedienungen	Fehlerwahrscheinlichkeit/ Bedienhandlung
Kf-Verfahren	$1 * 10^{-4}$
Zwei verschiedene Personen entscheiden	$1 * 10^{-5}$
Theoretischer Maximalwert	$1 * 10^{-6}$

Es wurde veranschaulicht, jedoch nicht bewiesen, dass das Kf-Verfahren nicht das Herbeiführen von zwei unabhängigen Entscheidungen unterstützt. Es muss daher angenommen werden, dass die erneute Entscheidung nicht stochastisch unabhängig von der ersten ist. Jedoch finden sich in diesem Bereich keine einschlägigen Studien, die dies belegen oder widerlegen. Unter Anwendung des Kf-Verfahrens wird in vielen Rückfallebenen durch den Bediener Sicherheits-

verantwortung übernommen. Dies soll im nächsten Kapitel verdeutlicht werden.

2.5 Betriebliche und Technische Rückfallebenen

Mit Blick auf die im Kapitel zur Redundanz getroffenen Aussagen soll sich nun dem Thema der betrieblichen Rückfallebenen genähert werden. Da auch bei hochverfügbaren Systemen **mit Störungen gerechnet werden** muss, sind **Rückfallebenen notwendig**. Nach der Definition des Begriffs werden anhand von Beispielen die verschiedenen Formen von Rückfallebenen beschrieben.

Als Rückfallebene wird ein definierter Betriebszustand genannt, der nicht die Regelebene ist. Der Begriff Regelebene impliziert schon deren Bedeutung *der vollen Funktion aller am Bahnbetrieb beteiligten technischen Systeme aber auch der Personale*.

Die **Rückfallebenen unterscheiden sich von der Regelebene** durch **Verfügbarkeit** (eingeschränkte Leistungsfähigkeit bei gleichem Verkehrsaufkommen) **und Sicherheit**. Die letzte Rückfallebene ist im Bahnbereich immer der Stillstand. Um diesen totalen Verfügbarkeitseinbruch zu vermeiden gibt es Zwischenstufen wie in Abbildung 10 veranschaulicht.

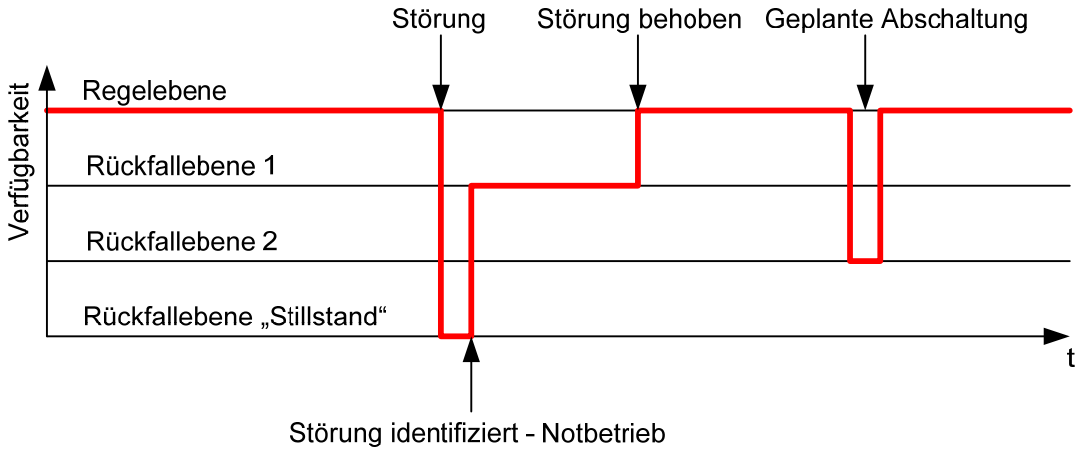

Abbildung 10 Prinzip der Rückfallebenen

Fällt eine technische Komponente aus oder kann sie aus betrieblichen Gründen nicht benutzt werden, so muss diese entweder durch vorgehaltene Redundanz oder betriebliche Maßnahmen ersetzt werden. Oft besteht die Rückfallebene aus Kombinationen. Drei Beispiele sollen dies verdeutlichen:

Eine **technische Redundanz** wird beim **Anschluss von Unterzentralen an Betriebszentralen** eingebaut. Ist die Vorzugsleitung nicht verfügbar, so wird auf eine Ersatzleitung umgeschaltet. Ist durch einen zweiten Fehler die redundante Verbindung ebenfalls ausgefallen, so kann die Zuglenkung der Unterzentrale den Verkehr für 30 Minuten derart aufrecht erhalten, als dass diese den eingespeicherten Zuglenkplan abarbeitet. In dieser Zeit kann der Notbedienplatz der Uz mit Personal besetzt werden, das mit dem Fahrdienstleiter fernmündlich in Kontakt steht und dessen Anweisungen ausführt. Die beschriebene Struktur ist in Abbildung 11 veranschaulicht. **Sowohl bei der Ersatzleitung als auch beim Notbedienplatz handelt es sich um strukturelle (technische) Redundanz im Kaltbetrieb**. Das bedeutet, dass sie der Verfügbarkeitssteigerung dienen. Das Umschalten auf die redundante Leitung erfolgt ohne großen Zeitverlust, während **das Besetzten des Notbedienplatzes einige Zeit in Anspruch nimmt**. Diese Zeit wird durch die Zuglenkung überbrückt. Vergleichbar ist dies mit dem Anlaufen eines Notstromgenerators bei Netzausfall. Um die benötigte Zeit zu überbrücken werden Batterien verwendet.

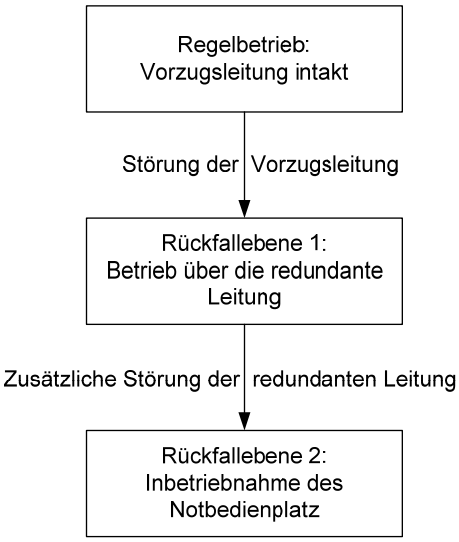

Abbildung 11 Rückfallebene Datenübertragung

Eine **betriebliche Rückfallebene** stellt die in (24) diskutierte **Räumungsprüfung** dar, welche bei gestörtem selbsttätigem Streckenblock eingeführt wird. Ein Zug darf nur in einen Blockabschnitt eingelassen werden, wenn dieser frei ist und der vorausgefahrene Zug durch ein Signal gedeckt ist (Blockbedingungen). Ist die Technik gestört, müssen diese Bedingungen betrieblich sicher gestellt werden. Die Signaldeckung kann nur über das Meldebild festgestellt werden, bei der Prüfung des Freiseins verlässt man sich darauf jedoch nicht. **Bei der Räumungsprüfung muss die Vollständigkeit des vorausfahrenden Zuges durch Hinsehen festgestellt werden**. Dazu holt der Fahrdienstleiter von einem örtlichen Mitarbeiter eine Zugschlussmeldung ein. Ist die Räumungsprüfung nicht möglich, weil die Zugfahrt schon vor längerer Zeit stattgefunden hat oder weil kein örtlicher Mitarbeiter vorhanden ist, so muss dem Lokführer der Auftrag zum Fahren auf Sicht gegeben werden. Dies stellt eine weitere Rückfallebene dar, siehe Abbildung 12.

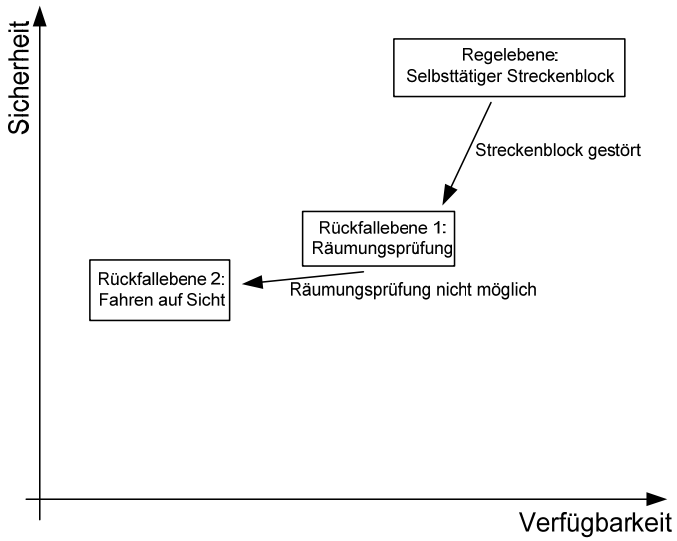

Abbildung 12 Rückfallebenen bei Blockstörung

Eine Kombination **von technischer und betrieblicher Rückfallebene** stellt das **hilfsweise Einstellen von Zugfahrstraßen** dar. Dazu soll zuerst die Regelebene betrachtet werden, siehe hierzu auch (25).

(26) nennt im Regelwerk (3) die entsprechenden Module 408.0231 – Fahrweg prüfen, 408.0232 – Fahrweg sichern, 408.0233 – Fahrweg prüfen und sichern, Mitarbeiter, Melden, Nachweis sowie 408.0261 – Zugfahrten durchführen. Diese Regeln sind immer einzuhalten.

In der Regelebene wird durch Start-Ziel Bedienung eine Fahrstraße ausgewählt. Diese wird markiert und durch den Bediener kontrolliert. Dann wird der Bildungsprozess durch das Betätigen der Schaltfläche „Verarbeiten“ angestoßen. Die Fahrstraße wird dann vollautomatisch gebildet.

Als erstes wird eine einmalige Zulässigkeitsprüfung durchgeführt. Der Stellbefehl wird erst auf formale Fehler überprüft und dann auf Zulässigkeit aus sicherungstechnischer Sicht. Anschließend werden die Weichen in der richtigen Lage verschlossen. Ist dies alles geschehen, läuft die Fahrstraßenüberwachung an. Diese überwacht kontinuierlich den einmal erreichten Sicherungsstand. Sie kennt zwei Sicherungsstufen welche durch den Fahrstraßenüberwachungsmelder (Füm) dargestellt angezeigt werden.

Die Zulässigkeitsprüfung überprüft vom Start- bis zum Zielelement und den D-Weg auf folgende Punkte:

- Das Fahrstraßenziel ist aufgelöst (Zfm[8] ist in Grundstellung)
- Es sind keine der benötigten Weichen
  - In anderen Fahrstraßen verschlossen
  - In der Nicht-Solllage gesperrt
- Für kein benötigtes Fahrwegelement ist eine Befahrbarkeitssperre gespeichert (außer bei entsprechender Vorbedienung)
- In keiner Schlüsselsperre an der Fahrstraße der Schlüssel freigegeben ist.

Sind diese Bedingungen erfüllt, wird **das Fahrstraßenband dargestellt** d.h. die Fahrwegelemente grün dargestellt (bei besetzten Elementen rot) und dadurch als verwendet markiert. **Die Weichen laufen** durch die Weichenlaufkette (Wlk) initiiert, **in die Solllage** um und werden **einzeln verschlossen**.

Die Weiche darf dazu:

- Nicht verschlossen oder gesperrt sein
- Nicht als belegt gemeldet sein
- Nicht aufgefahren sein.
- Die Wlk darf nicht gesperrt sein

In diesem Stadium **läuft die Fahrstraßenüberwachung an**. Die überwachten Funktionen der beiden Stufen sind in Tabelle 5 zusammen gestellt.

Tabelle 5 Technische Sicherung der Fahrstraßen

Füm zeigt:	Ruhelicht	Blinklicht
Weichen im Fahrweg sind in der richtigen Lage verschlossen	ja	ja
Alle Schlüssel für handbediente Weichen im Fahrweg sind eingeschlossen	ja	ja
Die Gleisfreimeldeanlage meldet den Fahrweg, den D-Weg und den Flankenschutzraum frei.	ja	nein
Fahrweg und D-Weg erhalten Flankenschutz	ja	nein

[8] Zielfestlegemelder

Die Haltprüfung am Zielsignal ist positiv verlaufen[9]	ja	nein
Sperrsignale, Hauptsignale und Zusatzanzeiger innerhalb der Fahrstraße zeigen den geplanten Begriff	ja	nein

Nur wenn der **Fahrstraßensicherungsvorgang vollständig** durchlaufen ist, kann **das entsprechende Signal die Fahrtstellung einnehmen**. Um Zugfahrten auch bei Störungen oder anderen Hinderungsgründen zulassen zu können, ist als **Rückfallebene das Ersatzsignal Zs 1**[10] mit dem Befehl EE1 oder EE2 vorgesehen. Genau genommen stellt der Befehl EE2 eine Rückfallebene des Befehls EE1 dar. Eine weitere Rückfallebene ist das Zulassen der Fahrt mit schriftlichem Befehl.

Das Ersatzsignal kann mit dem **Befehl EE1** bei vorhandener Fahrstraßenüberwachung gestellt werden, d.h. der Füm muss entweder Ruhelicht oder mindestens Blinklicht zeigen. Streng genommen handelt es sich hier also ebenfalls um zwei Rückfallebenen. Das betriebliche **Sichern der Fahrstraßenbestandteile,** die nicht überwacht werden, **liegt in der Verantwortung des Bedieners**.

Voraussetzung für das Bedienen des Ersatzsignals mit dem **Befehl EE2** ist nur die abgeschaltete Weichenlaufkette. Das betriebliche **Sichern der gesamten Fahrstraße liegt in der Verantwortung des Bedieners**. Dies gilt ebenfalls bei Ausstellen des schriftlichen Befehls.

Eine weitere Rückfallebene wurde mit der **Funktion FPÜ** geschaffen. Sie ist zwischen Füm-Ruhelicht und Füm blinkend einzuordnen. Hat eine Fahrstraße den Sicherungsstand Füm blinkend erreicht, so können mit FPÜ die Hinderungsgründe zum Erreichen des Zustands Füm-Ruhelicht angezeigt werden. Unter **hilfsweiser Umgehung** der entsprechenden Elemente kann der Zustand Füm-Ruhelicht erreicht werden. Das umgangene Element muss dann **hilfs-**

[9] Der zuletzt am Zielsignal gestartete Zug wurde durch das haltzeigende Zielsignal gedeckt. Außerdem darf nicht Sh1 oder Zs1 oder ein anderes Zusatzsignal anzeigen oder es störungsmäßig dunkel sein.

[10] Das Ersatzsignal wird hier stellvertretend auch für das Vorsichtssignal Zs 7/Zs 11(=Ersatzsignal + Auftrag zum Fahren auf Sicht) und das Falschfahrauftragssignal Zs 8 (=Ersatzsignal + Auftrag zur Fahrt auf dem Gegengleis) besprochen.

weise gesichert werden. Während beim Zustand Füm-blinkend alle nicht überwachten Elemente hilfsweise gesichert werden müssen, ist dies bei Anwendung von FPÜ nur für die tatsächlich ursächlichen Elemente erforderlich. Dies stellt einen erheblichen Sicherheitsgewinn dar.

Sobald eine der für Füm-Ruhelicht erforderlichen Bedingungen nicht mehr vorliegt **fällt das die Fahrstraße deckende Signal auf Halt**. Dies gilt sowohl für den beabsichtigten Haltfall als auch für nicht beabsichtigte Ursachen (z.B. kann versehentliches Kurzschließen eines Gleisstromkreises zum Haltfall zur Unzeit führen). Das **Auflösen der Zugfahrstraße erfolgt zugbewirkt**. Die Elemente werden einzeln aufgelöst wenn sie und die umliegenden Elemente in logischer Abfolge belegt waren.

Abbildung 13 ordnet die verschiedenen Rückfallebenen in das Verfügbarkeits-Sicherheitsdiagramm ein

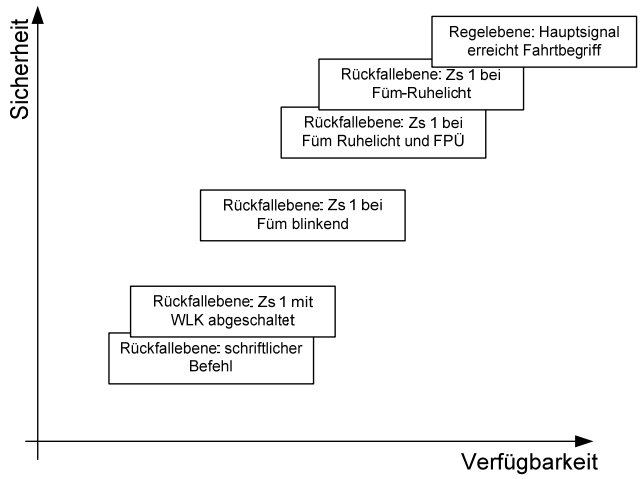

Abbildung 13 Rückfallebene Zulassen von Zugfahrten

Es wurden Beispiele für Rückfallebenen betrachtet. Die technische Realisierung von Rückfallebenen wurde anhand von Notbedienplätzen erläutert. Die betrieblichen Rückfallebenen wurden anhand der Räumungsprüfung bei gestörtem Streckenblock erläutert. Das Beispiel für ein Zusammenspiel von betriebli-

chen und technischen Rückfallebenen war die hilfsweise Zulassung einer Zugfahrt. Es konnte festgestellt werden, dass bei Letzterem mehrere Ebenen zur Verfügung stehen, jeweils mit unterschiedlicher Verfügbarkeit und Sicherheit. Dabei wurde betont, dass die Funktion FPÜ wesentlich zur Sicherheit dieser Rückfallebenen beitragen kann.

3 Anforderungen an Bedienplätze für ESTW

Es sollen in diesem Teil der Arbeit die Anforderungen erarbeitet werden, die ein zulassungsfähiger Bedienplatz erfüllen muss. Dabei werden, gefolgt von Begriffsdefinitionen und der Erläuterung grundlegender Zusammenhänge, die gegenwärtig verwendeten Bedienplatzsysteme vorgestellt und bewertet. Es folgt eine Diskussion über die Zulassung von Sicherungstechnik im Allgemeinen und Bedienplatzsystemen im Besonderen. Dabei wird auch auf die Ergebnisse der Risikoanalyse ESTW eingegangen, die dem Autor nicht vorliegt. Im letzten Kapitel dieses Teils werden die betrieblichen Forderungen an Bedienplatzsysteme analysiert. Abschließend wird noch auf betriebliche Paradigmen anderer Bahnen an den Beispielen der österreichischen ÖBB und dem schwedischen Banverket eingegangen.

3.1 Definitionen und Grundlagen

Ein als sicher geltender Bedienplatz verfügt über:

- Eine **gesicherte Bedienplatzanzeige**. Diese muss sicherstellen, dass der Bediener in bestimmten Situationen mit der notwendigen Sicherheit die tatsächlichen Zustände der Außenanlagen angezeigt bekommt.
- Die **gesicherte Befehlseingabe** für sicherheitskritische Befehle, welche dafür sorgen soll, dass nur die richtigen Befehle zur Ausführung kommen.
- Eine **gesicherte Datenübertragung** vom Bedienplatz zum Stellwerk und umgekehrt, welche die Datenintegrität sicherstellt.

Man kann unterscheiden zwischen **technischen Methoden** und **verfahrensbasierten Methoden** zur Herstellung der Sicherheit. Je nach Blickwinkel werden die Begriffe unterschiedlich erklärt:

Technik orientierte Definition:

- Unter der verfahrensbasierten Sicherung wird das Programmieren fehlertolerierender Anwendersoftware verstanden, also die Verwendung von funktioneller Redundanz und Informationsredundanz. Hingegen können Standardhardware und Betriebssysteme verwendet werden.

- Technikbasierte Sicherung bedeutet für den Informatiker die Verwendung von spezieller Hardware und Betriebssystem und Standardanwendungen. Die Fehlerreaktionen erfolgen durch Hardware und Betriebssystem, also mittels struktureller Redundanz.

Betrieblich orientierte Definition:

- Der betriebsorientierte Anwender versteht unter einer Verfahrenssicherung die Einbindung des Bedieners in den Sicherungsvorgang, dieser muss eine vorgegebene Handlungskette abarbeiten.
- Unter technikbasierter Sicherung versteht der Bediener die vor dem Anwender verborgene Sicherung der Vorgänge.

Folgende Begriffe werden in dieser Arbeit verwendet:

- Die **technikbasierte Sicherung** des Informatikers,
- Die **verfahrensbasierte Sicherung** des betriebsorientierte Anwenders,
- **Technisch-verfahrensbasierte Sicherung** soll die Verfahrenssicherung darstellen, wie sie der Informatiker versteht.

Im Sinne dieser Arbeit ist davon auszugehen, dass die Sicherungsebene des Stellwerks den Zustand der Außenanlage fehlerfrei ausgibt und keine unzulässigen Befehle des Bedieners zulässt. Es gibt jedoch **Situationen in denen die Sicherungsebene umgangen werden muss** und der Bediener direkt auf die Elemente zugreift. Dies sind:

- die Rücknahme von Regelbedienungen (Bsp. Fahrstraßenhilfsauflösung)
- Störungen (Bsp. Achszählgrundstellung)
- aber auch Manipulationen an der Sicherungsebene selbst (Bsp. Rücknahme einer Befahrbarkeitssperre).

In diesen Fällen kann die Sicherungsebene die Handlungen des Bedieners nicht kontrollieren, die Sicherheitsverantwortung für die durchzuführende Bedienung wird vom Bediener übernommen. Wie aus dem erweiterten Regelkreis der Sicherungstechnik[11] in Abbildung 15 hervorgeht, kann eine **richtige Entschei-**

[11] Adaptiert aus (48)

dung nur auf Basis einer richtigen Datengrundlage hervorgehen. Der Bediener muss sich in diesem Fall auf die Richtigkeit der Anzeige verlassen können. Was dies bedeutet wird im Verlauf dieser Arbeit zu klären sein.

<table>
<tr><td colspan="2">Kf-Pflichtige Bedienung</td><td>Nicht Kf-Pflichtige Bedienung</td></tr>
<tr><td>Hilfsbedienung</td><td colspan="2">Regelbedienung</td></tr>
<tr><td>Hilfsbedienung</td><td>Kf-Pflichtige Regel-bedienug</td><td>Nicht Kf-Pflichtige Bedienung</td></tr>
</table>

Abbildung 14 Systematik der Bedienkommandos

Die Systematik der Bedienkommandos ist in Abbildung 14 dargestellt. Bedienkommandos bei denen die Sicherungsebene umgangen wird, werden Hilfsbedienungen genannt, von den RSTW auch als zählpflichtige Bedienhandlungen bekannt. Im ESTW sind diese Bedienungen eine Untermenge der Kf-Pflichtigen Befehle. Zusätzlich zu den Hilfsbedienungen sind Befehle Kf-Pflichtig, deren falsche Verwendung größere betriebliche Probleme entstehen lassen würden. Dies sind die Kf-Pflichtigen Regelbedienungen.

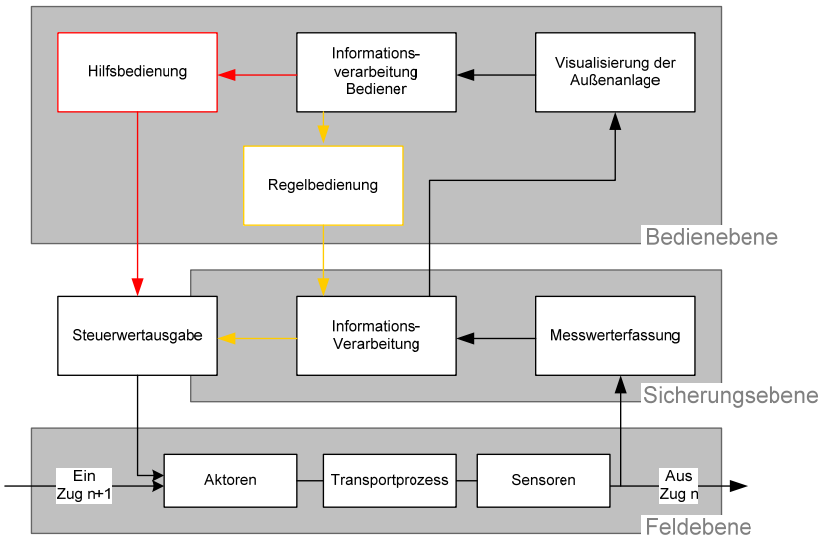

Abbildung 15 Erweiterter Regelkreis der Sicherungstechnik: Hilfsbedienung

Weiterhin wird das **Meldebild benötigt um das korrekte Umsetzen der Befehle zu beobachten**.

In diesem Kapitel sollen die **Anforderungen abgeleitet werden**, die den gebräuchlichen Bedienplätzen zugrunde liegen. Dazu werden verschiedene Systeme beschrieben und im Anschluss analysiert.

3.2 Beschreibung einiger Bedienplatzsysteme

3.2.1 Kommando-Freigabe Verfahren (Kf)

An dieser Stelle soll das **Kf-Verfahren kurz erläutert werden** um Redundanzen in den folgenden Abschnitten zu vermeiden. Das Verfahren dient der Sicherung von sicherheitsrelevanten Befehlsabgaben (27) und ist als Verfahrenssicherung mit Technikverfahrenssicherung realisiert. **Es soll verhindern**:

- **Eingabefehler** des Bedieners, die auf einem **Denkfehler** beruhen,
- Eingabefehler des Bedieners, die auf einem **falschen Meldebild** beruhen,
- dass **alte Befehle** zur Ausführung gelangen,
- dass der **Befehl falsch zur Ausführung** kommt.

Der eingegebene Befehl wird an die Sicherungsebene übertragen, dort als Kf-Befehl erkannt und an den Bedienplatz zurückgespiegelt und ausgegeben. Es wird eine Anzeigensicherung initiiert, die Anzeige befindet sich nun im sogenannten Kf-Modus. **Der Bediener ist angehalten, den ausgegebenen Befehl mit dem eingegebenen zu vergleichen** und sich außerdem nochmals zu vergewissern, dass es sich um das gewollte Kommando handelt. Ist das so, betätigt der Bediener die freigegebene Kf 1 Taste, nach drei Sekunden, die dem nochmaligen vergewissern dienen sollen, dann die Kf 2 Taste. Mit den Freigabetelegrammen der Kf Tasten werden **weitere Informationen übermittelt**:

- Um die Telegramme auf der Sicherungsebene zu authentifizieren, werden dort **Transaktionsnummern** (TAN) generiert und an den Bedienplatz gesendet. Diese werden dem Kf-Telegramm beigefügt und auf der Sicherungsebene mit den ursprünglichen Nummern verglichen.
- Die **Prüfsummen der Meldebildprüfungen** werden übertragen und auf der Sicherungsebene nochmals verglichen.
- Ein **Freigabecode**, der auf der Sicherungsebene die Zulässigkeit von Kf-Bedienungen bestätigt wird übermittelt. Dieser wird in den Bedienplatzrechnern einmalig generiert und bei Auftreten eines Fehlers im Anzeigesystem gelöscht.

Sind die Angaben durch die Sicherungsebene verifiziert worden, wird der Befehl ausgeführt.

3.2.2 Umschaltverfahren

Beim Umschaltverfahren wird das **Meldebild direkt im ESTW erzeugt**, zweikanalig bis zur Ausgabe des analogen Signals geführt und dort **durch einen Umschalter abwechselnd im Takt aufgeschaltet**. Das auch in Abbildung 16 dargestellte Verfahren wird darum Umschaltverfahren genannt und wird auch in (28) vorgestellt. Die Sicherung erfolgt ausschließlich mittels **struktureller Redundanz** und stellt darum eine technikbasierte Sicherung dar. Tritt ein Übertragungsfehler auf so wird angenommen, dass dieser nur in einem Kanal auftritt. Die Bilder stimmen dann bei der Ausgabe nicht überein und die falsch Übertragene Stelle blinkt im Umschalttakt. Bei diesem Verfahren werden nur **maximal zwei Lupenbilder** abgesichert. Das sichere System ist dabei **völlig unabhängig vom restlichen Bedienplatz**, wie beispielsweise den Bereichsübersichten. Zur Eingabesicherung kommt das oben beschriebene Kf-Verfahren zum Einsatz.

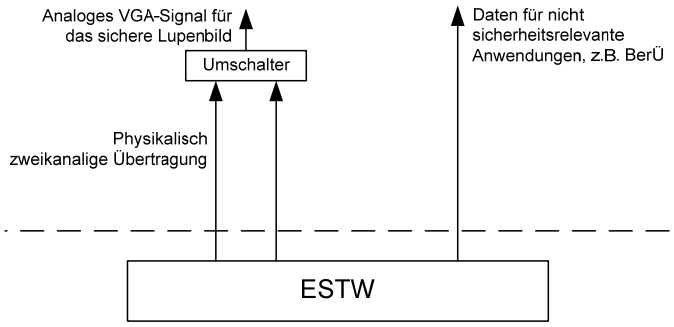

Abbildung 16 Prinzip Umschaltverfahren

Die **Kontrollanzeigen** wie in Abbildung 17 gezeigt (29), bestehen aus dem Umschaltmelder (U), dem Aktualitätsmelder (A), sowie dem Farbbalken.

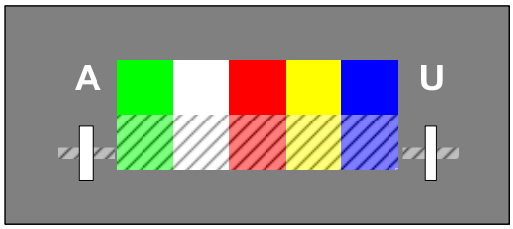

Abbildung 17 Kontrollanzeige Umschaltverfahren

Der **Umschaltmelder** dreht sich scheinbar im 90° Winkel, da das Signal des einen Rechners den Balken waagerecht einprogrammiert hat, der andere senkrecht. Bei jedem Umschaltvorgang wechselt die Anzeige. Der **Aktualitätsmelder** indiziert, dass alle empfangenen Telegramme verarbeitet wurden. Der **Farbbalken** demonstriert die Anzeigbarkeit der Farben sowie deren Fähigkeit zu Blinken.

Der große Nachteil war bei diesem System die benötigte spezielle Hardware und die damit einhergehende Inflexibilität. Das Lupenbild wurde innerhalb der Sicherungsebene des ESTW erzeugt und zweikanalig an den Bedienplatz übertragen, wo maximal zwei Lupen angesteuert werden konnten. Da das Verfahren **nicht mehr den Stand der Technik** repräsentiert, wird es nicht weiter betrachtet.

Das Umschaltverfahren wird heute nicht mehr eingebaut. Einerseits wollte man dem **Bedienpersonal die Verantwortung nehmen**, die Sicherheit der Anzeige festzustellen, andererseits gab es diverse **technische Probleme**, z.B. sollten die gleichen hochauflösenden Monitore zum Einsatz kommen wie für die Bereichsübersichten[12] um letztlich das **Lupensystem in das Bedienplatzsystem integrieren** zu können. Dadurch konnten **Übertragungskanäle gespart** werden, was entscheidend war für die Realisierung des Bz-Konzepts.

Die Firmen Siemens und Thales (ehemals Alcatel SEL) entwickelten unterschiedliche Lösungen. Beiden Weiterentwicklungen gemeinsam ist, dass die

[12] Durch die höhere Auflösung wäre es beim Umschaltverfahren zu aufwendig gewesen, die beiden Bilder zu synchronisieren, was ein unruhiges Bild zur Folge gehabt hätte.

Anzeigensicherung nun integriert im Anzeigesystem erfolgt, außerdem wird das sichere Meldebild nun nicht mehr im ESTW generiert sondern im Bedienplatz.

3.2.3 Einkanaliges Rückleseverfahren der Firma Siemens

Das Rückleseverfahren stellt eine Modifikation des Umschaltverfahrens dahingehend dar, dass **anstelle des Umschalters ein technischer Vergleich** stattfindet, der die Fehlerfreiheit der Anzeige elektronisch überwacht. Da die Anzeige nur als sicher gilt, wenn der Vergleich in einem sicheren Rechner durchgeführt wird, werden die Prüfwerte bei Bedarf **in die Sicherungsebene des ESTW zurückgelesen**.

Die einkanalige Übertragung wird über **Prüfsummen und laufende Nummern** realisiert. Dabei ist eine **Hammingdistanz von mindestens 6** gefordert (30). Im Gegensatz zu physikalisch zweikanaligen Verbindungen ist es bei einkanaligen Verbindungen **nicht ohne weiteres möglich, eine Unterbrechung zu offenbaren**. Zu diesem Zweck kommt ein „Ping“ zum Einsatz der von der Bedienebene an das ESTW gesendet wird um dort zurück an die Bedienebene übermittelt zu werden. Der „Ping“ muss innerhalb einer bestimmten Zeit (üblicherweise 3 Sekunden) am Ziel angekommen sein.

Die nachstehende Beschreibung erfolgt anhand des Bedienplatzsystems 901 der Firma Siemens, allerdings stellt **das Verfahren eine Art Standard** dar, das meistens Anwendung findet wenn eine gesicherte Anzeige gefordert wird. So streben scheinbar auch die Firmen Funkwerk (ehem. Vossloh) und Scheidt und Bachmann eine Anzeigensicherung nach diesem Verfahren an, die Firma Bombardier hat diese bereits realisiert und auch in Systemen der Firma Thales wurde das Prinzip bereits angewendet (31). Ein neues Produkt der Fima Thales wird ebenfalls nach diesem Prinzip arbeiten.

Zu Aufbau und Funktion des Verfahrens siehe auch (27). Mit der Bildung von Betriebszentralen wurde eine physikalisch zweikanalige Datenübertragung als zu teuer angesehen. Abbildung 18 zeigt den Aufbau des Systems, das eine Mischung aus Technikverfahrenssicherung und technischer Sicherung ist. Durch

den **Verzicht auf ein ständig gesichertes Meldebild** konnte auf ein einkanaliges System gewechselt werden. Dies bedeutet, dass die Datenübertragung zwischen sicherem ESTW und COMS physisch einkanalig realisiert wird. Eine logische Zweikanaligkeit besteht jedoch weiterhin durch eine **doppelte Übertragung der Telegramme** in veränderter Darstellung. Es wurde also **strukturelle Redundanz durch logische und funktionelle Redundanz ersetzt**. Im COMS werden die diversitären Telegramme mittels diversitärer Software ausgewertet. Der COMS ist an das redundante LAN der Bedienebene angeschlossen, die Datenübertragung erfolgt ab da somit wieder physisch zweikanalig und somit strukturredundant.

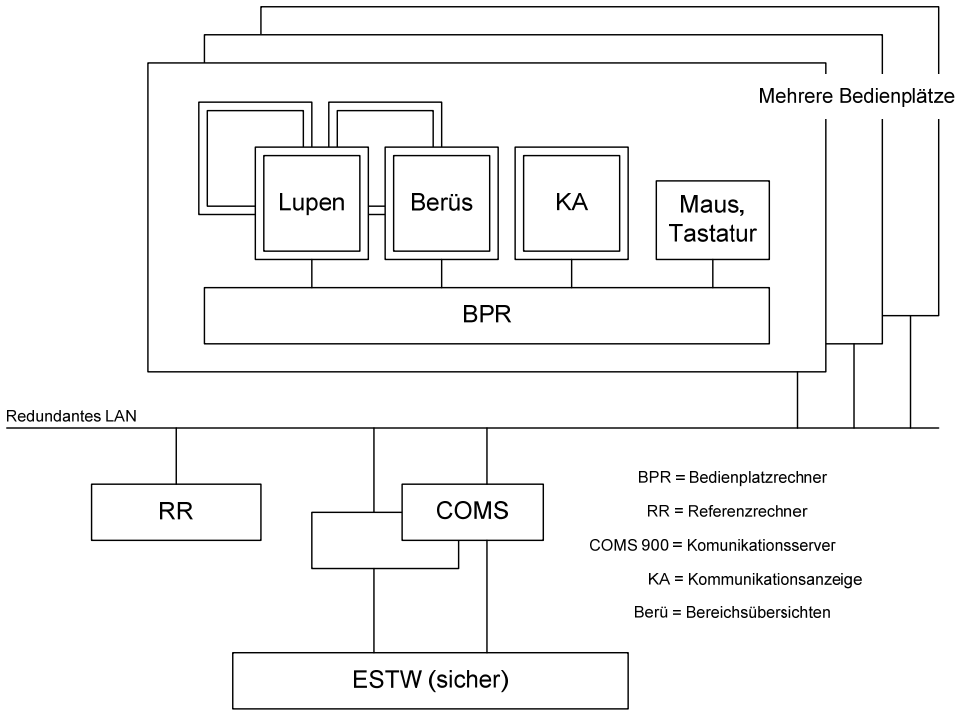

Abbildung 18 Aufbau des Bedienplatzsystem BPS 901 der Firma Siemens

Die in der Telegrammauswertung entnommenen **Prozessdaten aktualisieren ein Prozessabbild**, welches den Zustand des Stellwerks spiegelt. Im Bedienplatzsystem werden die **Prozessdaten mit statischen Bilddaten[13] versehen**

[13] Die Prozessdaten enthalten Informationen zu den Elementzuständen. Die statischen Bilddaten enthalten Informationen, wo das entsprechende Element dargestellt werden muss und die Grafik für die verschiedenen Systemzustände (z.B. Weiche links oder rechts).

und über die X11 Schnittstelle **in den Bildspeicher eingelesen**. Dieser wird zyklisch ausgelesen und als analoge Bildinformationen zum Monitor übertragen.

These 6: Durch die Verwendung statischer Bilddaten (Elementbibliothek) gibt es nur definierte Anzeigenzustände.

Es werden **nur zufällige Hardwareausfälle angenommen** die jederzeit vorkommen können. Ist der Fehlerfall eingetreten wird angenommen, dass innerhalb der vom EBA festgelegten **Ausfalloffenbarungszeit (Aoz) von 10 Stunden** kein zweiter zufälliger (jederzeit möglicher) Hardwarefehler eintritt. Der erste Fehler muss daher innerhalb dieser Zeit offenbart und das System in einen sicheren Zustand gebracht werden (Kf-Bedienungen werden gesperrt).

Die **Sicherung der Anzeige** teilt sich in einen **zyklischen Teil und in einen Bedarfsteil**. Der **zyklische Teil** wird mindestens einmal innerhalb der Aoz durchgeführt. Bei nicht erfolgreicher Prüfung werden Kf-Bedienungen gesperrt. Dabei handelt es sich um Funktionsprüfungen der beteiligten Hardware indem im Bedienplatzrechner und dem funktionsgleichen Referenzrechner die gleiche Funktion angestoßen wird und die Ergebnisse gegenseitig verglichen werden, siehe Abbildung 19.

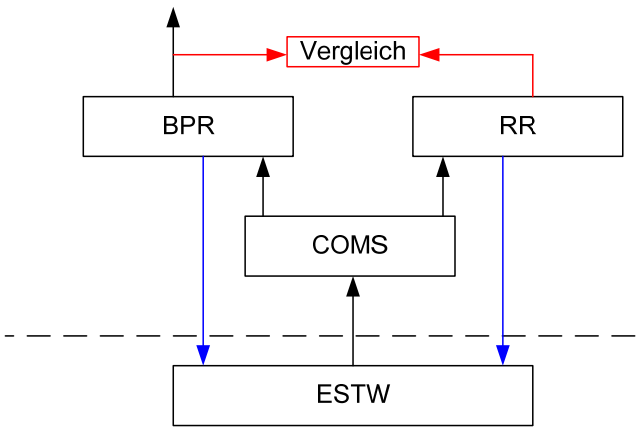

Abbildung 19 Sicherungsverfahren beim Rückleseverfahren

- Zum **Testen der Prozessdaten** werden durch Relativtests die verschiedenen Meldebilder in beiden Rechnern aufgeschaltet und verglichen (Relativtest).

- Zur **Überprüfung der Telegrammauswertung** und des Grafiksystems wird ein virtueller Bahnhof mit allen möglichen Elementen aufgeschaltet. Die entsprechende Prüfsumme wird mit Referenzwerten verglichen (Absoluttest).

Die **Bedarfsprüfung** wird **nur beim Anstoßen einer Kf-pflichtigen Handlung** durchgeführt. Hier wird das komplette entsprechende Meldebild in beiden Rechnern aufgeschaltet und mittels Prüfsumme verglichen. Die jeweiligen Prüfsummen werden, wie bereits im Kapitel über die Kf Bedienung beschrieben, an die Kf1 und Kf2 Telegramme angehängt und im sicheren ESTW nochmals verglichen. Nur nach dieser Bedarfsprüfung gilt das Meldebild als sicher.

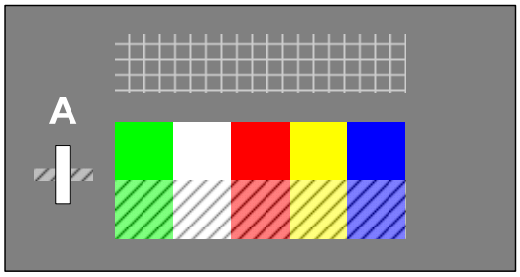

Abbildung 20 Kontrollanzeige einkanaliges Rückleseverfahren

Wie in Abbildung 20 zu sehen fehlt beim einkanaligen Rückleseverfahren der Indikator für die sichere Anzeige. Da die Anzeige jedesmal wenn dies erforderlich ist neu gesichert wird, wäre ein solcher Melder ohne Wert. Neu hinzugekommen ist das Gitter. Dies soll bei Tft-Monitoren das Einfrieren von Bildschirmteilen offenbaren.

3.2.4 Integrierte sichere Anzeige (ISA)

Das Relaisfernsteuersystem Comand 900 ist der Vorgänger der ISA und kommt auch heute noch zum Einsatz. Eine Beschreibung gibt (32). Das Anzeigesystem der C900 entsprach jedoch nicht den hohen Anforderungen des EBA und musste mit zusätzlichen Prüfroutinen ausgerüstet werden.

Der direkte Weg von der Sicherungsebene des ESTW bis zu Anzeige unterscheidet sich bei der ISA nicht wesentlich vom Rückleseverfahren. Es wird jedoch **komplett einkanalig übertragen und geprüft**, während beim Rücklese-

verfahren wie oben beschrieben das Meldebild zweimal erstellt wird, das Meldebild wird also **ausschließlich technisch-verfahrensgesichert**. Die Eingabesicherung wird auch hier mit dem Kf-Verfahren realisiert. Da **kontinuierlich sicher**, müssten bei der ISA keine Prüfsummen der Meldebilder an die Kf-Telegramme angehängt werden. Da aber die Bedienplätze von Siemens und Thales gegenseitig kompatibel sein sollen, wird dies trotzdem gemacht.

Die **Anzeigetelegramme werden einkanalig übertragen**, auch hier müssten die Telegramme doppelt und invers übertragen werden, mit einer CRC-Prüfsumme mit der Hammingdistanz von 6 versehen und durchnummeriert werden. Im APS werden die Telegramme empfangen und die Prozessdaten doppelt und invers abgelegt. Die abgelegten Daten werden regelmäßig ausgewertet, im MOS mit den entsprechenden Grafikinformationen aus dem Anzeigekatalog versorgt und das grafische Bild erzeugt. Dieses wird im Bildwiederholspeicher abgelegt, wo es abgetastet und in ein analoges VGA-Signal umwandelt wird. Bei der ISA wird die **Meldebildsicherung vollständig über Informationsredundanz und funktionale Redundanz realisiert**. Auf strukturelle Redundanz wird (zur Anzeigensicherung) völlig verzichtet. Auch bei der ISA wird ein „Ping“ zur Verfügbarkeitsmessung der einkanaligen Übertragung verwendet. Der Aufbau des Bedienplatzsystems ist in Abbildung 21 dargestellt.

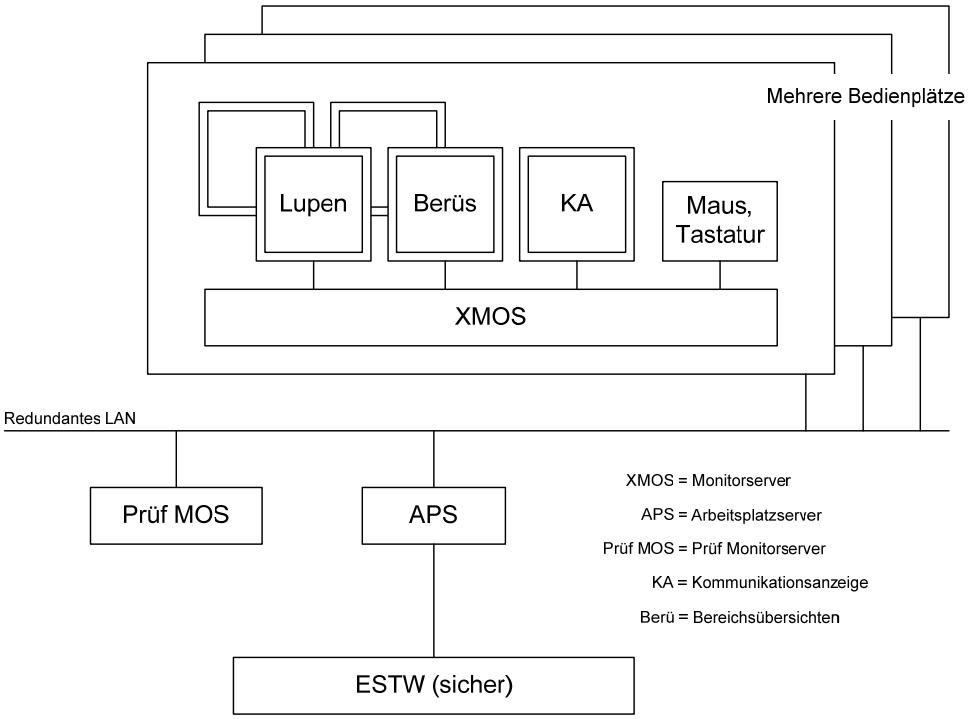

Abbildung 21 Aufbau des Bedienplatzsystems BO L ISA der Firma Thales

Die **Funktionsfähigkeit der Rechner APS und MOS muss kontinuierlich überwacht** werden (33). Dazu werden **Elementzustände aus dem Bildwiederholspeicher ausgelesen und im ASP mit dem Sollbild verglichen**. Wird die Prüfung positiv abgeschlossen, kann auf die korrekte Funktion des ASP geschlossen werden. Dies ist in Abbildung 22 blau dargestellt. Bei jeder Änderung eines Elements wird zusätzlich sofort die entsprechende Prüfung eingeleitet.

Der **APS wird durch den Prüf-MOS überwacht** (rote Darstellung). Dieser sendet **Datentelegramme aus einem Testbahnhof an den APS** und vergleicht das zurückgesendete Prozessbild mit einem Referenzkatalog. Stimmen die Werte überein, kann auf die Funktionsfähigkeit geschlossen werden.

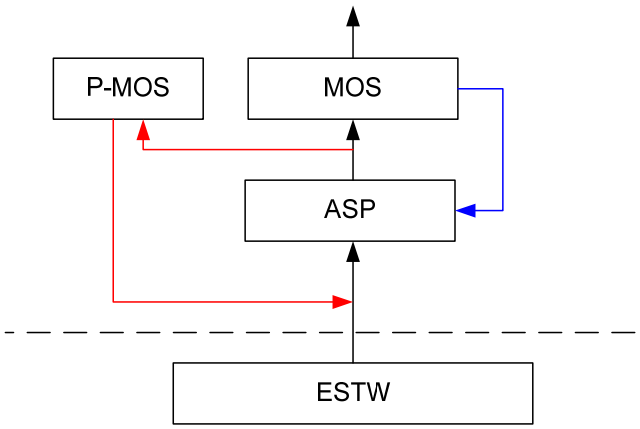

Abbildung 22 Sicherungsverfahren ISA

An der **Kontrollanzeige der ISA** fällt das weiße „S“ auf, das die sichere Anzeige indiziert. Zeigt es rot, ist eines der Prüfverfahren negativ verlaufen und die Anzeige nicht sicher. Auf das Gitter wird hier verzichtet. Man vertraut auf die Ausfallsicherheit der Monitore.

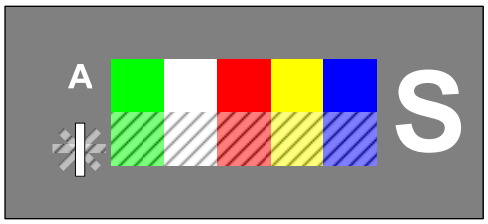

Abbildung 23 Kontrollanzeige ISA

Der **Nachteil der ISA** ist die **große Datenmenge**, die durch die Prüfungen anfällt. Der **Vorteil ist eine dauerhaft sichere Anzeige**, deren Aufwand jedoch nach Meinung des Betreibers den Nutzen übersteigt. Es wird daher bereits an einem neuen Anzeigesystem gearbeitet, das dem Rückleseverfahren angelehnt ist.

3.2.5 Verfahrensgesicherte Anzeige

Die Sicherungsverfahren der österreichischen und der schweizerischen Bundesbahnen basieren auf dem beschriebenen System. Das schweizer System nennt sich ILTIS und wurde von Siemens entwickelt, die EBO 2 wurde von Thales Austria für die ÖBB entwickelt.

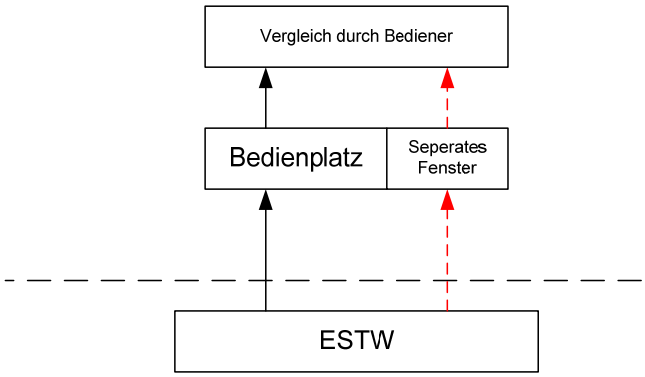

Abbildung 24 Sicherungsverfahren mit Einzelelementübermittlung

Abbildung 24 stellt das Verfahren dar. Im Regelbetrieb ist nur der schwarz gezeichnete Kanal wirksam. Sollen **Hilfsbedienungen** durchgeführt werden, wird eine **Checkliste geöffnet**, die abgearbeitet werden muss. Auf dieser Liste werden alle durchzuführenden Prüfungen aufgeführt, unter anderem die Elemente, deren richtige Anzeige der Bediener per Einzelelementprüfung sichern muss. Der Bediener sendet das Einzelprüfungskommando für das entsprechende Element. Es wird dann der **rot gezeichnete Kanal geöffnet** und der **Zustand des entsprechenden Elements** in alphanumerischer Form im „Alternativen Statusdisplay" **angezeigt**. Durch das Schließen des Fensters, wird der entsprechende Punkt in der Liste abgehakt.

Da dies **für große Betriebsstellen sehr zeitraubend** ist, wird dort eine dem Prinzip der FPÜ angelehnte Funktion verwendet. Beim Anstoßen einer Ersatzsignalfahrstraße werden im Rahmen der Checkliste nur die Hinderungsgründe angezeigt. Dadurch müssen nur die gestörten Elemente behandelt werden (34).

Nachteil des Verfahrens ist hier die größere Sicherheitsverantwortung die der Bediener überantwortet bekommt. Dies wird aber einigermaßen ausgeglichen durch die Tatsache, dass dem Bediener die einzelnen Schritte des Sicherungsprozess über die Menüführung vorgegeben werden. Er entgeht dadurch der komplexen Meldebildauswertung des deutschen Verfahrens, bei dem der Bediener ohne Hilfestellung die Auswertung vornehmen muss. Als **Vorteil** kann die einfache technische Realisierbarkeit angeführt werden.

3.2.6 Verfahrenssicherung unter Einbeziehung von Personal vor Ort

Das beschriebene Verfahren kommt derzeit nur **auf Strecken des ESZB zum Einsatz**, also auf Stecken, bei denen Zugleitbeitrieb mit elektronischem Stellwerk durchgeführt wird. Das **Zugrundelegen des Zugleitbetriebs** bietet eine **größere Freiheit** in der Ausgestaltung der Sicherungstechnik, da bei diesem Betriebsverfahren ursprünglich auf jegliche technische Sicherung verzichtet wurde, was die anerkannten Regeln der Technik wesentlich einfacher werden lässt.

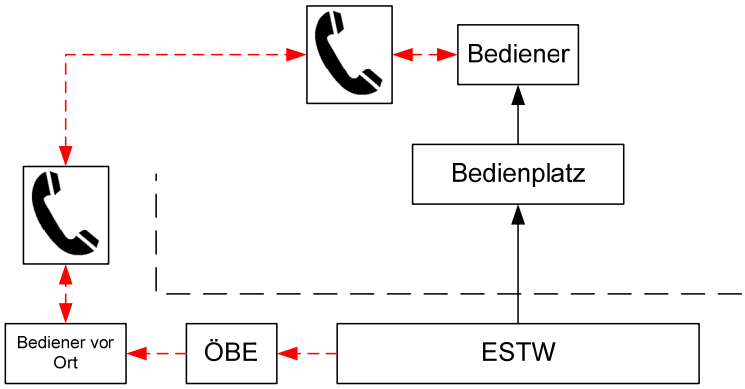

Abbildung 25 Sicherungsverfahren beim ESZB

Das in Abbildung 25 dargestellte Verfahren arbeitet im Regelbetrieb ebenfalls einkanalig. Soll eine **Hilfsbedienung** vorgenommen werden so **muss Personal vor Ort**, meistens der Lokführer, die örtliche Bedieneinrichtung (ÖBE) aufsuchen und **in Zusammenarbeit mit dem Zugleiter** (Bediener) die Hilfsbedienung durchführen.

Wird eine Hilfsbedienung nötig, fordert der Zugleiter das Personal vor Ort auf, die ÖBE zu bedienen, das Verfahren ist auch in (35) beschrieben. **An der ÖBE wird die entsprechende Bedienung ausgewählt**. Der Befehl wird an das ESTW gesendet, worauf dieses eine Prüfnummer generiert und an die ÖBE zurück sendet. Nur unter **Eingabe einer entsprechenden zweiten Nummer** an der ÖBE **kann der Befehl freigeschaltet werden**. Die Nummer der ÖBE muss am Zugleiter-Bedienplatz eingegeben werden um dort die zweite Num-

mer zu generieren. Die **Übertragung der Nummern** zwischen Bedienplatz und ÖBE erfolgt **fernmündlich**.

Das System bietet ein **relativ preiswert** zu realisierendes Bediensystem bei vergleichsweise **hohem Sicherheitsstandard** an. Im Standardbetriebsverfahren wird das Verfahren nicht angewendet, da bei diesem örtliches Personal nicht mit in den Sicherungsprozess eingebunden werden soll.

3.2.7 Bewertende Zusammenfassung

Es werden die **betrachteten Verfahren gegenübergestellt** und in den Punkten Verfügbarkeit, Sicherheit und Kosten verglichen. Es wird dabei auch der Bediener als Fehlerquelle mit einbezogen. Dabei handelt es sich um relative und qualitative Angaben da andere nicht möglich sind.

Alle gängigen Verfahren arbeiten mit einer **einkanaligen Datenübertragung** zwischen ESTW und Bedienplatz. Vermutlich wird in allen Systemen – bestimmt jedoch beim Rückleseverfahren und der ISA – eine doppelte und diversitäre Telegrammübertragung realisiert. Dies und die Anfügung von Informationsredundanz sollen Übertragungsfehler aufdecken. Ein „Ping“ als funktionale Redundanz soll Verbindungsunterbrechungen offenbaren, das versehen der Telegramme mit einer laufenden Nummer soll verlorengegangene und zu viel gesendete Telegramme bemerken. Diese relativ einfach umzusetzenden Verfahren dürften bei allen Systemen ähnlich sein.

Um die **Richtigkeit des Meldebilds** gewährleisten zu können sind weitere Maßnahmen erforderlich. Es sind die betroffenen Hardwarekomponenten der Bedienebene auf Fehlerfreiheit zu überprüfen. Dies wird durch strukturelle Redundanz (2v2/2v3 Systeme) gewährleistet. Außerdem werden die Ergebnisse der Berechnungen mittels funktioneller Redundanz geprüft. In der Realisation dieser Punkte unterscheiden sich die Systeme. Ein System das als nicht sicher gilt ist nicht zwingend unsicherer als andere Systeme, es hat nur keine EBA-Zulassung.

Die angenommene Sicherheit und Verfügbarkeit sind in Abbildung 26 dargestellt. Unstrittig sind vermutlich die **Einordnung des Rückleseverfahrens und der ISA** in den Hochverfügbarkeits- und Hochsicherheitsquadranten. Bei der **Verfahrenssicherung** ist wegen der umfangreichen Einbindung des Bedieners in den Hilfshandlungsvorgang und dem zumindest bei deutschem Betriebsverfahren ungelösten Problem der Kommandos und Meldungen ohne Prozesswirkung sowohl die Sicherheit als auch die Verfügbarkeit als wesentlich geringer eingestuft worden. Die Platzierung der „**Verfahrenssicherung unter Einbeziehung von Personal vor Ort**“ wird einerseits als wesentlich fehlerresistenter gegenüber menschlichen Bedienfehlern angesehen da zwei relativ unabhängige Personen am Prozess beteiligt sind, andererseits stellt sich ebenfalls das Problem der Befehle und Meldungen ohne Prozesswirkung.

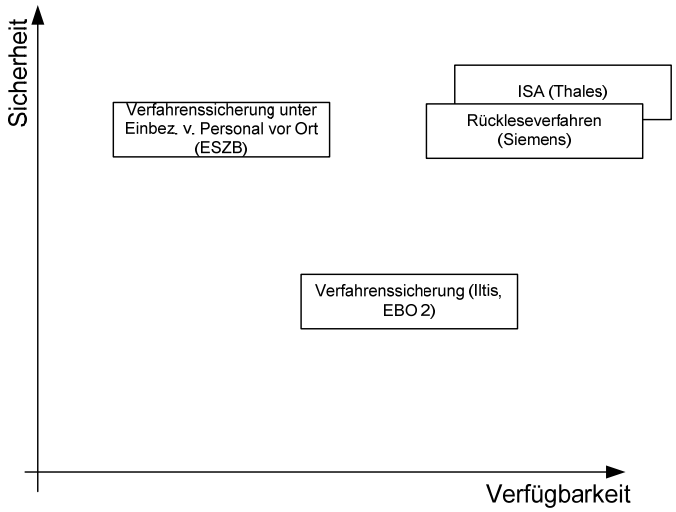

Abbildung 26 Einordnung der Bedienplatzsicherungsverfahren nach Sicherheit und Verfügbarkeit

These 7: ISA und Rückleseverfahren bieten die meiste Sicherheit und Verfügbarkeit. Die „Verfahrenssicherung mit Personal vor Ort“ ist sehr resistent gegen menschliche Fehler und erreicht eine hohe Sicherheit. Die Verfahrenssicherung bietet eine hohe Verfügbarkeit.

Eine Einschätzung des (finanziellen) Aufwands ist in Abbildung 27 illustriert. Die **ISA** weist die größte Zuverlässigkeit auf, da sie eine kontinuierlich sichere An-

zeige bietet. Gleichzeitig ist der Aufwand der größte, der zur Sicherung betrieben werden muss. Beim **Rückleseverfahren** ist die Anzeige nur im Kf-Modus gesichert. Dies bringt eine deutliche Aufwandsreduzierung. Es wird vermutet, dass die **Verfahrenssicherung** ein ähnliches Verhältnis von Zuverlässigkeit zum Aufwand auf geringerem Niveau aufweist während das Verhältnis bei der **Verfahrenssicherung mit örtlichem Personal** ein deutlich günstigeres Verhältnis aufweist. Der Grund ist in der hohen Einschätzung der Sicherheit bei relativ geringem Aufwand zu sehen.

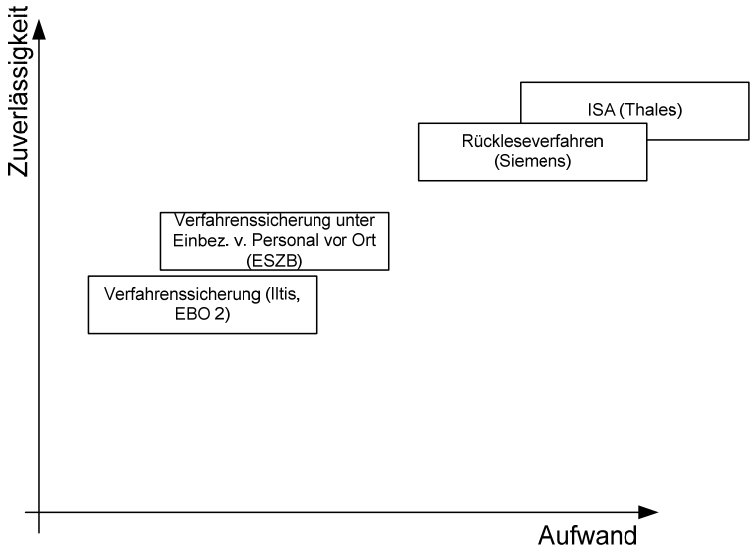

Abbildung 27 Einschätzung der Sicherungsverfahren nach Zuverlässigkeit und Aufwand

These 8: Das Zuverlässigkeits-Aufwands-Verhältnis ist beim Rückleseverfahren und bei der ISA schlechter als bei den verfahrensbasierten Sicherungen.

Die Betrachtungen legen den Gedanken nahe, dass die verfahrensbasierten Sicherungen auch im Bereich des ESTW-R Anwendung finden sollten. Diese Möglichkeit wird in Kapitel 4 weiter betrachtet.

3.3 Möglichkeiten der Zulassung

In diesem Kapitel sollen Möglichkeiten der **Zulassung eines neuen vereinfachten Bedienplatzes** untersucht werden. Dazu werden die gängigen Möglichkeiten beschrieben und auf ihre Anwendbarkeit untersucht. Der Zulassungsprozess durchlief in den letzten Jahren einen großen **Paradigmenwechsel**. So wurden in der Mü 8004 konkrete Vorgaben gemacht mit dem Ziel, den Anwender von der Aufgabe zu befreien, selbst wahrscheinlichkeitstheoretische Betrachtungen anstellen zu müssen, welches die Gefahr der „Multiplikation" von Vermutungen mit sich gebracht hätte (36). Die Zulassung war ein Vorgang der einmalig am Ende des Entwicklungsprozesses anstand. Über Funktionstests wurde die Sicherheit nachgewiesen.

Während diese Norm sich am fertigen Produkt orientierte ist nun ein bestimmter **Entwicklungs- und Herstellungsprozess Bestandteil der Zulassung**. Die Sicherheitsziele müssen **anwendungsbezogen über eine Risikoanalyse** ermittelt werden. Den Grund dafür gibt (36) mit der steigenden **Komplexität der Mikroprozessortechnologie** an: „*die Annahme, dass sich eine hinreichende Fehlerfreiheit bei komplexen Einrichtungen nur erreichen lässt wenn schon der Entwicklungsprozess in die Sicherheitsbetrachtung mit einbezogen wird und dies auch Normativ gefordert wird.*" Damit sind systematische Fehler gemeint, die sich vor allem im Softwarebereich nicht vermeiden lassen jedoch durch Qualitätsmanagement (RAMS-Management) verringern lassen.

Anhand einer Risikoanalyse sollen **potentielle Gefährdungen für die Umgebung** ermittelt werden, die von einer Einrichtung ausgehen und darüber die Anforderungen an die Sicherheitsfunktionen, die sogenannten SIL festgelegt werden. Dies sind die sogenannten **Risikoakzeptanzkriterien**. Der Nachweis gleicher Sicherheit stellt eine Abkürzung dar. Die Risikoakzeptanz wird nicht über eine Risikoanalyse sondern über eine Gefährdungsanalyse ermittelt. Die im Folgenden vorgestellte Risikoanalyse der Version 1.c stellt eine solche Abkürzung dar.

3.3.1 Risikoanalyse ESTW

Für ESTW wurde diese Analyse im Auftrag der DBAG durch die Firma Siemens erstellt. Dabei wurde **das Siemens eigene ESTW Bottom-up[14] analysiert** und die resultierenden Sicherheitslevels als maßgeblich gesetzt. (37)

In der Systemdefinition des ersten Teils der Risikoanalyse (1.c) wurden die Schnittstellen der Innenanlage betrachtet. In einem **zweiten Teil soll durch die DBAG eine ganzheitliche Betrachtung** unter Einbeziehung des Betriebsverfahrens und der handelnden Personen erfolgen. Zurzeit liegen die Anforderungen an die Schnittstellen der Innenanlage vor, die im Teil 1.c festgelegt wurden und laut EBA-Bescheid bis Ende 2007 gültig sind. (37)

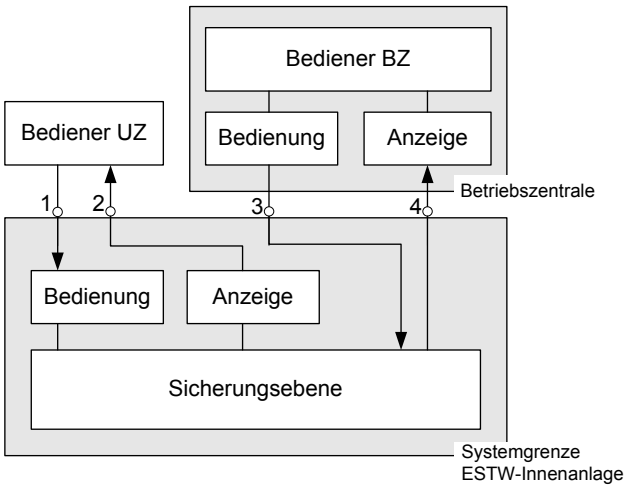

Abbildung 28 Systemdefinition: Schnittstellen zum Bedienplatz

Abbildung 28 zeigt den Ausschnitt aus der Systemdefinition, der den Bedienplatz betrifft(38; 37; 31). Es wird offensichtlich **unterschieden zwischen dem Bedienplatz der Betriebszentrale** (Bz) als externem System **und dem Bedienplatz der Unterzentrale** (Uz) als Bestandteil der Innenanlage.

[14] D.h. es wurde anhand der Referenztechnik die erreichte Sicherheit ermittelt und als THR (Tolerable Hazard Rate) festgelegt. Durch das klassifizieren der THRs erhält man die geforderten SIL.

Die für die Schnittstellen geforderten SIL sind in Tabelle 6 (31) aufgeführt. Anzumerken ist, dass **die Schnittstellen 1 und 2 MMIs[15] darstellen**, während es sich bei den **Schnittstellen 3 und 4 um System-System Schnittstellen** handelt. Dies erklärt die unterschiedlichen Anforderungen, begründet diese aber noch nicht.

Die Aussage der SIL beschränkt sich auf die Verarbeitung der Signale in der Innenanlage. Ausgehende Daten sind mit der entsprechenden Sicherheit fehlerfrei. Eingehende Daten werden mit der entsprechenden Fehlerwahrscheinlichkeit im Zuge der Weiterverarbeitung verfälscht. Es **bedeutet demnach nicht**, dass eine Kf-pflichtige Bedienung mit dem entsprechenden SIL an der Schnittstelle 3 ankommen muss. Die Logik legt diese Annahme jedoch nahe, da eine Gesamtfunktion nur dann SIL 4 erfüllen kann, wenn alle Teilprozesse die in wahrscheinlichkeitstheoretischer Reihe geschalten sind ebenfalls SIL 4 erfüllen.

Tabelle 6 Geforderte SIL für Schnittstellen

Nr.	Funktion	Regel-Modus	Kf-Modus
1	Bedienung Uz	SIL 0	SIL 4
2	Anzeige Uz	SIL 2	SIL 4
3	Bedienung Bz	SIL 4	SIL 4
4	Anzeige Bz	SIL4	SIL 4

Das **Vernachlässigen der Umgebung** im ersten Teil der Risikoanalyse war möglich, da diese **immer gleich bleibt**. Der große Nachteil ist die mögliche **Risikoüberbewertung**, die mit diesem Verfahren einhergeht. Vielfach ist dem alten Zulassungsparadigma vorgeworfen worden, über das notwendige Sicherheitsniveau hinaus zu gehen und keine Relativierung zu Gunsten der Wirtschaftlichkeit zuzulassen. Durch die beschriebene Herangehensweise werden diese Unflexibilitäten in das neue System importiert.

[15] Mensch Maschine Interface

In diesem Zusammenhang ist es Aufgabe des Betreibers, also der DBAG, eine ganzheitliche Risikoanalyse für Bediensysteme zu erstellen, welche die Anforderungen an einen Bedienplatz aufgrund tatsächlich vorhandener Risiken definiert und auf deren Grundlage neue Systeme zugelassen werden können. Die vorhandene Risikoanalyse nutzt das Potential der neuen Normen nicht aus. Laut (39) sind jedoch im Bereich des Bedienplatzes keine Veränderungen im Teil 2 der Risikoanalyse zu erwarten.

These 9: Die Risikoanalyse ESTW überträgt die undifferenzierten Anforderungen der Vergangenheit auf die neuen flexibleren Zulassungsverfahren.

Trotz der Bezeichnung „Risikoanalyse" handelt es sich hier um eine Gefährdungsanalyse mit dem Ziel, Sicherheitsziele festzulegen, die das Kriterium „mindestens gleiche Sicherheit" erfüllen. Eine Risikoanalyse die tatsächlich das Risiko analysiert ist weiterhin nicht in Sicht. Eine Risikoanalyse die den Spezialfall „Regionalverkehr" analysiert erst recht nicht.

Es wurde festgestellt, dass die einzige Möglichkeit in der Zulassung von Sicherungstechnik im Nachweis der gleichen Sicherheit besteht. Den Maßstab gibt die Risikoanalyse ESTW an. Die Ergebnisse der Analyse erschweren das Vereinfachen von Bedienplätzen.

3.4 Betriebliche Forderungen

In diesem Kapitel sollen die **Forderungen ermittelt werden, die der Bahnbetrieb an ein Bedienplatzsystem stellt,** um dann in der Synthese Möglichkeiten der Vereinfachung herauszuarbeiten. Die Grundlage dazu liefern (40; 41). Es werden die Interaktionstypen Bediener-Bedienplatz vorgestellt, die anschließend zu Anzeige-Bedienung Gruppen kombiniert werden. Schließlich werden die Kommandos und Anzeigetypen definiert, die bei der Vereinfachungsdiskussion zugrunde liegen sollen.

Das **Standardbetriebsverfahren der DBAG** ist ein Betriebsverfahren, bei dem für die Fahrweg- und Fahrtensicherung ausschließlich der Fahrdienstleiter verantwortlich ist. Das bedeutet, das Zugpersonal kann im Normalfall nicht heran-

gezogen werden[16]. Die Ursache ist in der Vergangenheit zu suchen. Das Betriebsverfahren wurde **von Anfang an dezentral** organisiert. Es war **immer Personal vor Ort**, das den Fahrweg auf Freisein prüfen konnte und das im Störungsfall eingreifen konnte. Mit der **zunehmenden Zentralisierung** wurde den Fahrdienstleitern ein reales Bild der Örtlichkeit an die Hand gegeben, um das Betriebsverfahren so weit wie möglich aufrecht erhalten zu können. Dies ist nicht unproblematisch, wie in (42) berichtet wird.

These 10: Das gegenwärtige Standardbetriebsverfahren der DBAG ist der Versuch, eine dezentrale Organisation auf zentralisierte Technik zu übertragen.

Laut „Koril 408 0231 - Grundsatz" „Züge fahren und Rangieren" müssen für die **Zulassung einer Fahrt** im Bahnhof folgende Bedingungen erfüllt sein:

- Die zu befahrenden Weichen und die Weichen im Durchrutschweg, sowie die Weichen des Flankenschutzes müssen richtig gestellt und verschlossen sein.
- Der Fahrweg muss frei von Fahrzeugen sein
- Der Durchrutschweg muss frei von Fahrzeugen sein
- Die einmündenden Gleisabschnitte müssen bis zum Grenzzeichen frei von Fahrzeugen sein.
- Zwischen Flankenschutzeinrichtung und dem Grenzzeichen einer Fahrwegweiche dürfen sich keine Fahrzeuge befinden.
- Rangierverbote müssen beachtet werden
- Bahnübergänge müssen gesichert sein wenn es die örtlichen Richtlinien bestimmen.

Wenn eine Fahrstraßenanforderung durch den Bediener vorliegt, werden diese Voraussetzungen **in der Logik des ESTW überprüft** (siehe Kapitel 2.5), im Störungsfall muss die Einhaltung der Grundsätze ebenfalls sichergestellt werden.

Unter Aufrechterhaltung des Betriebsverfahrens muss der Bedienplatz daher so ausgestaltet werden, dass der Fahrdienstleiter auch bei sicherheitsrelevanten

[16] Es gibt Ausnahmen, wie die Reisendensicherung bei Kreuzungen in unbesetzten Bahnhöfen.

Bedienhandlungen autonom agieren kann. Abbildung 29 zeigt die verschiedenen **Interaktionen des Bedieners mit dem Bedienplatz und umgekehrt** nach (40).

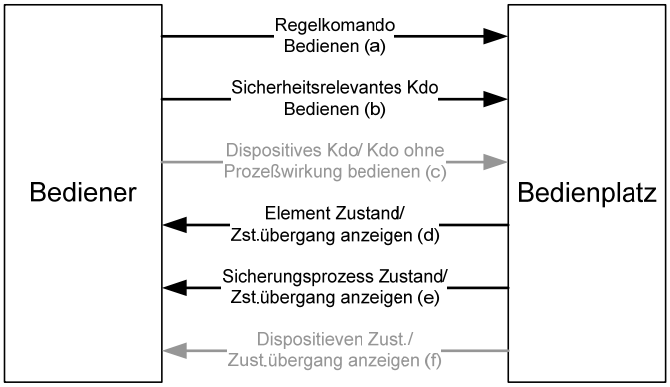

Abbildung 29 MMI Interaktionen beim Bedienplatz ESTW

Pfeile vom Bedienplatz zum Bediener stellen die Anzeige dar, in umgekehrter Richtung handelt es sich um die Bedieneinrichtung. Die einzelnen Interaktionstypen werden im Folgenden erläutert.

Die (a) „**Regelkommandos**" gehen an die Sicherungsebene. Dort werden sie auf Plausibilität überprüft (siehe Kapitel betriebliche Rückfallebenen) und gegebenenfalls zur Ausführung gebracht.

Das (b) „**sicherheitsrelevante Kommando**" kann unter **Umgehung der Sicherungsebene** Prozesse auslösen. Es gibt dann nur eingeschränkte bis keine technische Überwachung, die eine Fehlbedienung verhindern können.

Der **Anzeigetyp** (d) „**Element Zustand/Zustandsübergang**" bringt den Zustand der **Feldebene zur Anzeige**, also die Stellung von Weichen und Signalen. Für diese Anzeige gibt es ein physisches Äquivalent. Die Richtigkeit der Anzeige kann bei Bedarf vor Ort durch Hinsehen überprüft werden.

Beim **Anzeigetyp** (e) „**Zustand und Zustandsübergang des Sicherungsprozesses anzeigen**" werden Zustände angezeigt, die **kein physisches Äquivalent** das durch Hinsehen überprüft werden könnte besitzen. Dies sind beispielsweise Befahrbarkeitssperren oder der Füm.

Bedienung und Anzeige dispositiver Zustände (c,f) werden nicht weiter betrachtet, da von diesen keine Sicherheitsrelevanz ausgeht.

Die beschriebene Unterteilung in verschiedene Interaktionstypen ist **differenzierter als dies beim Kf-Verfahren** der Fall ist, zum Teil auch widersprüchlich. Im Kf-Zustand werden immer sämtliche Sicherungstypen durchgeführt – Eingabesicherung und Anzeigesicherung. Dies ist jedoch nicht immer nötig. Durch die Differenzierung kann eine **bedarfsgerechte Bedienplatzsicherung** abgeleitet werden. (43)

Im Folgenden sollen die **Kombinationen der Interaktionstypen** mit Beispielen vorgestellt werden:

- (a) **Regelbedienung** ohne besondere Anforderung an die Anzeige: Weiche umstellen, Regelzugfahrstraße einstellen.
- (a)+(e) **Regelkommando der Sicherungsebene** durchführen bei denen das **Wissen um deren Ausführung sicherheitsrelevant** ist: Befahrbarkeitssperre eingeben, Weichenlaufkette sperren. Es handelt sich um das Ausschalten von leittechnischen Funktionen oder das Sperren von Elementen. Diese Befehle haben keine sichtbaren Auswirkungen, sie wirken nur systemintern. Es ist jedoch von sicherheitsrelevanter Bedeutung, dass die Befehle auch ordnungsgemäß durchgeführt werden. Die **einzige Möglichkeit dies zu kontrollieren** ist auf der **Meldebildanzeige**. Daher muss eine besondere Sicherung der Anzeige der Sicherungsprozesse nach der Befehlsabgabe durchgeführt werden und möglicherweise die Auswertung des Meldebilds durch den Bediener nach der Befehlseingabe erzwungen werden.
- (b)+(d) **Sicherheitsrelevante Kommandos** bei denen der Bediener **vor Durchführung** das Meldebild auf **korrekten Zustand der Elemente auswerten** muss: Ersatzsignal (EE1,EE2), Weichenlaufkette einschalten, Befahrbarkeitssperre löschen. Es handelt sich um Funktionen bei denen die **Sicherungsebene umgangen** wird. Von sicherheitsrelevanter Bedeutung ist hier, dass dem Bediener kein fehlerhaftes **Meldebild als Entscheidungsgrundlage** vorliegt. Ebenfalls müssen **Bedienfehler verhindert** und möglicherweise die Auswertung des Meldebilds erzwungen werden. Hingegen ist die Erfolgskontrolle wie sie in der Kombination (a)+(e) benötigt wird nicht sicherheitsrelevant.
- (e) **Zustand/Zustandsübergang der Sicherungsebene** anzeigen, **ohne vorherige Bedienhandlung** (spontan auftauchende Meldungen (43)): Fü-Büsa Störungsmeldung, Füm einer Hilfszugfahrstraße erlischt unerwartet. Diese Zu-

stände müssen immer sicher angezeigt werden und durch den Bediener überwacht werden.

Es ist somit klar, dass auch **bestimmte Regelbedienungen ein gesichertes Meldebild benötigen**. Bei Systemen die das Kf-Verfahren anwenden, wird dies nicht gefordert. Vielmehr ist dies (vor allem die spontan auftauchenden Meldungen) die Begründung für die Forderung nach einer dauerhaft mit SIL 2 gesicherten Anzeige (auch (43)).

Ein Beispiel für ein Betriebsverfahren bei dem **kein gesicherter Bedienplatz** gefordert wird **ist der Zugleitbetrieb**. In der Ausführung mit ESTW kann der Zugleiter (Bediener) die Regelbedienungen durchführen, die keine sichere Anzeige benötigen. Das Durchführen von sicherheitsrelevanten Kommandos ist unter Einbindung von Personal vor Ort, meistens dem Lokführer möglich – siehe die entsprechende Beschreibung im Kapitel 3.2.6. Kommandos zum Eingriff in die Sicherungsebene sind entweder nicht vorhanden (das Ersatzsignal Zs 1 kann nur bei einem mit Füm-Ruhelicht vergleichbaren Zustand durchgeführt werden. Eine Sperrung der Weichenlaufkette ist daher obsolet.) oder mit betrieblichen Redundanzen verknüpft (eine Befahrbarkeitssperre wird nur im nicht-sicheren Bedienrechner gespeichert. Ein Eintrag im Zugmeldebuch für SZB-E ist zusätzlich nötig).

Nachfolgend sind die **Funktionen aufgelistet** und kurz erläutert, die bei den Vereinfachungsdiskussionen berücksichtigt werden. Die Aufzählung erhebt keinen Anspruch auf Vollständigkeit.

Funktionen bei denen die Sicherungsebene umgangen wird (44):

- Weichen, Gleissperren, Kreuzungen, Schlüsselsperren und Gleise
    - AWU – Weiche oder Kreuzung mit Auffahrmeldung umstellen
        - Die Meldung wird generiert, wenn eine Weiche die Sollstellung „selbstständig“ verlässt und somit einen nicht definierten Zustand eingenommen hat.
        - Bevor mit dem Kommando AWU ein definierter Zustand wieder hergestellt werden darf muss der ordnungsgemäße Zustand der Weiche vor Ort festgestellt werden (25).
    - FAHE – Weiche, Kreuzung oder Gleis einzeln hilfsauflösen

        - Diese Bedienung wird benötigt, wenn die Funktion FHA nicht möglich ist da eine der Voraussetzungen nicht erfüllt ist.
        - Voraussetzung ist, dass die Fahrstraße noch festgelegt ist (Zfm), die Bedienung muss von Start in Zielrichtung durchgeführt werden. Dies entspricht der zugbewirkten Auflösung.
    - KLO – Anschlusskennung löschen
        - Wurde für einen Zug durch Start-Ziel Bedienung für eine Fahrt in eine Awanst eine Anschlusskennung generiert so kann diese mit dem Kommando KLO gelöscht werden. Die Awanst kann dann durch diesen Zug nicht mehr bedient werden.
    - SLHE – Awanst bei gestörter Gleisfreimeldung freigeben
        - Die hilfsweise Schlüsselfreigabe für die Awanst wird benötigt, wenn die Bedingungen für eine reguläre Schlüsselfreigabe nicht vorliegen.
        - Voraussetzungen sind die Blockgrundstellung und eine Befahrbarkeitssperre für den Blockabschnitt.
    - WHU – Weiche hilfsweise umstellen
        - Wenn die Bedingungen für ein Umstellen mit WU nicht vorliegen
        - Die Weiche darf nicht gesperrt und nicht aufgefahren sein. Eventuelle Folgeabhängigkeiten werden kontrolliert.
- Signale: Hauptsignale können nur dann einen Fahrtbegriff zeigen, wenn alle Bedingungen dafür erfüllt sind. Ist dies nicht der Fall, kann eine Zugfahrt hilfsweise auch mit einem Ersatzsignal zugelassen werden.
    - EE1 – Ersatzsignal bedienen (Wlk nicht gesperrt)
        - Der Füm muss mindestens blinken oder Dauerlicht zeigen, der Abschnitt vor einem Einfahrtsignal muss belegt sein, das Signal darf keinen Fahrtbegriff zeigen.
    - EE2 – Ersatzsignal bedienen (Wlk gesperrt)
        - Die Weichenlaufkette muss gesperrt sein
    - FE – Falschfahrt-Auftragssignal bedienen (Zugstraße bis Füm-Dauerlicht eingelaufen)
    - LE1 – Linksfahrersatzsignal bedienen (Wlk nicht gesperrt)
        - Wie EE1 mit zusätzlichem Auftrag zur Fahrt auf dem Gegengleis
    - LE2 – Linksfahrersatzsignal bedienen (Wlk gesperrt)
        - Wie EE2 mit zusätzlichem Auftrag zur Fahrt auf dem Gegengleis
    - VE1 – Vorsichtssignal bedienen (Wlk nicht gesperrt)
        - Wie EE1 mit zusätzlichem Auftrag zur Fahrt auf Sicht
    - VE2 – Vorsichtssignal bedienen (Wlk gesperrt)
        - Wie EE2 mit zusätzlichem Auftrag zur Fahrt auf Sicht
- Fahrstraßen

    - FHA – Zugstraße hilfsauflösen
        - wird benötigt bei Auflösestörungen und der Rücknahme falsch eingestellter Fahrstraßen
        - Die Fahrstraßenfestlegung muss bestehen, bei haltzeigendem Startsignal (z.B. durch HaGT), der Anrückabschnitt muss frei sein, bei Mittelweichen zeigt das Zielsignal keinen Fahrtbegriff und der Reihenfolgenzwang bei mehreren Fahrstraßen wird beachtet.
- Streckenblock: die folgenden Kommandos bewirken das Gleiche bei unterschiedlichen Blocktechniken. Die Kommandos werden angewendet, wenn die zugbewirkte Grundstellung nicht gewirkt hat, z.B. durch eine Gleisfreimeldestörung. Es ist eine Räumungsprüfung durchzuführen.
    - BG – Ausfahrsperre bzw. Block in Grundstellung bringen
    - BHA – Zentralblock hilfsauflösen
        - Das Startsignal muss Halt zeigen
    - HRB – hilfsrückblocken von Hand bei gestörter Gleisfreimeldung
- Achszähler
    - AZG – (Eingeschränkte Grundstellung) Achszähleinrichtung einer Weiche, einer Kreuzung oder eines Gleises in Grundstellung bringen
        - Die letzte Zählung muss eine auszählende Achse gewesen sein
    - VAZG – Vorbereitend Achszähleinrichtung eines Blockabschnittes in Grundstellung bringen
        - Es muss eine Fahrt durchgeführt werden, bei der die Achsen einmal korrekt ein- und ausgezählt werden. (Räumungsprüfung)
- Bahnübergänge
    - UHA – signalgesteuerte Büsa hilfsausschalten
        - Wenn die Fahrstraße zurückgenommen werden muss und die Fahrt nicht stattfindet, wird der Bü mit UHA hilfsausgeschaltet. Die Fahrstraße muss dazu bereits aufgelöst sein.
    - UHF – signalgesteuerte Büsa hilfsfreimelden
        - Die technische Freimeldung für einen Bü mit Vollschranken ist defekt und wird durch betriebliche Maßnahmen ersetzt.

Kommandos der Sicherungsebene, deren Erfolgskontrolle sicherheitsrelevant ist:

- Ausschalten von leittechnischen Funktionen
    - WLS – Weichenlaufkette sperren
    - SBA – Selbststellbetrieb ausschalten
    - ZLA – Zuglenkung ausschalten
- Sperren von Gleisen oder Elementen

- WUS – Weiche gegen Umstellen sperren
- SS – Signal sperren
- BS – Selbst- oder Zentralblocksignal sperren
- ME – Merkhinweis für Fahrwegelement eingeben (mit Befahrbarkeitssperre verbunden)

Spontan auftauchende Meldungen:

- Störungsmeldung Ebüt-Fü
- Füm bei Zugfahrten die ohne Hauptsignal zugelassen werden

Die zu untersuchenden Interaktionskombinationen wurden identifiziert. Dies sind die sicherheitskritischen Bedienungen, die Bedienungen bei denen die Erfolgskontrolle sicherheitsrelevant ist und spontan auftauchende Meldungen. Nach einem Blick zu anderen Bahnen werden diese Erkenntnisse im nächsten Teil dieser Arbeit dazu genutzt, ein nicht gesichertes Meldebild zu diskutieren.

3.5 Sicherungsparadigmen anderer Bahnen

Der schwedische Netzbetreiber Banverket verzichtet wie viele Eisenbahnen außerhalb des deutschsprachigen Raums auf eine spezielle Sicherung des Fahrdienstleiterbedienplatzes bei ESTW oder RSTW.

In (45) heißt es: Das Meldebild in Fernsteuerzentralen ist nicht als Sicherheitssystem aufgebaut. Es ist nicht abgesichert, dass alle Anzeigen in allen Fällen die wirklichen Verhältnisse der Außenanlage wiedergeben.

Es werden Instruktionen zur Auswertbarkeit der Anzeigen gegeben:

Der **Fahrdienstleiter darf sich auf die Richtigkeit von Anzeigenänderungen verlassen wenn diese auf eine entsprechende Bedieneingabe folgen**. Als Beispiele werden genannt:

- Die Anzeige, dass eine Fahrstraße verschlossen wurde, nach dem Einstellen der Fahrstraße.
- Die Anzeige, dass eine Weiche in einer bestimmten Lage befindet, als Antwort auf einen Umstellbefehl aus der anderen Lage.

- Das Anzeigen der Erlaubnis für eine bestimmte Blockrichtung als Antwort auf das Wechseln der Erlaubnis.
- Auf die Anzeige, dass sich ein Zug an einer bestimmten Stelle befindet darf sich der Fahrdienstleiter verlassen, wenn er das logische Zustandekommen der Belegung beobachtet hat.

Einzelne Anzeigen die sich nicht verändern ergeben **keine Auswertbare Information**:

- Es ist nicht sicher, dass eine Weiche in einer angezeigten Endlage befindet.
- Ein als belegt angezeigter Abschnitt dass sich dort tatsächlich Fahrzeuge befinden.

Es handelt sich hierbei um das **Prinzip „Auswertung des Zusammenhangs von Ort und Zeit bei einem Zustandswechsel"** wie es in (41) genannt wird. Das schwedische Betriebsverfahren ist darauf ausgerichtet und am ehesten mit dem Zugleitbetrieb mit ESTW zu vergleichen. Der Fahrdienstleiter hat eher die Funktion einer Zugdisposition, das Personal vor Ort ist aktiv in die Sicherung mit eingebunden. So wird eine Streckensperrung durch manuelles kurzschließen der Gleisstromkreise realisiert (46), was auch der Grund ist, warum Banverket gänzlich auf Achszähltechnik verzichtet. Es wird im Störungsfall dem beteiligten Personal ein wesentlicher Teil der Sicherheitsverantwortung auferlegt.

Die österreichische Bundesbahn (ÖBB) verzichtet hingegen nicht auf eine Anzeigesicherung. Das Prinzip der EBO2 (Einheitsbedienoberfläche) wurde bereits in Kapitel 3.2.5 vorgestellt. Um einen den Zustand eines Elements auswerten zu können muss der Bediener die erneute Übermittlung anfordern. Das Element wird dann diversitär, über einen zweiten Kanal übertragen, der Bediener muss das sich öffnende Zusatzfenster mit der Anzeige vergleichen. Es handelt sich nach (41) um das Prinzip **„Auswertung der Identität von zwei logisch gleichen, verschieden codierten Informationen"**

These 11: Die Prinzipien „Auswertung des Zusammenhangs von Ort und Zeit bei einem Zustandswechsel" und „Auswertung der Identität von

zwei logisch gleichen, verschieden codierten Informationen“ können auch im Bereich deutscher Eisenbahnen gelten.

4 Ansätze zur Vereinfachung von Bedienplätzen

Es sollen verschiedene Ansätze zu Vereinfachung der Bedienplatzsysteme diskutiert werden. Im ersten Kapitel wird mit der Forderung nach einer **Vereinfachung der Definition** einer sicheren Anzeige vor allem auf eine Vereinfachung des Zulassungsprozess hingewirkt. Im zweiten Kapitel wird auf die die **Anzeigensicherung verzichtet** und der **Einfluss auf die Rückfallebenen** diskutiert. In weiteren Kapiteln werden einfache Sicherungsmaßnahmen wieder eingeführt um den Einfluss auf die Rückfallebene zu begrenzen und die Einführung der verfahrensbasierten Anzeigesicherungen diskutiert. Dabei wird davon ausgegangen, dass Eingabe- und Datenübertragungssicherung relativ einfach zu realisieren sind und die Anzeigesicherung den meisten Aufwand erfordert.

Es sei darauf hingewiesen, dass den Ausführungen **keinerlei Felddaten zu Grunde liegen** und diese somit den Charakter von Gedankenexperimenten haben. Die Basis bilden die in den vorherigen Abschnitten gebildeten Thesen.

4.1 Verändern der Definition einer sicheren Anzeige

Die Diskussion zur Risikoanalyse im Kapitel 3.3.1 sowie zur funktionalen Sicherheit (Kapitel 2.3) und dem Menschen unter Sicherheitsverantwortung (Kapitel 2.4) bilden die Grundlage zu den folgenden Ausführungen. Gegenstand der Kritik ist die mangelnde Einbindung des Bedienpersonals und die **Berücksichtigung des Menschen als Fehlerfaktor** bei der Festlegung von Anforderungen zur funktionalen Sicherheit. Es soll argumentativ begründet werden, dass eine funktionale Sicherheit für das Bediensystem im Kf-Modus von SIL 2 ausreichend ist, gegenwärtig wird SIL 4 gefordert.

4.1.1 Diskussion der Fehlerwahrscheinlichkeit im Kf-Modus

Bei der Durchführung von Hilfshandlungen wird durch den Bediener direkte Sicherheitsverantwortung übernommen. An Abbildung 15 lassen sich die Verhältnisse verdeutlichen. In Abbildung 30 ist die maßgebliche Stelle herausgezogen und mit den möglichen Bedienerfehlern dargestellt.

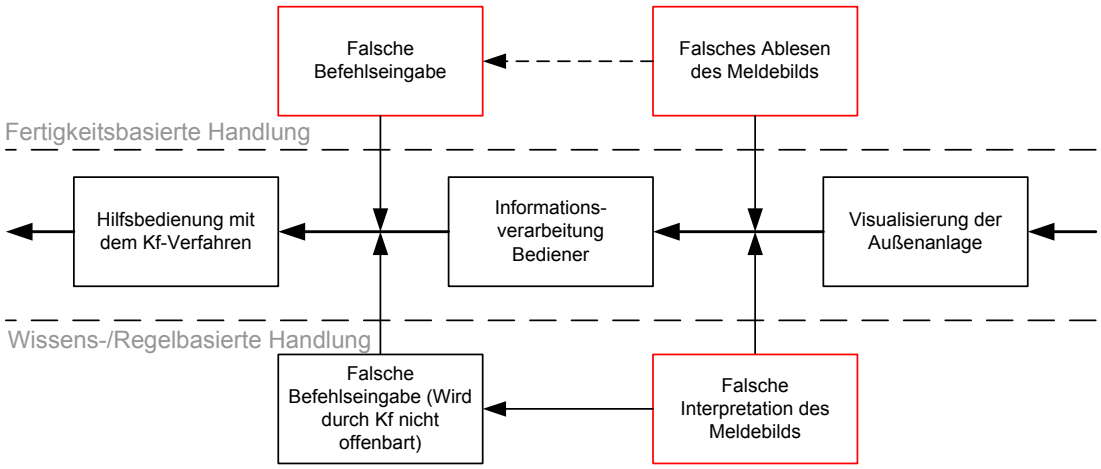

Abbildung 30 Bedienerfehler

Der Bediener nimmt Informationen durch das Meldebild auf und verarbeitet diese. Das Resultat sind Bedienhandlungen, die sicherheitsrelevant sein können. In diesem Fall wird eine Anzeigensicherung vorgenommen und der Befehl wird über das Kf-Verfahren autorisiert. Die Befehlsübertragung erfolgt ebenfalls unter höchsten Sicherheitsanforderungen. Dabei **sind Bedienfehler möglich** die, die fertigkeitsbasierte Handlungsebene vorausgesetzt, entweder in einem **falschen Ablesen des Meldebilds**, in einer **falschen Informationsverarbeitung** oder in einer falschen Befehlseingabe resultiert. Die Gesamtfehlerwahrscheinlichkeit wurde unter Anwendung des Kf-Verfahrens in Tabelle 4 mit $10^{-4}/\text{Bedienhandlung}$ festgelegt.

Es ist hierbei zu beachten, dass nicht von jedem dieser Fehler eine Gefährdung ausgeht. Den Quotienten von nicht gefährdenden Fehlhandlungen zur Gesamtzahl der Fehlhandlungen kann man als Fehlertoleranz bezeichnen. Das Kf-Verfahren soll die Fehlertoleranz positiv beeinflussen. Da mangels Daten über die Fehlertoleranz keine Aussage getroffen werden kann, werden alle Fehler bei Kf-Bedienungen die darüberhinaus zählpflichtigen Hilfshandlungen sind als gefährlich angenommen.

Bei angenommen zwei zählpflichtigen Kf-Bedienungen pro Tag[17] kann die angegebene Fehlerwahrscheinlichkeit auf einen Fehler je 500 Tage oder $8{,}33 * \frac{10^{-6}}{h} \approx \frac{10^{-5}}{h}$ beziffert werden.

Das Meldebild muss gleichzeitig Anforderungen des SIL 4 genügen. Für dieses Sicherheitslevel ist eine Ausfallwahrscheinlichkeit von $< \frac{10^{-8}}{\mathrm{h}}$ vorgeschrieben.[18] Gleiches gilt für die Übertragung der Kf-Befehle. Abbildung 31 zeigt den Zusammenhang zwischen Bedienerfehler und technischen Fehlern an.

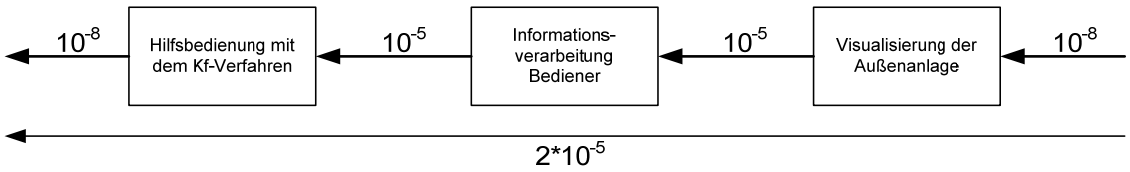

Abbildung 31 Fehlerwahrscheinlichkeit während einer Kf-Bedienung

Die technischen Fehler sind gegenüber den Bedienerfehlern vernachlässigbar. Nach dem Grundsatz, dass die schlechteste Fehlerwahrscheinlichkeit das SIL einer Funktion bestimmt, erhält man eine dem SIL 1 genügende Fehlerwahrscheinlichkeit. Bei einem System wie dem hier betrachteten ist dies nicht zufriedenstellend, da Fehler große Auswirkungen haben können.

[17] Es muss beachtet werden, dass es sich um eine rein spekulative Annahme handelt, da auch hier das Problem des Datenmangels eine begründete Schätzung nicht zulässt. Daher ist auch eine Berücksichtigung der vorhandenen Abhängigkeit vom Betriebsprogramm und der Anlagengröße nicht sinnvoll, dies würde eine nicht vorhandene Genauigkeit vortäuschen. Diese Größenordnung wurde jedoch von mehreren Fachleuten als realistisch bewertet, unter anderem durch (30).

[18] Die EN 61508 unterscheidet bezüglich der SI-Level zwischen niedriger und hoher Anforderungsrate. Hohe Anforderungsraten gelten für Systeme deren Funktion öfter als einmal im Jahr in Anspruch genommen werden. Es wird dann mit Ausfällen pro Stunde gerechnet.

These 12: Nach dem Grundsatz des schwächsten Glieds ist bei Hilfsbedienungen die Fehlerrate des Menschen die maßgebliche Größe. Unter Anwendung des Kf-Verfahren entspricht dies SIL 1.

4.1.2 Maßnahmen zur Erhöhung der Sicherheit

Es sei betont, dass diese Abschätzung nur für die Übernahme der Verantwortung für die Sicherheit durch den Bediener gilt. Im Regelfall liegt die Sicherheitsverantwortung bei der Technik und erfüllt Forderungen nach SIL 4. Eine Strategie zur Steigerung der Gesamtsicherheit ist es, möglichst zu vermeiden, dass der Bediener Sicherheitsverantwortung übernimmt.

Die Anzahl sicherheitskritischer Entscheidungen soll auf ein Minimum reduziert werden. Dies kann z.B. durch die im Kapitel 2.5 erläuterte Funktion FPÜ erfolgen. FPÜ wird jedoch **im Lastenheft ESTW-R als nicht-benötigte Funktion** geführt, da die Funktion nur für Fahrstraßen mir vielen Elementen durch das EBA verbindlich gefordert wird.

Eine weitere Möglichkeit, die Sicherheit unter Verantwortung des Menschen zu erhöhen ist die **Verbesserung des Kf-Verfahrens** – und hier ist ausschließlich der Teil des Verfahrens gemeint der zur Fehlerreduktion des Bedieners dient. Das Verfahren verlangt gegenwärtig nur das erneute Bestätigen einer Bedienung, so zu sagen um dem Bediener bewusst zu machen, dass eine sicherheitsrelevante Bedienung durchgeführt wird.

Eine Möglichkeit dies zu erreichen könnte das **Einbinden eines zweiten Bedieners** sein, der die Bedienung verifiziert und somit eine relativ unabhängige zweite Entscheidung bietet. Man könnte sich ein Kartenlesegrät vorstellen, das die Kf-Tasten ersetzt und nur durch die Karte eines nicht angemeldeten Fahrdienstleiters bedient werden kann. Möglicherweise kann so die Kf-Bedienung den Bereich von SIL 2 erreichen. Dieses Thema aus dem Bereich der MMI sollte Bestandteil weiterer Untersuchungen sein.

Im Gegenzug wird empfohlen die Anforderungen an ein gesichertes Meldebild **von SIL 4 auf z.B. SIL 2 zu senken**. Dies entspricht einer tolerierten Fehler-

wahrscheinlichkeit von $\frac{10^{-6}}{h}$ und liegt noch immer über der des Bedieners. Dies würde demzufolge einem unmerklichen Sicherheitsverlust gleichkommen. In Verbindung mit der oben diskutierten Modifizierung der Bedieneingabe kann eine deutliche Verbesserung der Sicherheit erreicht werden.

Es wurde die **Definition einer sicheren Anzeige angezweifelt**. Dies geschah auf der Grundlage der Annahme dass eine Funktion nur so sicher sein kann wie das unsicherste Teilsystem das zum Funktionieren beiträgt. Dies ist im Falle der Hilfshandlungen der Bediener mit der dem Menschen innewohnenden Fehlerrate. Es wird empfohlen, die Anzeige nur mit SIL 2 zuzulassen und den marginalen Sicherheitsverlust durch das Einführen der Funktion FPÜ und einer verbesserten Eingabekontrolle auszugleichen. Dies soll die Zulassungskosten für ein neues Produkt das tatsächlich jedoch die gleichen Anforderungen erfüllt wie ein SIL 4 Produkt. Eine Veränderung des Betriebsverfahrens ist somit nicht nötig.

4.2 Verzicht auf die gesicherte Anzeige

In diesem Kapitel sollen die **Auswirkungen eines nicht gesicherten Meldebilds auf die Rückfallebenen** des deutschen Eisenbahnbetriebs diskutiert werden. Grundlage ist dabei das Prinzip der Auswertung des Zusammenhangs von Ort und Zeit. Der komplette Verzicht auf eine sichere Anzeige bringt zweifellos einen Sicherheitsverlust mit sich. Der **Mensch wird stärker in die Verantwortung genommen**, was, wie bereits mehrfach ausgeführt, als kritisch zu bewerten ist. Vordergründig steigt die Verfügbarkeit da das Anzeigensicherungssystem keine eigenen Fehler mehr produziert. Es wird jedoch im Verlauf dieses Kapitels erläutert, warum die **Verfügbarkeit in der Summe vermutlich zurück gehen wird**.

Es wurden im Rahmen dieser Arbeit Anstrengungen unternommen, Felddaten zu Anzeigefehlern zu Erhalten um die Differenz an Anzeigefehlern zwischen einem gesicherten und einem ungesicherten System zu erhalten, was sich als nicht möglich herausgestellt hat. Denn Fehlerdatenbanken sind für diese Art der Analysen unbrauchbar da entweder nur Fehler aufgenommen werden, die

Verspätungsminuten erzeugt haben, was das Ergebnis verfälschen würde, andererseits ist es nicht zulässig, bei einem falsch angezeigten Element direkt auf einen Anzeigefehler zu schließen. Bestes Beispiel sind freie Gleisabschnitte, die als belegt angezeigt werden. Meisten ist die Ursache im Gleisfreimeldesystem zu finden, das die Meldung falsch generiert hat.

Eine andere Herangehensweise auf Basis von Felddaten war, die Anzahl Fehler zu ermitteln, die durch ein sicheres Anzeigesystem offenbart wurden. Dies hätte sich auf die Frage reduziert, wie oft das dauerhaft gesicherte System ISA die Anzeige als nicht sicher meldet. Bei einem derart komplexen Sicherungssystem muss jedoch von einem hohen Eigenfehleranteil ausgegangen werden. Diese Fehler können von tatsächlichen Anzeigefehlern nicht unterschieden werden. Die Analyse in diesem Kapitel kann also ausschließlich auf theoretischer Basis stattfinden.

Es werden im Folgenden die vier in Kapitel 3.4 identifizierten Funktionsgruppen betrachtet:

- **Regelbedienungen**,
- **(Sicherheitsrelevante) Bedienungen** bei denen das Meldebild vor der Bedienung ausgewertet werden muss,
- Bedienungen der Sicherheitsebene, bei der eine **Erfolgskontrolle** sicherheitsrelevant ist,
- Anzeigen die **kontinuierlich überwacht** werden müssen und spontan auftauchende Meldungen

Der gänzliche Verzicht auf eine gesicherte Anzeige wird den **möglichen Befehlsvorrat einschränken**. Es wurde der in Kapitel 3.4 aufgeführte Funktionsvorrat analysiert. **Grundsätzlich sind Regelbedienungen möglich**, deren Ausführung anhand von **Zustandsänderungen der Außenanlage** kontrolliert werden kann (siehe Kapitel 3.4 und 3.5).

4.2.1 Sicherheitsrelevante Bedienungen

Soll für sicherheitsrelevante Bedienungen das Meldebild ausgewertet werden, so ergeben sich drei Betrachtungsfälle:

- Die Anzeige **stimmt mit der Außenanlage überein** und ist korrekt.
- Die Anzeige **zeigt die Inanspruchnahme eines Elements** an, während dies tatsächlich **nicht der Fall ist**. (fail safe)
- Die Anzeige **zeigt die nicht-Inanspruchnahme an**, obwohl das betreffende Element **gerade in Anspruch genommen wird**. (kritisch)

Betrachtet werden muss der letze Punkt. Dieser wird durch eine Meldebildsicherung theoretisch ausgeschlossen. Bei einem ungesicherten Meldebild muss damit jedoch gerechnet werden. Dabei wird davon ausgegangen, dass die sichere Ebene fehlerfrei ist und die Inanspruchnahme kennt. Tabelle 7 zeigt die Verwendbarkeit der Kommandos.

Tabelle 7 Anwendbarkeit der Funktionen bei nicht sicherer Anzeige[19]

Kommandos	AWU	FAHE	KLO	SLH	WHU	EE/LE1	EE/LE2	VE1	VE2	FHA	BHA	AZG	VAZG	UHA	UHF
Uneingeschränkt verwendbar	x		x	x								x	x	x	x
Eingeschränkt verwendbar					x			x	x	x	x				
Nicht verwendbar		x				x	x								

Die **uneingeschränkte Verwendung ist möglich wenn** z.B. sich Personal vor Ort befindet, was bei den Kommandos AWU, SLH und UHF der Fall ist. Bei fälschlicher Verwendung von KLO entsteht kein unsicherer Zustand, UHA kann erst nach der Fahrstraßenauflösung angewendet werden.

Die Funktionen AZG und VAZG werden bei gestörtem (fälschlicherweise als belegt gemeldetem) Achszählabschnitt angewendet. Dazu muss vorher eine **Räumungsprüfung** durchgeführt werden (siehe Kapitel 0). Wird die Rotausleuchtung auf der nicht sicheren Anzeige angezeigt, kann diese Prozedur durchgeführt werden.

[19] Die Funktionen wurden in Kapitel 3.4 erläutert.

Bei nicht gesicherter Anzeige muss auch **mit einer fälschlichen Freimeldung gerechnet werden**, die durch einen Übertragungsfehler verursacht wird. In diesem Fall wird eine Regelfahrstraße nicht zustande kommen ohne, dass jedoch der Bediener die Ursache erkennen kann. Diese Fehler können, sollten sie länger andauern, nur durch die Fachkraft LST behoben werden.

Sicherheitskritisch scheint in diesem Fall vor allem das Erkennen der Situation durch den Bediener. Betrachtet man die Situation eines abgewiesenen Fahrstraßenanstoßes aus dem Blickwinkel des Bedieners so ist selbst bei Erkennen des Fehlers nicht sicher, ob noch weitere Fehler das Zustandekommen der Fahrstraße verhindert haben.

Um eine Räumungsprüfung dennoch durchführen zu können, muss – unter der Voraussetzung, dass andere Zugfahrten als Ursache ausscheiden – **sämtliche Sicherheitsverantwortung auf den Triebfahrzeugführer übertragen werden**. Dies ist mit dem Fahren auf Sicht und dem kontrollieren aller spitzbefahrenen Weichen sowie Bahnübergängen verbunden.

Nach der Zugfahrt und einer Zugschlussprüfung kann der AZA in Grundstellung gebracht werden. Sind Regelbedienungen wieder möglich, war dies der einzige Fehler, sonst liegt ein Anzeigefehler vor. Es ist dann wie oben beschrieben zu verfahren.

Um tatsächlich andere, vergessene **Zugfahrten als Fehlerquelle auszuschließen**, muss die Blockbelegung in ein Zugmeldebuch ausgedruckt werden und durch den Bediener kontrolliert werden oder es muss handschriftlich geführt werden. Es muss dann vor dem hilfsweisen Zulassen einer Zugfahrt kontrolliert werden.

Das Verwenden von Ersatzsignalen ist in diesem Zusammenhang fraglich, da ihr Anzeigen das gesichert sein des Fahrwegs durch den Fahrdienstleiter implizieren könnte. Vielmehr werden **schriftliche Befehle empfohlen** da dies die Besonderheit der Lage verdeutlicht. Auch muss ein Befehl in jedem Fall ausgeschrieben werden, da der Triebfahrzeugführer zur Kontrolle der spitz befahrenen Weichen aufgefordert werden muss. Dabei kann das **Ausstellen von Be-**

fehlen in den Bedienplatz integriert werden und die Funktionen des Ersatzsignals ablösen. Dies ist im Lastenheft ESTW-R bereits so vorgesehen.

Zusammenfassend noch einmal die Sicherheitsverantwortung die von den beteiligten Personen übernommen werden muss:

- Der Bediener muss feststellen, dass er **einen Fehler nicht orten kann** und darf sich selbst bei einem georteten Fehler sich nicht sicher sein, ob nicht ein zweiter Fehler vorliegt.
- Der Bediener muss bei Zulassung einer Zugfahrt ohne Hauptsignal **sicherstellen, dass keine feindliche Zugfahrt** die Ursache ist.
- Der Triebfahrzeugführer muss die **Streckensicherung übernehmen**.

Eine Ausnahme stellt die **Hilfsauflösung von Fahrstraßen** dar. Diese muss, wie international üblich zeitgesteuert erfolgen. Gleiches gilt für Blockhilfsauflösung und die Auflösung des Durchrutschwegs. Nach der abgelaufenen Zeit wird die Fahrstraße komplett aufgelöst, die elementweise Auflösung darf keine Anwendung finden.

These 13: Bei der hilfsweisen Zulassung einer Zugfahrt an einem Bedienplatz ohne gesichertem Meldebild, muss dem Lokführer die volle Verantwortung über die Fahrwegsicherung übertragen werden.

4.2.2 Kommandos an die Sicherungsebene mit Erfolgskontrolle

Die zweite zu betrachtende Gruppe ist die der Befehle an die Sicherungsebene, deren **Erfolgskontrolle Sicherheitsrelevant** sind, also bei denen nach der Befehlseingabe das Meldebild ausgewertet werden muss. Auch hier kann man sich die drei Szenarien denken:

a. Die Anzeige **stimmt mit der Sicherungsebene überein** und ist korrekt.
b. Die Anzeige **zeigt das Vorhandensein** einer Befahrbarkeitssperre o.a. an während diese **in der Sicherungsebene nicht eingespeichert ist**. (kritisch)
c. Die Anzeige **zeigt die Sperre nicht an, obwohl** diese auf der Sicherungsebene **hinterlegt ist**. (fail safe)

Szenario c. ist in zweierlei Hinsicht sicher. Zum einen **wirkt die Sperre wie gewünscht**, auch wenn der Bediener sie vergisst. Zum Anderen kann der Be-

diener **die fehlende Anzeigereaktion feststellen** und entsprechende Maßnahmen treffen.

Der **kritische Zustand b.** soll näher betrachtet werden. Aus Kapitel 3.3.1 ist bekannt, dass die Verarbeitung von Regelkommandos mit SIL 0 erfolgt während die Anzeige im Regelmodus SIL 2 erfüllt. Die Sicherungsebene selbst erfüllt immer SIL 4. Um Zustand c. zu erzeugen müsste ein Fehler der Sicherungsebene vorliegen da diese Stellkommando, Ausführung und Anzeige ursächlich miteinander verknüpft und ein Zusammentreffen eines zeitlich völlig zufälligen bestimmten Anzeigefehlers mit einem ebenso zufälligen Ausführungsfehler des Kommandos dessen Ausführung falsch angezeigt wird als unwahrscheinlich betrachtet wird. Fehler c. ist demnach sehr unwahrscheinlich.

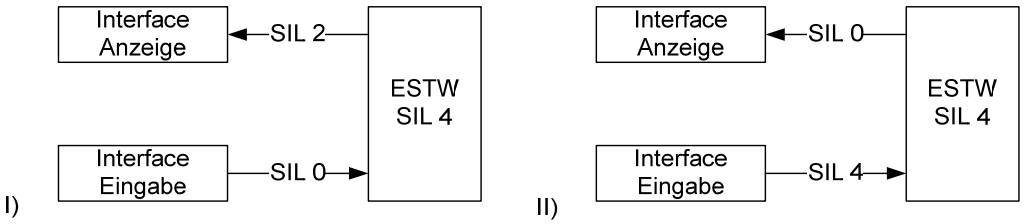

Abbildung 32 Anzeigen von Funktionen der Sicherungsebene

Abbildung 32 I stellte den gegenwärtigen Zustand dar, der offenbar vor allem zu Szenario a. tendiert. Will man auf eine Anzeigensicherung verzichten, so kann man, wie in Abbildung 32 II dargestellt, **über eine Befehlssicherung** die Wahrscheinlichkeit erheblich senken, dass der Befehl falsch oder nicht durchgeführt wird, die Anzeigesicherung ist dann nicht mehr grundsätzlich nötig, das System **tendiert eher zu dem als sicher betrachteten Szenario c.** Zusätzlich kann durch das Führen eines Zugmeldebuchs, also durch betriebliche Redundanz, die Fehlerwahrscheinlichkeit des Bedieners reduziert werden

Ist das **Ausschalten von leittechnischen Funktionen** Voraussetzung für die Zulassung einer Zugfahrt so muss dies **in die Zulässigkeitsprüfung mit aufgenommen werden**. Dies gilt für das Ausschalten der Weichenlaufkette, des Selbststellbetriebes und der Zuglenkung.

Tabelle 8 Maßnahmen bei Kommandos der Sicherungsebene[20]

Kommandos	WLS	SBA	ZBA	WUS	SS	BS	ME
Eingabesicherung	x	x	x	x	x	x	x
Einbinden in Zulässigkeitsprüfung	x	x	x				
In Zugmeldebuch eintragen				x	x	x	x

These 14: Ist bei Bedienungen die Erfolgskontrolle sicherheitsrelevant, so kann auch auf eine Eingabesicherung ausgewichen werden welche die Übertragung mit SIL 4 gewährleistet.

4.2.3 Spontan auftauchende Meldungen

Die laut (43) am schwierigsten zu beherrschenden Funktionen sind die spontan auftauchenden Meldungen und kontinuierlich zu überwachenden Funktionen der Sicherungsebene. (43) nennt als Beispiele **den Füm bei Zugfahrten ohne Hauptsignal** und **Störungsmeldungen von Fü-Büsa** die hier stellvertretend betrachtet werden sollen. Da die Meldung nicht wie in den anderen Fällen vom Bedienplatz stammt sondern in der sicheren Ebene selbst erzeugt wird, können nur folgende Szenarien eintreten:

- Die Meldung kommt zur Anzeige
- Die Meldung kommt nicht zur Anzeige (kritisch)

Tritt eine Zustandsänderung ein, z.B. eine Störungsmeldung eines Bahnübergangs, und wird diese nicht sicher an den Bediener übertragen, so entsteht ein gefährlicher Zustand da sie Meldung nicht in den Sicherungsprozess eingreift. Es ist daher nötig, diese Funktionen in die Stellebene zu integrieren, was im Fall der Fü-Büsa auch bereits umgesetzt wird (47).

[20] Die Funktionen wurden in Kapitel 3.4 erläutert.

Bei Zulassen einer **Zugfahrt ohne Hauptsignal** wurden bereits in Kapitel 2.5 verschiedene Ebenen der hilfsweisen Sicherung besprochen. Wird die Hilfsfahrstraße durch den Zustand **Füm-Ruhelicht** gesichert, besteht ein der Regelzugfahrstraße vergleichbarer Schutz. Beim Füm handelt es sich jedoch um ein künstliches Element der Sicherungsebene. Erlischt der Füm wegen einer durch Störung weggefallenen Bedingung nach bereits gegebener Fahrerlaubnis so entsteht ein **gefährlicher Zustand**, der Bediener muss **Maßnahmen zur Sicherung ergreifen**. Wird diese Zustandsänderung z.B. wegen eines Anzeigefehlers nicht angezeigt, ist dies nicht möglich. Es sind daher zusätzliche Sicherungsmaßnahmen erforderlich.

Wie bereits weiter oben ausgeführt muss der **Lokführer bei Fahrten ohne Hauptsignal** die Verantwortung für die **Fahrwegsicherung übernehmen** wenn der Stellwerksbediener ohne sichere Anzeige arbeitet. Dadurch ist dieses Problem relativ einfach gelöst. Um zu verhindern, dass Selbstellbetrieb oder Zuglenkung aufgrund der Störung flankierende Fahrstraßen einstellen können, sind die Kontrolle des ausgeschalteten Zustands in die Zulässigkeitsprüfung für das Vorsichtssignal/ den Befehl zu integrieren.

4.2.4 Zusammenfassung

Es wurde der **gänzliche Verzicht auf eine Anzeigesicherung diskutiert**. Dies geht einher mit der **Verlagerung der Sicherheitsverantwortung auf den Menschen** wobei auch der Triebfahrzeugführer einen wesentlichen Teil der Verantwortung tragen muss. Faktisch ist dies eine **Annäherung an den Zugleitbetrieb**, bei dem genau dies der Fall ist. Das Problem ist weniger die Durchführung von Hilfshandlungen als **zuverlässige Erkennung von Störungen**. Es muss daher beim hilfsweisen Zulassen einer Zugfahrt immer davon ausgegangen werden dass noch Hinderungsgründe vorliegen. Die einzige Möglichkeit trotzdem zu fahren ist, die **Verantwortung zur Fahrwegsicherung komplett auf den Triebfahrzeugführer zu übertragen**. Zusammenfassend noch einmal die nötigen Einschränkungen bei den Rückfallebenen:

- Bei Zugfahrten die ohne Hauptsignal zugelassen werden, muss der Lokführer die Verantwortung für die Fahrwegsicherung übernehmen. Dies beinhaltet die

Fahrt auf Sicht sowie das Kontrollieren und Sichern von spitzbefahrenen Weichen.
- Der Fahrdienstleiter muss sicherstellen, dass keine feindlichen Zugfahrten verkehren können. Dies kann über ein Zugmeldebuch geschehen, das von Hand oder per Drucker geführt wird, wenn der Fahrdienstleiter kontrollieren kann, dass die Zugbewegungen korrekt wiedergegeben werden.
- Sperren von Gleisabschnitten, Weichen und Signalen sollte über ein Zugmeldebuch dokumentiert werden.

Technische Maßnahmen sind zu treffen:

- Melder die eine Zustandsänderung der Sicherungsebene melden und die vom Bediener daraufhin überwacht werden müssen, sind in die Sicherungsebene einzubinden.
- Einbinden der Befehlsabgabe in das technische System, wie durch das Lastenheft ESTW-R bereits gefordert wird.
- Einbinden der Aus-Prüfung der Selbststellbetriebs und der Zuglenkung in alle Varianten, bei denen eine Zugfahrt ohne Hauptsignal zugelassen wird.
- Fahrstraßenhilfsauflösung mittels Zeitverzögerung einführen.

4.3 Sichern der Anzeige durch diversitäre Information

In diesem Kapitel soll auf der Grundlage der Ergebnisse über den Betrieb mit nicht sicherer Anzeige einige Methoden vorgestellt werden, welche die Sicherheitslücke zwischen nicht sicherem und sicherem Meldebild verkleinern sollen. Es wird dabei auf das in Kapitel 3.5 eingeführte **Prinzip der diversitären Datenübertragung** zurückgegriffen.

4.3.1 Hilfsumgehungen

Bereits mehrmals wurde in dieser Arbeit die Funktion FPÜ angesprochen. Dabei diente die Funktion immer der Vereinfachung komplizierter Bedienvorgänge. In diesem Fall tritt eine andere Eigenschaft der diversitären Datenübertragung in den Vordergrund.

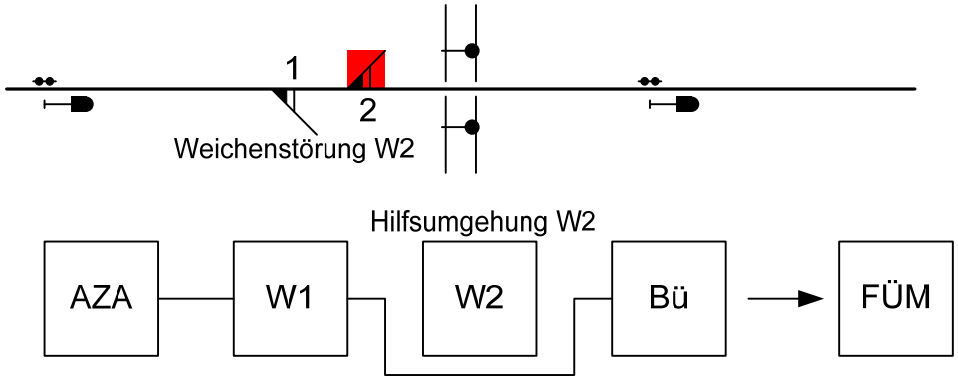

Abbildung 33 Prinzip der Hilfsumgehung

Geht man davon aus, dass **sicherheitsrelevante Bedienungen nur durchgeführt werden, wenn eine entsprechende Regelbedienung abgewiesen wurde**, also dass eine bestimmte Voraussetzung dafür nicht erfüllt ist, muss es auch immer möglich sein, dem Bediener per Extrafenster mitzuteilen, warum die Bedienung abgewiesen wurde. Eine an FPÜ angelehnte Funktion sollte daher bei jeder abgelehnten Regelbedienung die Gründe automatisch nennen, z.B. beim Umstellen einer Weiche mit WU sollte anstelle eines kleinen „Abgewiesen" in der Verarbeitungszeile, ein an Windows-Funktionen orientiertes Quittierungsfenster geöffnet werden mit der Information „Weiche yx nicht frei gemeldet – WU abgewiesen" Werden diese Meldungen diversitär übertragen, kann man von einer Anzeigensicherung genau für die sicherheitsrelevante Bedienung sprechen, deren zugehörige Regelbedienung abgewiesen wurde.

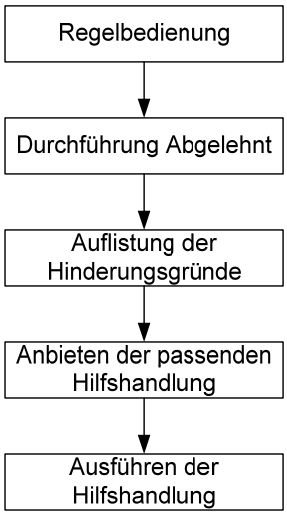

Abbildung 34 Durchführung von sicherheitsrelevanten Bedienungen mit FPÜ

Ordnet man jeder sicherheitsrelevanten Bedienung eine Regelbedienung zu, die zuvor abgewiesen worden sein muss und verknüpft das mit einer Hilfsumgehung erhält man den in Abbildung 34 dargestellten Ablauf. Dies ist mit einem erheblichen Sicherheitsgewinn verbunden denn der Bediener weiß genau, dass er sich nur um die im Quittierungsfenster genannten Probleme kümmern muss und alles andere technisch abgesichert ist.

These 15: Bei Anwendung einer an FPÜ angelehnten Funktion können auch ohne gesichertes Meldebild Zugfahrten sicher hilfsweise zugelassen werden, da alle Fehler diversitär an den Bedienplatz übertragen werden.

4.3.2 Diversitäre Rückmeldung

Der Sicherheitsrelevanz von **Erfolgsmeldungen für Kommandos auf Sicherungsebene** kann ebenfalls über ein diversitäres Quittierungsfenster Rechnung getragen werden. Das Telegramm muss erzeugt werden, wenn sich eine Zustandsänderung in der Sicherungsebene ergibt. Folgt das Quittierungsfenster einer entsprechenden Bedienhandlung, ist das Prinzip des Zusammenhangs von Ort und Zeit ebenfalls erfüllt.

Ist keine entsprechende Bedienhandlung vorausgegangen, handelt es sich um die **spontan auftauchenden Meldungen**, die schon mehrfach erwähnt wur-

den. Hier gilt zwar nicht das Kriterium des Zusammenhangs von Ort und Zeit, jedoch das der diversitären Übertragung. Im Gegensatz zur Erfolgskontrolle einer Bedienhandlung muss man sich in diesem Fall nicht sicher sein können, dass etwas passiert ist. Es ist vielmehr entscheidend, dass eine der beiden diversitären Meldungen angezeigt wird um den Bediener auf die Gefahr aufmerksam machen zu können. Ob dies bereits ausreicht kann hier nicht entschieden werden. Grundsätzlich sollten wie bereits festgestellt diese Meldungen in die Sicherungslogik eingearbeitet werden.

Die Quittierung der Fenster muss durch den Bediener erfolgen. Dabei muss dieser kontrollieren ob auch im graphischen Meldebild die entsprechenden Elemente korrekt angezeigt werden. Stattet man das Quittierungsfenster nur mit einer „Ok" Schaltfläche aus, erreicht man annähernd den gegenwärtigen Sicherheitsstandard. Der Lösungsvorschlag orientiert sich an (41).

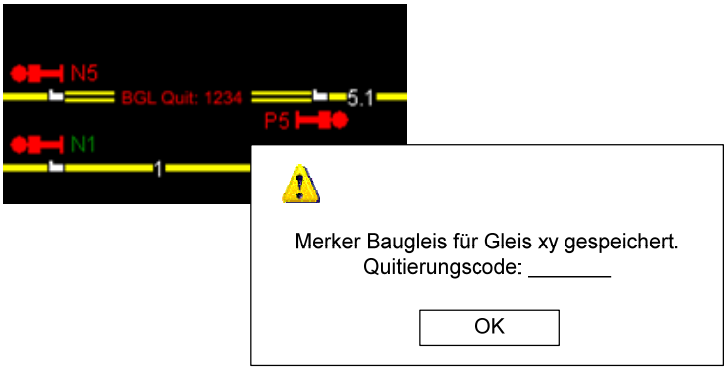

Abbildung 35 Zwangsauswertung der diversitären Meldung

Besser jedoch ist es wie in Abbildung 35, den Vergleich des Meldebilds mit dem Bedienfenster zu erzwingen. Der Grund ist wieder die Fehlerwahrscheinlichkeit des Menschen. Dies kann über ein Nummernfreigabeverfahren erfolgen. Ein in der Sicherungsebene generierter Code wird in den diversitären Meldungen mit übertragen. Er wird im grafischen Meldebild direkt an der entsprechenden Anzeige angezeigt und muss in das diversitäre Medium, dem Quittungsfenster eingegeben werden. Damit ist sichergestellt, dass beide Telegramme die gleiche Information übertragen hatten. Allerdings verlangt das ver-

sehen der Anzeigeelemente mit Quittungsnummern eine vermutlich relativ aufwendige durchgehende Modifikation der Anzeigelogik von der Sicherungsebene bis zur Grafikerzeugung. Möglicherweise ist der Aufwand aber bei Verwendung einer nicht-sicheren Anzeige vertretbar.

4.3.3 Zusammenfassung

Unter Verwendung einer an FPÜ angelehnten Funktion kann ein Großteil der fehlenden Anzeigesicherung kompensiert werden. Es werden in einem Extrafenster die Hinderungsgründe für das Einstellen einer Regelfahrt aufgezählt. Unter Umgehung der nun bekannten Störungen kann die restliche Fahrstraße gesichert werden. Die Störungen werden nun hilfsweise behandelt.

Spontan auftauchende Meldungen sollten nicht vorkommen. Ist es dennoch nötig, so wird eine diversitäre Übertragung und Anzeige der Meldung gefordert. Es ist in diesem Fall nur wichtig, dass die Meldung ankommt, ein Fehler auf einem Kanal ist noch nicht bedenklich. Das Erzwingen der Meldebildauswertung wird angesprochen.

Bei Bedienungen der Sicherungsebene, für die eine Erfolgsmeldung sicherheitsrelevant ist, wird das Einführen der Eingabesicherung empfohlen. Ein Fehler offenbart sich so mit hinreichend hoher Wahrscheinlichkeit. Zusätzlich ist eine Erfolgsmeldung in separatem Fenster diversitär anzuzeigen und das Fenster zu quittieren.

4.4 Anwendung der Verfahrenssicherung

Dem Leser wird möglicherweise die Ähnlichkeit der Vorschläge mit der Verfahrenssicherung der EBO 2 (Kapitel 3.2.5) aufgefallen sein. In der Tat sind die Unterschiede klein. Der Grund sich dem Thema noch einmal unbefangen zu nähern war die ablehnende Haltung von (43) zur Verwendung der EBO 2 im Bereich der Deutschen Bahn.

Begründung war der **hohe Bedienaufwand beim Prüfen von Fahrstraßenelementen** in größeren Betriebsstellen für die Zulassung einer Fahrt auf Er-

satzsignal. Dem kann jedoch entgegnet werden, dass unter Verwendung einer FPÜ Funktionalität der Aufwand keineswegs groß ist da nur die tatsächlich gestörten Elemente betrachtet werden müssen.

Weiterhin kann argumentiert werden, dass die diskutierten **ESTW-R vor allem im Bereich von Regionalstrecken zum Einsatz kommen** auf denen große Betriebsstellen eher selten vorkommen, nach der Modellstrecke des R 120 sind dies durchschnittlich alle 100 km. ESTW-As können bis zu 40 km (48) von der zugehörigen ESTW-Z entfernt stehen, was eine Ausstreckung von 80 km bedeutet. Es ist also je ESTW-R mit einer größeren Betriebsstelle zu rechnen. Dabei wird diese größere Station nur dem ESTW-R zugeschlagen, wenn sie nicht ebenfalls zu einer Strecke des Fern- und Ballungsnetz gehört was aber oft der Fall sein wird.

Es bleibt das **Problem der menschlichen Fehlerrate**. Bei dem besprochenen Verfahren wird noch mehr Verantwortung auf den Bediener übertragen als bei den in Deutschland üblichen Systemen. Unter Beachtung des in Kapitel 2.2.2 geschriebenen kann dies jedoch möglicherweise in Kauf genommen werden. Man bedenke, dass sich die Diskussion in dieser Arbeit nur für die seltenen Fälle des Verlassens der Regelebene gilt. Die geringere Sicherheit des Systems wirkt sich daher unterproportional aus. Um das System zur Anwendung zu bringen muss für den Spezialfall des Regionalverkehrs die gleiche Sicherheit nachgewiesen werden, was darum auch realistisch ist. Jedoch wurde bereits Zweifel daran geäußert, dass ein solcher Nachweis in naher Zukunft erfolgt.

4.5 Anwendung der „Verfahrenssicherung unter Einbindung von Personal vor Ort“

Mit Blick auf Kapitel 2.2.3 sollte auch dieses Verfahren (Kapitel 3.2.6) nicht ausgeschlossen werden. Geht man davon aus, dass an der Außenanlage letztlich immer Personal vorhanden ist, sei es der Triebfahrzeugführer, der Rangierer oder der Rottenführer, so können diese **unter Inkaufnahme von Wartezeiten** (Verfügbarkeit) in den Sicherungsvorgang einbezogen werden. Über den Austausch des Nummerncodes wird sichergestellt dass beide beteiligten den glei-

chen Kenntnisstand haben, durch die **doppelte Anzeige werden Anzeigefehler offenbart.** Es wird also bewusst darauf gesetzt, dass weiterhin zwei Personen am Verfahren beteiligt sind. Bei Ausfall des Bedienplatzes kann der Lokführer überdies seine Fahrstraße selbst einstellen.

Der Einsatz des Verfahrens hängt vor allem von der Bereitschaft ab, auf einen Teil der Verfügbarkeit zu verzichten. In welchem Umfang dies geschehen kann wurde in Kapitel 2.2.3 diskutiert und ist im Einzelfall zu entscheiden. Da bei ESTW-R auf Ersatzsignale verzichtet werden soll, muss der Lokführer einen schriftlichen Befehl entgegen nehmen. Dies darf nur bei Stillstand des Zuges erfolgen. Geht man davon aus, dass der Zug am Bahnsteig oder auf offener Strecke nur vor einem Signal hält, währe auch immer eine ÖBE in der Nähe. **Der zusätzliche Zeitbedarf** setzt sich also zusammen aus dem sichern und entsichern des Führerstands, dem Verlassen dem Besteigen des Zuges, dem Fußweg zur und von der ÖBE und dem durchführen des Prozedere.

Üblicherweise wird die Bedienung erfolgen, wenn der Zug am Bahnsteig steht und dem Fahrgastwechsel zur Verfügung steht. Hier ist der Weg von und zur ÖBE der kritische Vorgang. Je nach Standort des Zuges kann dieser bis zu 100 m betragen[21] und somit bei schnellem Gehen von 3 m/s 67 Sekunden, gut eine Minute. Berücksichtigt man die Zeit zur Durchführung des Procedere mit einer Minute und das sichern des Führerstands sowie das ein- und aussteigen mit 30 Sekunden, erhält man einen zusätzlichen Zeitbedarf von 2,5 Minuten. Beachtet man, dass nur Züge im Personenverkehr in dieser Entfernung von Signal halten, kann man eine Minute abziehen, in der gleichzeitig Fahrgastwechsel stattfindet. **Es ergibt sich eine Verzögerung von 1,5 Minuten.** Dies ist in Tabelle 9 zusammen gefasst. Ebenfalls wurde eine Schätzung für den selteneren Fall des Bedienens einer ÖBE am Einfahrtsignal durchgeführt.

[21] Maximallänge für Bahnsteige im Regionalverkehr sind 210 m nach Koril 813. Der Zug steht üblicherweise an der Bahnsteigmitte.

Tabelle 9: Geschätzte Verzögerungszeiten bei Bedienung der ÖBE

Vorgang	Bahnsteig	Einfahrsignal
Sichern und entsichern, Führerstand	30 s	30 s
Aus- und Einsteigen	23 s	60 s[22]
Fußweg zur/von der ÖBE	67 s	10 s
Durchführen Procedere	60 s	60 s
Gegenzurechnende Zeit	- 60 s[23]	- 20 s[24]
Summe	**90 s**	**140 s**

Weiterhin kann die Trennung von Infrastruktur und Fahrbetrieb als Grund gegen dieses Verfahren angeführt werden. Man müsste sich darauf einigen, dass diese politische Entscheidung hier nicht zielführend ist. Der durchaus sinnvollen Trennung ist bereits genüge getan, wenn die **Diskriminierungsfreiheit gewahrt bleibt**. Da jeder Lokführer, unabhängig von der Firma, die ÖBE bedienen muss, ist dies der Fall.

Trotzdem wird das Verfahren als Zwei-Mann-Bedienung von der DBAG nicht für den Standardbetrieb in Erwägung gezogen. Vielmehr werden Bemühungen von Seiten der DBAG angestellt, daraus wieder eine Ein-Mann-Bedienung zu entwickeln wie in (40) beschrieben. Dies wird vom Autor als unbrauchbar zurückgewiesen, da dies dem grundlegenden Gedanken des Verfahrens wiederspricht und ebenfalls auf einer Anzeigensicherung nach dem Rückleseverfahren (43) beruht. Es wird vielmehr empfohlen, den Umfang der Einbindung von Personal vor Ort auszuweiten, z.B. auf das Eingeben von Befahrbarkeitssperren. Es sollte hier das umgekehrte Verfahren angewendet werden. Der Rottenführer gibt eine Befahrbarkeitssperre ein welche durch den Bediener mittels einer generierten Nummer bestätigt werden muss. Beim Entfernen der Sperre wird wie-

[22] Abhängig vom Fahrzeug

[23] Gleichzeitiger Fahrgastwechsel

[24] Empfangen des gewöhnlichen Befehls entfällt

der der normale Ablauf angewendet. Gegenwärtig wird die Verantwortung für die Beachtung von Befahrbarkeitssperren dafür auf den Bediener übertragen.

Unter Inkaufnahme von Verfügbarkeitsverlusten wird eine hohe Sicherheit realisiert. Das Verfahren ist kompatibel zur besprochenen Verfahrenssicherung (EBO 2) und kann im selben Meldebild zur Anzeige gebracht werden. Dies ermöglicht eine Bahnhofsscharfe Entscheidung für eines der Verfahren.

5 Perspektiven

Bei ESTW nach Systemvertrag (Voll ESTW) wird das Auftragsvolumen über eine bestimmte Zeit, abhängig von den jeweiligen Lastenheften, festgelegt. Zwischen der DBAG und dem Hersteller ergaben sich so die verschiedenen Versionen der Systemverträge. Die Beauftragung zum Bau eines **ESTW-R hingegen** wird über Ausschreibungen durchgeführt. Es ist daher für den Hersteller von Sicherungstechnik von Bedeutung wie eine Anzeigensicherung vom Auftraggeber eingeschätzt wird, um Nachteile zu vermeiden.

Die **herstellerbezogenen Lebenszykluskosten** (LCC) setzen sich bei der Meldebildsicherung vor allem aus Entwicklungskosten und Zulassungskosten zusammen. Die Kosten für die eigentliche Hardware ist sind dagegen relativ gering. Ist der Hersteller in der Lage eine Anzeigensicherung mit anzubieten so hatte dieser bereits diesen Kostenaufwand und einen Vorteil gegenüber den Mitbewerbern. Es ist also im Interesse des Herstellers die Anzeigensicherung auch mit anzubieten und zu verkaufen. Das Anbieten einer ungesicherten Anzeige ist interessant, sobald dies zulässig ist und sich dadurch die Konkurrenzsituation ändert. Ein eigenes Bestreben zu einer nicht sicheren Anzeige kann aber von diesem Teilnehmer nicht erwartet werden.

Auf **Betreiberseite** ist man an einem möglichst niedrigen Kaufpreis interessiert. Nach den Gesetzen des Marktes ist dazu ein Käufermarkt nötig, also viele Anbieter. Der Verzicht auf die Forderung nach einer technischen Meldebildsicherung würde die Anzahl potentieller Anbieter erhöhen. Diese weisen eine wesentlich niedrigere Gewinnschwelle auf, da sie den Entwicklungsaufwand für die Meldebildsicherung noch nicht betrieben haben. Dies würde also zu wesentlich günstigeren Preisen führen. Anstrengungen in diese Richtung werden nach Ansicht des Autors nur sehr verhalten unternommen.

Die **betreiberseitige LCC** für ein Bedienplatzsystem setzt sich aus den Hauptkostenpunkten Anschaffungskosten und Betriebskosten zusammen. Die Kosten für die Anschaffung werden durch Verzicht auf die technische Meldebildsicherung sinken. Harte Betriebskosten wie Datenübertragungskosten ändern

sich nicht. Eine Möglichkeit, die Betriebskosten mit einzubeziehen bietet sich über die Monetarisierung der Zuverlässigkeit der einzelnen Systeme. Verspätungen sind ohne Zweifel ein Kostenfaktor und wird die Meldebildsicherung über ein betriebliches Verfahren realisiert erzeugt dies größere Verzögerungen als dies bei einer technischen Sicherung der Fall währe, siehe Kapitel 4.5. Ebenfalls die Sicherheit ist ein solcher Faktor. Da aber der Nachweis der gleichen Sicherheit erbracht werden muss, ist dies für diese Betrachtung hinfällig. Es kann also die Erstinvestition mit den kumulierten und monetarisierten zu erwartenden Verspätungen (siehe auch Kapitel 2.2.3) addiert werden. Diese Größe könnte ein Vergleichswert für die verschiedenen Anzeigesicherungssysteme ergeben. Der Zusammenhang von Investition und Zuverlässigkeit wurde bereits in Abbildung 6 und Abbildung 27 hergestellt.

Soll eine Verfahrenssicherung ohne Modifikation des Betriebsverfahrens zum Einsatz kommen, wird das Verfahren nach Vorbild der **EBO 2 empfohlen**. Es zeichnet sich durch hohe Flexibilität aus und ist Preiswert realisierbar. Da sich sicherheitsrelevante Prozeduren ändern, kann die Zulassung nur auf Basis einer Risikoanalyse für den Einsatzbereich des ESTW-R erfolgen. Da das System bereits erfolgreich bei der ÖBB eingesetzt wird, können möglicherweise Erfahrungen und Felddaten direkt in die Risikoanalyse mit eingehen und den Prozess dadurch vereinfachen. In diesem Fall bedarf es Erhebungen im Bereich der ÖBB. Der etablierte Hersteller von Sicherungstechnik im Bereich der ÖBB ist die Firma Thales, im Bereich der Schweizer Bundesbahn, die über ein vergleichbares Anzeigesicherungssystem verfügen, ist es die Firma Siemens. Beide Firmen könnten somit relativ unkompliziert diese Felddaten erheben.

Für eine abschließende Beurteilung sind **Untersuchungen zur Fehlerrate des Menschen** in seiner Eigenschaft als Bediener eines Stellwerks am Bildschirmarbeitsplatz nötig. Dabei muss vor allem die Wirksamkeit von Eingabesicherungsverfahren wie dem Kf-Verfahren untersucht werden. Ebenfalls muss die Herangehensweise an die Auswertung des Meldebilds untersucht werden. Dem deutschen Fahrdienstleiter wird hier zugemutet, ein komplexes Meldebild ohne Hilfestellung auszuwerten während bei der EBO 2 eine Checkliste ab-

gearbeitet wird. Diese Studien sind für die Beurteilung der Sicherheit von Bedienplätzen unabdingbar.

Es sollte auch in Betracht gezogen werden, **Betriebsverfahren und Sicherungssysteme mit formalen oder Methoden zu beschreiben**. Dadurch wird man im Idealfall in die Lage versetzt, z.B. bei Verzicht auf die Anzeigensicherung computergestützt die genauen Auswirkungen auf Rückfallebenen zu bestimmen, ohne Gefahr zu laufen, wichtige Punkte vergessen zu haben. Erfahrungen in diesem Bereich beschreibt (49).

Mit der Verwendung der Verfahrenssicherung kann das Einrichten von **Regionalnetz-Betriebszentralen** erleichtert werden. Regionalnetze bestehen oft aus zusammenhängenden oder separaten Streckenfragmenten. Dabei sind einige Fragmente im Zugleitbetrieb zu betreiben, andere mit ESZB und die wichtigen Strecken mit dem ESTW-R. Mit der Verfahrenssicherung für den Bereich der ESTW-R könnte eine gemeinsame Bedienoberfläche geschaffen werden. Je nach dem unter welchem Stellwerkstyp eine Hilfshandlung durchgeführt wird, wird die Verfahrenssicherung mit Einzelelementsicherung oder die Verfahrenssicherung unter Einbindung von Personal vor Ort angestoßen. Der Bediener muss nicht selbst unterscheiden zwischen den Verfahren, sondern erkennt es an der Menüführung. Möglicherweise wird das ESZB sogar hinfällig, wenn dessen größter Vorteil (das ungesicherte Meldebild) auch mit dem ESTW-R realisiert werden kann.

Die **Erkenntnis dieser Arbeit** ist zum einen, dass in nächster Zukunft eine Verfahrenssicherung nicht zum Einsatz kommen kann, da die benötigte Risikoanalyse nicht zur Verfügung steht. Zum anderen muss die Tatsache anerkannt werden, dass für überflüssige Sicherheit vor allem in den Regionalnetzen kein Geld zur Verfügung steht. Der Investitionsstau erreicht Dimensionen in denen akuter Handlungsbedarf gegeben ist (siehe Einleitung). Dabei kann moderner und attraktiver Nahverkehr ohne zeitgemäße Leit- und Sicherungstechnik nicht stattfinden da die Betriebskosten der Alttechnik zu hoch sind. Hersteller und Betreiber müssen in diesem Marktsegment weiter die Kosten senken und diese Arbeit hat verdeutlicht, dass das nötige Potential vorhanden ist.

6 Zusammenfassung

Vor dem Hintergrund des zunehmenden Modernisierungsbedarfs der Leit- und Sicherungstechnik für Strecken mit schwachem bis mäßigem Verkehr bedarf es einer angepassten und dadurch preiswerten Technik. Es wurde in dieser Arbeit untersucht, wie eine Vereinfachung von Bedienplätzen für elektronische Stellwerke realisiert werden kann.

Nach einer Einordnung des Themas in den Komplex der Diversifizierung von Leit- und Sicherungstechnik wurden theoretische Betrachtungen zum Zusammenhang von Sicherheit und Verfügbarkeit angestellt. Deren praktischer Realisierung mittels Redundanz sowie Gedanken deren bewussten Veränderung wurde diskutiert. Es wurde festgestellt, dass die Variation der Sicherheit einer Risikoanalyse bedarf, die Variation der Verfügbarkeit (Verspätungsminuten) einer genaueren Betrachtung mit Felddaten zur Verfügbarkeit von LST Elementen. Da beides nicht zur Verfügung steht musste diese Arbeit sehr vage in ihren Aussagen bleiben und sich auf rein qualitative Aussagen beschränken.

Es wurde auf das wichtige Kapitel der funktionalen Sicherheit eingegangen, mit dem Ziel den Leser nochmals mit den Grundlagen dieses oft missverstandenen Themengebiets zu konfrontieren um dadurch einer falschen Interpretation später gemachter Aussagen vorzubeugen. Dem folgte eine eher praktische Diskussion zur menschlichen Fehlerwahrscheinlichkeit in der festgestellt wurde, dass gegenwärtige Bedienplatzsysteme die Fehlerwahrscheinlichkeit des Menschen vermutlich zu hoch ansetzen.

Der Komplex schließt mit einer Betrachtung der Rückfallebenen im gegenwärtigen Betrieb in der verschiedene Arten von Rückfallebenen beispielhaft anhand der im Kapitel zum Zusammenhang von Sicherheit und Verfügbarkeit beschriebenen Zusammenhänge besprochen wurden.

Anschließend wurden die Anforderungen erarbeitet, die ein zulassungsfähiger Bedienplatz erfüllen muss. Dabei wurden gefolgt von Begriffsdefinitionen und der Erläuterung grundlegender Zusammenhänge die gegenwärtig verwendeten

Bedienplatzsysteme vorgestellt und bewertet, gefolgt von einer Diskussion über die Zulassung von Sicherungstechnik im Allgemeinen und Bedienplatzsystemen im Besonderen. Im letzten Kapitel dieses Teils werden die betrieblichen Forderungen an Bedienplatzsysteme analysiert. Abschließend wird noch auf betriebliche Paradigmen anderer Bahnen an den Beispielen der österreichischen ÖBB und dem schwedischen Banverket.

Die Diskussion zu Vereinfachung von Bedienplätzen wurde durch zwei grundsätzliche Ansätze bestimmt. Dabei wurde davon ausgegangen, dass die Sicherung der Datenübertragung und der Kommandoeingabe unproblematisch ist und gegebenenfalls die Sicherheit darauf verlagert werden kann.

Im ersten Ansatz wurde die Definition einer sicheren Anzeige angezweifelt. Dies geschah auf der Grundlage der Annahme, dass eine Funktion nur so sicher sein kann wie das unsicherste Teilsystem das zum funktionieren beiträgt. Dies ist im Falle der Hilfshandlungen der Bediener mit der dem Menschen innewohnenden Fehlerrate. Es wird empfohlen, die Anzeige nur mit SIL 2 zuzulassen und den marginalen Sicherheitsverlust durch das einführen der Funktion FPÜ und einer verbesserten Eingabekontrolle auszugleichen. Dies soll die Zulassungskosten für ein neues Produkt minimieren, das tatsächlich jedoch die gleichen Anforderungen erfüllt wie ein SIL 4 Produkt. Eine Veränderung des Betriebsverfahrens ist somit nicht nötig.

Im zweiten Ansatz wurde der gänzliche Verzicht auf eine Anzeigesicherung diskutiert. Dies geht einher mit der Verlagerung der Sicherheitsverantwortung auf den Menschen wobei auch der Triebfahrzeugführer einen wesentlichen Teil der Verantwortung tragen muss. Faktisch ist dies eine Annäherung an den Zugleitbetrieb, bei dem genau dies der Fall ist. Das Problem ist weniger die Durchführung von Hilfshandlungen als zuverlässige Erkennung von Störungen. Es muss daher beim hilfsweisen Zulassen einer Zugfahrt immer davon ausgegangen werden dass noch Hinderungsgründe vorliegen. Die einzige Möglichkeit trotzdem zu fahren ist, die Verantwortung zur Fahrwegsicherung komplett auf den Triebfahrzeugführer zu übertragen.

Unter Verwendung der Funktion FPÜ kann dieses Problem umgangen werden. Es werden in einem Extrafenster die Hinderungsgründe für das Einstellen einer Regelfahrt aufgezählt. Unter Umgehung der nun bekannten Störungen kann die restliche Fahrstraße gesichert werden. Die Störungen werden nun hilfsweise behandelt.

Spontan auftauchende Meldungen sollten nicht vorkommen. Ist es dennoch nötig, so wird eine diversitäre Übertragung und Anzeige der Meldung gefordert. Es ist in diesem Fall nur wichtig, dass die Meldung ankommt, ein Fehler auf einem Kanal ist noch nicht bedenklich. Das Erzwingen der Meldebildauswertung wird angesprochen.

Bei Bedienungen der Sicherungsebene, für die eine Erfolgsmeldung sicherheitsrelevant ist, wird das einführen der Eingabesicherung empfohlen. Ein Fehler offenbart sich so mit hinreichend hoher Wahrscheinlichkeit. Zusätzlich ist eine Erfolgsmeldung in separatem Fenster diversitär anzuzeigen und das Fenster zu quittieren.

Es wird die Verwendung der Verfahrenssicherung und der Verfahrenssicherung unter Einbindung von Personal vor Ort diskutiert. Erstere bringt einen Verlust an Sicherheit mit sich, letztere bringt einen Verfügbarkeitsverlust.

Es wird empfohlen, die Verfahrenssicherung analog der ÖBB im Rahmen des ESTW-R zu übernehmen da diese einen flexiblen Betrieb ermöglicht und preiswert in der Anschaffung ist. Zudem ist es dann denkbar, im Rahmen einer Regionalnetz-Bz ESZB und ESTW-R in dasselbe Bedienplatzsystem zu integrieren. Um die Zulassung dafür zu erreichen wird eine Risikoanalyse für den Bereich der Regionalnetze benötigt. Um die Sicherheit einzelner Bedienplatzsysteme beurteilen zu können werden Studien zur menschlichen Fehlerwahrscheinlichkeit benötigt. Solange diese Erkenntnisse nicht zur Verfügung stehen, ist eine Einführung der Verfahrenssicherung oder anderer Systeme nicht wahrscheinlich.

Literaturverzeichnis

1. **Bromet, Jörg.** Anforderungen des Betreibers an den Life-cycle in der Fahrwegsicherungstechnik. *Signal und Draht.* 2007, 1+2.

2. **DB Netz AG.** *Richtlinie 413.0301 Infrastruktur gestalten, Streckenstandards.* 2002.

3. **DB-Netz AG.** *Konzernrichtlinie 408 - Züge Fahren und Rangieren.* 2005.

4. —. Betriebliches und technisches Lastenheft für elektronische Stellwerke Regional. *Anlage 1 - Ausschlussliste der Funktionen.* 2004.

5. *Kommentar zum ESTW Marktsegment II.* **Eisermann, Klaus.** mündlich.

6. **DB-Netz AG.** *Betriebliches und technisches Lastenheft für elektronische Stellwerke Regional.* 2005.

7. *Komentar zum Lastenheft ESTW-R.* **Eisermann, Klaus.** 2007. mündlich.

8. **DB-Netz AG.** *Lastenheft für ein elektronisches Stellwerk für den Signalisierten Zugleitbetrieb.* Entwurf H.

9. **Sölch, Roland, et al.** Signalisierter Zugleitbetrieb - Teil 2 Technisch/Funktionale und Bedien-Anforderungen. *Signal und Draht.* 2004, 5.

10. **Wieland, Florian.** *Technische Unterstützung des Zugleitbetriebs am Beispiel der Strecke Dresden Kotsche - Königsbrück.* Dresden : s.n., 2005. Studienarbeit an der TU-Dresden. www.flowi.eu/Arbeiten/Studienarbeit_ZLB_Wieland.pdf.

11. **Maschek, Ulrich.** *Analyse zur Gestaltung Elektronischer Stellwerke, Diplomarbeit.* 1996.

12. **Weller, Martin.** Das ESTW L90 im technologischen Wandel. *Signal und Draht.* 2002, 9.

13. **CENELEC.** *EN 50 126 - Bahnanwendungen - Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS).* 1999.

14. **Schnieder, Eckehardd.** Verlässlichkeit von Verkehrssystemen im Verfügbarkeits-Sicherheits-Diagramm. *Signal und Draht.* 2003, 10.

15. **Anders, Enrico.** *Sicherheitswissenschaft, Vorlesungsskript der Profesur für Verkehrssicherheit, TU Dresden.* 2004.

16. **Berlin-Brandenburgische Akademie der Wissenschaften.** Digitales Woerterbuch der deutschen Sprache des 20. Jahrhunderts. *Redundanz.* [Online] 2003. [Zitat vom: 21. 07 2007.] www.dwds.de.

17. **Echtle, Klaus.** *Fehlertoleranzverfahren.* Heidelberg : Springer, 1990. http://dc.informatik.uni-essen.de/Echtle/all/buch_ftv/.

18. **Hofferer, Michael.** *Proseminar Redundanz, Vortrag 1: Informationstheorie.* s.l. : Universität Karlsruhe, Fakultät für Informatik, 1998/99.

19. **Knoll, Alois.** *Skript zur Vorlesung Echtzeitsysteme, Fehlertoleranz, TU München.*

20. **Baumann, Wolfgang H.** Was ist ein Funktionssicherheitssystem. *rams-software.de.* [Online] RAMS Wolfgang H Baumann - Ingenieurbüro / Beratung+Vertrieb, 03. 01 2007. [Zitat vom: 08. 07 2007.] http://www.rams-software.de/beratung/safety/61508/index.html.

21. **Herczeg, Michael.** Sicherheitskritische Mensch-Maschine-Systeme: Rahmenbedingungen für sicherheitsgerichtetes Handeln. [Buchverf.] Deutsches Atomforum e.V. *Berichtsheft der Jahrestagung Kerntechnik 2003.* Berlin : INFORUM Verlags und Verwaltungsgeselschaft, 2003.

22. **Hinzen, Albrecht.** Der Einfluss des menschlichen Faktors auf die Sicherheit der Eisenbahn. *Eisenbahntechnische Rundschau.* 1996, 10.

23. **Anders, Enrico.** Ein Beitrag zu Komplexen Betrachtung des Bahnsystems. *Signal und Draht.* 2004, 6.

24. **Pachl, Jörn.** Betriebliche Rückfallebenen auf Strecken mit selbsttätigem Streckenblock. *Signal und Draht.* 2000, 7+8.

25. **Zoeller, Hans-Joachim.** *Handbuch der ESTW-Funktionen.* Hamburg : Tetzlaff Verlag, 2002. ISBN 3-87814-802-X.

26. **Homeyer, Dietmar.** Zugfahrten, die nicht durch Fahrtstellung eines Hauptsignals zugelassen werden. *Deine Bahn.* 2003, 12.

27. **Forstreuter, Horst und Weitner-von Pein, Achim.** Verfahrensgesicherte Meldebildanzeige für den Fdl-Arbeitsplatz bei der Deutschen Bahn AG. *Signal und Draht.* 1994, 10.

28. **Christoph, Herbert und Schaper, Hans-Joachim.** BPS 900 - ein modernes Bedienplatzsystem für den Fahrdienstleiter-Arbeitsplatz. *Signal und Draht.* 1993, 3.

29. **Speiser, Norbert.** Ein Bedienkomando im ESTW mit besonderer Bedeutung: BEFA - Teil 1. *BahnPraxis Aktuell.* 2007, 5.

30. **Eisenbahn Bundesamt.** *Mü 8004 - Leitlinien und Grundprinzipien: Grundprinzipien für eine sichere Meldebildanzeige beim elektronischen Stellwerk und beim elektronischen Block.* 1998.

31. *Gespräch zum Thema "Sichere Anzeige".* **Schäfer, Michael.** Stuttgart : s.n., 2007. mündlich.

32. **Weiß, Alfred, Schmitt, Alfred und Müller, Dietrich.** Innovative Fernsteuerung von Alcatel für die U-Bahn München. *Signal und Draht.* 2000, 7+8.

33. **Eisenbahn Bundesamt.** *Mü 8004 - Leitlinien und Grundprinzipien, Grundprinzipien für eine sichere Meldebildanzeige beim elektronischen Stellwerk und in Betriebszentralen durch die Integrierte sichere Anzeige (ISA).* 1997.

34. **ÖBB - Infrastruktur Betrieb AG.** *Pflichtenheft Einheitsbedienoberfläche 2 (EBO 2) Bedienkatalog.* Wien : s.n., 2005.

35. **Adam, Klaus und Wiegmann, Holger.** ÖBE - Verfahrensgesicherte Eingabe von Hilfshandlungen. *Signal und Draht.* 2005, 5.

36. **Kammel, Karl und Schneider, Friderich.** Technische Zulassung von Eisenbahnsicherungsanlagen unter dem Aspekt des Übergangs von nationalen zu europäischen Sicherheitsstandards. *Eisenbahningenieurskalender.* 2002.

37. *Präsentation zur ESTW-Risikoanalyse Teil 2 der Deutschen Bahn AG.* **Eberhardt, Markus.** 2007.

38. **Ziegler, Peter, Kupfer, Lars und Wunder, Hans-Jörg.** Erfahrungen mit der Risikoanalyse Elektronisches Stellwerk (DBAG). *Signal und Draht.* 2003, 10.

39. *Gespräch zur Risikoanalyse ESTW.* **Hoeft, Manuel.** Berlin : s.n., 2007. mündlich.

40. **Hoeft, Manuel und Oberländer, Werner.** Bediensysteme für Stellwerke auf Strecken mit geringer Betriebsdichte. *Signal und Draht.* 2007, 4.

41. *Diskussion von Aspekten der bedienerunterstützten sicheren Bedienoberflächen in der LST.* **DB Systemtechnik, Leit- und Sicherungstechnik. Zugbildungstechnologie.** Dresden, MDG-Fachausschusstagung „Telematik“ : s.n., 2005.

42. **Pachl, Jörn.** Vorschlag für eine neue Systematik der Betriebsverfahren deutscher Eisenbahnen. *Eisenbahningenieur.* 2004, 7.

43. *Gespräch zu Bedienplatzsystemen.* **Hoeft, Manuel.** Berlin : s.n., 2007. mündlich.

44. **DB-Netz AG.** *Richtlinie 482.9012 Signalanlagen bedienen - Elektronisches Stellwerk El S - Bedienkomandos und Funktionsbezeichnungen - Anhang 4.* 1998.

45. **Banverket, Stab Trafiksäkerhet och Tagplanering.** *SJF 010.16 - Föreskrifter för användning av fjb-indikeringssystem m.m. (Schwedisch: Vorschiften für die Nutzung von Anzeigen ferngesteuerter Stellwerke).* 1994.

46. **Banverket.** BVF 900.3 - Säkerhetsordning (Schwedisch: Fahrdienstvorschrift der schwedischen Bahn). *§ 29 (7.1) Maßnahmen vor dem beginn von Arbeiten auf der Strecke oder unbesetzten Stationen.* 2000.

47. *Komentar zu Fü-Büsa.* **Eisermann, Klaus.** Stuttgart : s.n., 2007. mündlich.

48. **Thales Rail Signalling Solutions.** *Planunfshandbuch ESTW L 90 - Stellentfernungen.* Stuttgart : s.n., 2006.

49. **Eriksson, L.-H. und Falen, Maria.** *An Interlocking Specification Language.* Uppsala : s.n., 1999.

50. **Maschek, Ulrich.** *Vorlesungsskript Verkehrssicherungstechnik, Professurfür Verkehrssicherungstechnik, TU Dresden.* Dresden : s.n., 2004.

Abbildungs- und Tabellenverzeichnis

Abkürzungsverzeichnis

Aoz	Ausfalloffenbarungszeit
ASP	Arbeitsplatzrechner
AWU	Aufgefahrene Weiche umstellen
AZG	Achszähleinrichtung in Grundstellung bringen
BEFEHLA	Schriftlichen Befehl abgeben (in ESTW Sicherungslogik eingebunden), Zustand Füm-Blinkend ist erreicht
BEFEHLB	Schriftlichen Befehl abgeben (in ESTW Sicherungslogik eingebunden), Wlk ist ausgeschaltet.
Berü	Bereichsübersicht
Bf	Bahnhof
BHA	Block hilfsauflösen
BPR	Bedienplatzrechner
Bsp.	Beispiel
Bz	Betriebszentrale
COMS	Comunikationsserver
CRC	Cyclic redundancy check – Zyklische Redundanzprüfung
DBAG	Deutsche Bahn Aktiengesellschaft
DB-Netz AG	Deutsche Bahn-Netz Aktiengesellschaft
D-Weg	Durchrutschweg
EAM	Elementansteuermodul
EBA	Eisenbahnbundesamt
EBO 2	Einheitsbedienoberfläche 2
EE1/LE1	Ersatzsignal einschalten 1/ Linksfahrersatzsignal einschalten 1
EE2/LE2	Ersatzsignal einschalten 2/ Linksfahrersatzsignal einschalten 2
EN	Europäische Norm
ESTW	Elektronisches Stellwerk
ESTW A	Abgesetztes elektronisches Stellwerk
ESTW L 90	ESTW der Firma Thales
ESZB	Elektronisches Stellwerk für den SZB
EUC	Equipment under Control
FAHE	Fahrstraße elementweise hilfsauflösen
FHA	Fahrstraße hilfsauflösen
FPÜ	Fahrstraßenprüfung und überwachung
Füm	Fahrstraßenüberwachungsmelder
ISA	Integrierte sichere Anzeige
ISDN	Integrated Services Digital Network
KA	Komunikationsanzeige
Kf	Kommandofreigabe

KLO	Anschlusskennung löschen
Koril	Konzernrichtlinie der DBAG
LCC	Life Cycle Costs - Lebenszykluskosten
LST	Leit- und Sicherungstechnik
max	Maximal
ME	Merker eingeben
MEM	Melde- und Eingabemodul
MMI	Man machine interface – Mensch-Maschine-Schnittstelle
MOS	Monitorserver
MS	Marktsegment
o.a.	oder andere(s)
ÖBB	Österreichische Bundesbahn
ÖBE	Örtliche bedieneinrichtung
RSTW	Relaisstellwerk
SBA	Selbststellbetrieb ausschalten
SEL	Standard electric Lorenz
Sh1	Rangiersignalbegriff
SIL	Safety integrity level - Sicherheitsintegritätslevel
SLHE	Schlüsselsperre hilfsweise entsperren
SM	Sicherungsmodul
SS	Signal sperren
SZB-E	Signalisierter Zugleitbetrieb mit elektronischen Stellwerk
TAN	Transaktionsnummer
Tft	Thinn film transistor – spezielle Bauform des Feldeffekttransistors zur Verwendung in Flachbildschirmen
UHA	Bahnübergangseinrichtung hilfsausschalten
UHF	Bahnübergangseinrichtung hilfsfreimeldung
Uz/Z	Unterzentrale/Zentrale eines ESTW
VAZG	Vorbereitende Achszählgrundstellung
VE1	Vorsichtssignal ein 1
VE2	Vorsichtssignal 2
WHU	Weiche hilfsumstellen
Wlk	Weichenlaufkette
WLS	Weichenlaufkette sperren
WUS	Weiche gegen umstellen sperren
z.B.	Zum Beispiel
ZBA	Zuglenkung ausschalten
Zs1	Zusazsignal 1 (Ersatzsignal)