(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 036 800 A2**

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
18.03.2009 Patentblatt 2009/12

(51) Int Cl.:
B61L 21/04 *(2006.01)*

(21) Anmeldenummer: **08011454.9**

(22) Anmeldetag: **24.06.2008**

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR
Benannte Erstreckungsstaaten:
AL BA MK RS

(30) Priorität: **11.09.2007 DE 102007043053**

(71) Anmelder: **Deutsche Bahn AG**
10785 Berlin (DE)

(72) Erfinder:
- **Kalberlah, Henning**
  38176 Wendburg (DE)
- **Bauer, Erik**
  55452 Guldental (DE)

(74) Vertreter: **Zinken-Sommer, Rainer**
Deutsche Bahn AG
Patentabteilung
Völckerstrasse 5
80939 München (DE)

(54) Signaltechnisch sichere elektronische Elementansteuerung zum Durchführen eines Fahrbetriebes von Schienenfahrzeugen

(57) Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur signaltechnisch sicheren elektronischen Ansteuerung von Elementen, die den Fahrbetrieb von Schienenfahrzeugen leiten und sichern.

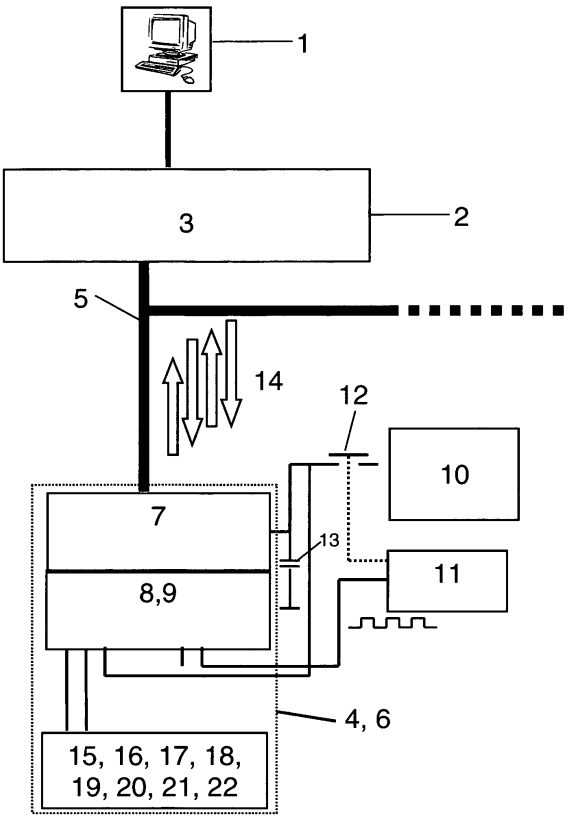
Hierbei wird unter Verwendung industrieller Standards für Leit- und Sicherungstechnik in einem elektronischen Stellwerk effizient und kostengünstig die elektronische Ansteuerung von Elementen, die den Fahrbetrieb von Schienenfahrzeugen leiten und sichern, dadurch realisiert, dass die sicherheitsgerichteten Prüfungen und Algorithmen zur Gewährleistung der Verfahrenssicherheit ausschließlich vom sicheren Rechnersystem der Sicherungsebene geleistet werden, wohingegen die Rechner beziehungsweise sonstigen Komponenten der Bedien- und Beobachtungsebene sowie der Prozessebene geringeren Sicherheitsansprüchen genügen können.

Hierbei ist auch die geforderte sichere Anzeige und Bedienung gewährleistet.

Der hohe Aufwand für sicheres Software-Design, sichere Programmierung und

Prüfung sowie sichere Hardware ist nur an der einen Stelle im sicheren Stellwerkskern erforderlich.

Figur 1



EP 2 036 800 A2

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur signaltechnisch sicheren elektronischen Ansteuerung von Elementen, die den Fahrbetrieb von Schienenfahrzeugen leiten und sichern.

[0002] Der Fahrbetrieb von Schienenfahrzeugen wird bei technisch gesicherten Strecken zentral von einem für den entsprechenden Infrastrukturbereich zuständigen Stellwerk geleitet und gesichert.

[0003] Die Elemente der Außenanlage des Stellwerks, wie z.B. Signale, Weichen, Bahnübergänge, Blockeinrichtungen etc. müssen von der Stellwerkslogik dabei signaltechnisch sicher gesteuert und überwacht werden, das heißt, dass sich die Elemente der Außenanlage mit hinreichend großer Wahrscheinlichkeit auch bei beliebig anzunehmenden Fehlern im System in einem Zustand befinden, der die Sicherheit des Fahrbetriebs nicht gefährdet.

[0004] Die signaltechnische Sicherheit von Stell- und Überwachungseinrichtungen wird mithilfe sicherungstechnischer Bauelemente realisiert, wobei alle in die Stellund Überwachungsvorgänge eingebundenen Komponenten entsprechend überprüft werden.

[0005] Eine vergleichende Übersicht der bei verschiedenen Bahnverwaltungen im Einsatz befindlichen unterschiedlichen elektronischen Stellwerkstypen hinsichtlich der verwendeten Rechnerkomponenten, Systemstrukturen, Sicherheitskonzepte sowie Gestaltung von Hard- und Software ist in dem Artikel "Sicherungs- und

[0006] Telekommunikationstechnik" in Signal + Draht 3, 1997, beschrieben. Die im Einsatz befindlichen Systeme unterscheiden sich unter anderem hinsichtlich Ein- oder Zweikanaligkeit, sicherer beziehungsweise nicht sicherer Bediensysteme, Betriebskonzept und Kosten.

[0007] So ist insbesondere in deutschen ESTW eine sichere Anzeige und Bedienung erforderlich.

[0008] Beispiele für die Systemarchitektur in deutschen ESTW finden sich in den Übersichtsartikeln "SIMIS D", in Signal + Draht 3, 2006 sowie "Die Bombardier-Lösung einer neuen ESTW-Bauform bei der DB AG", in Signal + Draht 5, 2005.

[0009] Alle etablierten, vornehmlich proprietären elektronischen LST-Konzepte basieren auf "Verfahrenssicherungen". Zum Beispiel besteht ein klassisches 2-von-3-Prozessorsystem aus marktüblichen elektronischen Bauteilen, wie beispielsweise dem Intel Pentium 1. Eine in den Standardprozessoren programmierte spezifische Applikation bildet die Sicherheitsmechanismen ab. Die Ergebnisse der Prüf-Applikationen werden auf aus Standard-Halbleiterbauelementen entworfenen Hardwarepartitionen verglichen und im Fehlerfall Sicherheitsabschaltungen ausgelöst.

[0010] Teilweise werden die Grundsätze der Verfahrenssicherung bereits heute in der Eisenbahnsicherungstechnik angewendet.

[0011] Für sicherheitsgerichtete Bedienungen in einem Stellwerk ist eine Verfahrenssicherung von Quelle zu Senke implementiert. Die von der DB AG vorgeschriebene firmenneutrale SBS-Schnittstelle definiert entsprechende Dialoge. Über korrespondierende Prozeduren im sicheren Stellwerkskern und im Bedienplatz wird für den Fall einer sicherheitskritischen Bedienung eine Fehlfunktion der Schnittstelle und der Anzeige mit ausreichender Wahrscheinlichkeit ausgeschlossen.

[0012] Um die hohen Sicherheitsanforderungen auch bei Bedienung und Anzeige zu erfüllen, war man allerdings bisher dazu gezwungen, nicht nur im Stellwerkskern sichere Rechnertechnik einzusetzen, sondern auch in den Bereichen der Elementsteuerung und Bedienung/Anzeige. Damit befinden sich an beiden Enden des Verfahrens, also bei Quelle und Senke, sichere und damit kostenintensive Komponenten.

[0013] In DE 10 2005 043 305 A1 ist eine System-Architektur zur Steuerung und Überwachung von Komponenten einer Eisenbahnsicherungsanlage beschrieben. Hierbei ist eine Automatisierungsplattform, die mehrere Module, insbesondere CPU, Stromversorgung, Modul für sicherheitsrelevante Signalverarbeitung, Modul für nicht sicherheitsrelevante Signalverarbeitung, Kommunikationsmodul, umfasst, über spezielle Schnittstellen mit sicherheitsrelevanten und nicht sicherheitsrelevanten Komponenten der Eisenbahnsicherungsanlage verbunden. Als Automatisierungsplattform dient eine speicherprogrammierbare Steuerung (SPS). Die vorgegebene Softwarestruktur der Automatisierungsplattform ist üblicherweise derart modular oder hierarchisch geordnet, dass die Logistik der Eisenbahnsicherungsanlage, insbesondere die Stellwerkslogistik, in funktionsspezifischen Softwareprogrammen organisiert werden kann.

[0014] Aus DE 196 06 894 C2 ist eine Einrichtung zur signaltechnisch sicheren Steuerung und Überwachung elektrischer Verbraucher im Eisenbahnwesen bekannt, bei der jeder Verbraucherstromkreis mindestens zwei in Reihe liegende, unabhängig voneinander steuerbare, signaltechnisch nicht sichere Schalter zum Öffnen/Schließen des Stromkreises aufweist. Die beiden Schalter sind durch unabhängige Rechnerkanäle eines sicheren Rechnersystems steuerbar. Jede Ader des Stromkreises enthält einen der beiden Schalter. Es ist mindestens ein Melder zum Erkennen einer aus einem über den Verbraucher fließenden Speise- oder Prüfstrom abgeleiteten oder vom Verbraucher mindestens mittelbar aufgeschalteten, vom Betriebszustand des Verbrauchers abhängigen Prüfspannung vorgesehen. Ein zur Unzeit geschlossener oder geöffneter Schalter verändert die Spannung in markanter Weise gegenüber der sich bei ordnungsgerechter Schalterstellung einstellenden Prüfspannung. Die Melder-Ausgangssignale werden von den beiden Rechnerkanälen des sicheren Rechnersystems bewertet, und das Rechnersystems erkennt ein unzeitiges Offensein/Geschlossensein mindestens eines der Schalter aus dem Auftreten von zu dieser Zeit nicht erwarteten Melder-Ausgangssignalen.

[0015] Aus DE 100 53 023 C1 ist ein Verfahren zum

Steuern eines sicherheitskritischen Bahnbetriebsprozesses und eine Einrichtung zur Durchführung dieses Verfahrens bekannt. Hierbei wird mindestens ein signaltechnisch sicherer Rechner verwendet, der aus eingehenden Kommandos nach Maßgabe einer Bahnbetriebsordnung signaltechnisch sicher erarbeitete Stellbefehle signaltechnisch sicher an Prozesselemente ausgibt und von dort stammende Meldungen einer Prozesszustandsüberwachung und Prozesssteuerung zuführt. Dabei wird im sicheren Rechner lediglich eine Systemsoftware hinterlegt, deren Programme den sicheren Rechner befähigen, eine signaltechnisch sichere Ein-/Ausgabe und den signaltechnisch sicheren Datenvergleich vorzunehmen. Die für den Bahnbetriebsprozess entscheidenden vorgegebenen Bedingungen und

[0016] Abhängigkeiten sind in einem oder mehreren nicht signaltechnisch sicheren kommerziellen Rechnern hinterlegt. Dabei erzeugt der signaltechnisch sichere Rechner aus den ihm zugeführten Kommandos und Meldungen Verarbeitungsaufträge, die an den oder die kommerziellen Rechner übermittelt werden und dort mindestens zweimal unabhängig voneinander abgearbeitet werden. Die dabei erarbeiteten Ergebnisse oder Zwischenergebnisse werden an den sicheren Rechner zurück übermittelt und dort signaltechnisch sicher auf inhaltliche Übereinstimmung geprüft.

[0017] Gemeinsamer Nachteil des oben beschriebenen Stands der Technik ist die immer noch recht aufwändige und damit kostspielige Systemarchitektur; auch bezogen auf die in Deutschland geforderte sichere Bedienung und Anzeige, die technisch umgesetzt werden muss.

[0018] Bei den etablierten Lösungen sorgen spezielle, herstellerspezifische "Stellteile" für die Anpassung an die bahnspezifischen Gegebenheiten und die Isolation.

[0019] Durch lange, sternförmige Kupferverbindungen zu den Außenelementen müssen hohe Spannungsfestigkeit und verschiedene Kabelfehler durch die Stellteile beherrscht werden. Dies führt klassischerweise zu aufwändigen bahnspezifischen Sonderentwicklungen.

[0020] Traditionell wird bei den Stellteilkonzepten bisher nicht das gewünschte Ereignis ausgewertet. Beim Signal wird z. B. der Lampenstrom geprüft und daraus gefolgert, ob die Signallampe mit ausreichender Wahrscheinlichkeit leuchtet. Bei Weichen geht man von einer formschlüssigen Verbindung der Stellstangen und der Lager- und Übertragungsteile mit den Weichenzungen oder dem Herzstück aus und wertet entsprechende Schalterpakete (meistens im Weichenantriebsgehäuse) für die Rückmeldung des Zustandes der Weiche aus. Die verwendeten 4-Draht Schaltungen reduzieren und verkomplizieren dazu noch die Anzahl der Rückmeldungen und deren sicherungstechnische Plausibilitätsprüfungen.

[0021] Es ist somit Aufgabe der Erfindung, unter Verwendung industrieller Standards für Leit- und Sicherungstechnik in einem elektronischen Stellwerk die elektronische Ansteuerung von Elementen, die den Fahrbetrieb von Schienenfahrzeugen leiten und sichern zu realisieren und dabei möglichst effizient und kostengünstig den hohen Anforderungen hinsichtlich Sicherheit und Funktion im Netz der Deutschen Bahn AG zu genügen.

[0022] Hierbei ist auch die geforderte sichere Anzeige und Bedienung zu gewährleisten.

[0023] Diese Aufgabe wird gemäß den Merkmalen des Oberbegriffs des Patentanspruchs 1 gelöst.

[0024] Die Systemarchitektur orientiert sich am bewährten industriellen Ebenenmodell, bestehend aus einer Bedien- und Beobachtungsebene, einer Sicherungsebene und einer Prozessebene.

[0025] Erfindungsgemäß stellt ein vollgrafisches, auf Marktstandards basierendes System die Bedien- und Beobachtungsebene dar.

[0026] Die Sicherungsebene wird von einem sicheren Rechnersystem gebildet.

[0027] In der Prozessebene befinden sich die anzusteuernden Elemente der Außenanlage sowie andere signaltechnische Einrichtungen, wie Nachbarstellwerke, Blockeinrichtungen, Bahnübergänge, etc.

[0028] Die Komponenten der verschiedenen Ebenen kommunizieren über entsprechende Datenübertragungseinrichtungen.

[0029] Die sicherheitsgerichteten Prüfungen und Algorithmen zur Gewährleistung der Verfahrenssicherheit werden ausschließlich vom sicheren Rechnersystem der Sicherungsebene geleistet, wohingegen die Rechner beziehungsweise sonstigen Komponenten der Bedien- und Beobachtungsebene sowie der Prozessebene geringeren Sicherheitsansprüchen genügen können.

[0030] Das Verfahren basiert sicherheitstechnisch auf einer Variante der bekannten Verfahrenssicherung, wobei erfindungsgemäß die Sicherungsprozeduren zwar jeweils konsequent an den Endpunkten (Quelle und Senke) der Aktionen greifen, die Zwischen- und Endergebnisse jedoch nur im sicheren Stellwerkskern geprüft werden. Somit lässt das Verfahren für alle Komponenten außerhalb des sicheren Stellwerkskerns, das heißt sowohl für die Kommunikation als auch für die Prozessebene, kostengünstige Komponenten nach Industriestandard zu, die einem geringeren Sicherheitslevel genügen.

[0031] Ein großer Vorteil des Verfahrens ist, dass der hohe Aufwand für sicheres Software-Design, sichere Programmierung und Prüfung sowie sichere Hardware nur an der einen Stelle im sicheren Stellwerkskern erforderlich ist.

[0032] Durch Anwendung der CENELEC-Normen ist eine quantitative Betrachtung des Fehlverhaltens einzelner Module, Programme und Datenverbindungen möglich, so dass sich unterschiedliche Arten der Verfahrenssicherung hinsichtlich der geforderten SIL berechnen lassen.

[0033] In Anspruch 2 ist beschrieben, wie von dem Verfahren Befehle zur Ansteuerung von Elementen der Prozessebene sicher ausgelöst werden. Dabei muss unterschieden werden, auf welchem Weg Befehle an die Prozessebene erteilt werden.

[0034] Wenn Befehle von der Bedienereingabe auf der Bedien- und Beobachtungsebene eingegeben werden, so werden diese mit einer Datenübertragungseinrichtung an das sichere Rechnersystem in der Sicherungsebene übertragen, und dort auf Plausibilität überprüft. Plausible Befehle werden neu codiert, und an die Bedien- und Beobachtungsebene zurück übertragen. In dem mindestens einen Rechner der Bedien- und Beobachtungsebene wird der neu codierte Befehl des sicheren Rechnersystems ebenfalls auf Plausibilität überprüft und das Ergebnis der Plausibilitätsprüfung in final codierter Form an das sichere Rechnersystem in der Sicherungsebene übertragen.

[0035] Zusätzlich muss im Allgemeinen bei solchen sicherheitsrelevanten manuellen Bedieneingaben über einen separaten Kommunikationsweg gewährleistet werden, dass die Bedienung in dieser Form explizit gewünscht ist. Hierfür wird insbesondere ein gedoppelter oder antivalenter Kontakt geschlossen, und/oder werden zusätzlich codierte digitale Adressen eingelesen und geprüft.

[0036] Sind alle diese Bedingungen erfüllt, so ist mit ausreichender Sicherheit davon auszugehen, dass eine Elementansteuerung von der Bedien- und Beobachtungsebene einerseits tatsächlich gewünscht ist und andererseits der Befehl plausibel ist sowie die Kommunikation mit dem Element und die richtige Adressierung des Elementes in der Prozessebene einwandfrei funktioniert. Dementsprechend kann der Befehl zur Ansteuerung des Elements vom sicheren Rechner ausgelöst werden.

[0037] Sobald jedoch mindestens eine der zuvor genannten Plausibilitätsüberprüfungen der verwendeten Befehle in mindestens einem der beteiligten Rechner negativ ausfällt, muss die Ansteuerung von Elementen der Prozessebene mit einer entsprechenden Fehlermeldung sicher abgebrochen werden.

[0038] Werden die Befehle zur Ansteuerung von mindestens einem Element der Prozessebene aufgrund des internen Programmablaufs im sicheren Rechnersystem der Sicherungsebene erteilt, so wird von dem sicheren Rechnersystem der Sicherungsebene die Ansteuerung direkt ausgelöst.

[0039] In Anspruch 3 ist beschrieben, wie das von dem gemäß Anspruch 2 ausgelösten Befehl erzeugte Ansteuerungsereignis signaltechnisch sicher überwacht wird.

[0040] Nachdem der Befehl zur Ansteuerung eines Elements der Prozessebene vom sicheren Rechnersystem der Sicherungsebene ausgelöst wurde, wird er über eine Datenübertragungseinrichtung an das passende Element in der Prozessebene übertragen. Die Wirkung dieses Befehls führt zu mindestens einem Ansteuerungsereignis, dessen Ergebnis von einer geeigneten Sensorik überwacht und an das sichere Rechnersystem in der Sicherungsebene zurückgemeldet wird. Die Ergebnisse eines jeden Ansteuerungsereignisses müssen mehrfach hinsichtlich der geforderten logischen und zeitgerechten Abfolge überprüft werden. Da nur ein sicheres Rechnersystem im sicheren Stellwerkskern zur Verfügung steht, müssen alle Prüfungen auch dort erfolgen. Dies wird durch mehrfache, aber zeitversetzte Prüfungen im einzigen sicheren Rechnersystem realisiert, so dass für jedes Ergebnis Mehrfachdialoge entstehen, die bis hin zum Endergebnis geführt werden. Nach positiver Prüfung aller Ergebnisse zu den Ansteuerungsereignissen wird im sicheren Rechnersystem von einer erfolgreichen Elementansteuerung ausgegangen und dies offenbart. Ergibt die Prüfung von mindestens einem Ergebnis der Ansteuerungsereignisse in mindestens einem der Mehrfachdialoge einen Widerspruch zur geforderten logischen und zeitgerechten Abfolge, so geht das sichere Rechnersystem von einer fehlerhaften Elementansteuerung aus und offenbart auch dies.

[0041] Die mehrfache, zeitversetzte Prüfung der unterschiedlichen Ereignisse an nur einer Stelle im sicheren Stellwerkskern erfordert eine leistungsfähige Rechnerarchitektur. Sie muss sicherstellen, dass der Zeitaufwand für die je nach gewünschtem Sicherheitslevel erforderlichen Prüfungen und das anschließende Stellen der Elemente der Prozessebene nicht mehr Zeit aufgewendet wird, als die von der Zulassungsbehörde geforderte Maximalzeit, innerhalb der der Signalbegriff "Halt" gezeigt werden muss (Haltfallzeit).

[0042] Die heute zur Verfügung stehenden, erprobten Prozessoren und Kommunikationssysteme machen dies möglich.

[0043] Gemäß Anspruch 4 besteht eine vorteilhafte Ausgestaltung der Erfindung darin, dass das sichere Rechnersystem der Sicherungsebene aus einem modularen System für Industrie-Automatisierungsanlagen besteht. Somit entfallen die bisher erforderlichen aufwändigen Sonderentwicklungen für den Bahnbetrieb.

[0044] In Anspruch 5 ist eine dezentralisierbare Prozessebene beschrieben, die über ein Datennetzwerk mit der Sicherungsebene verbunden ist. Hierbei werden auf der Prozessebene logisch passive Komponenten eingesetzt, die die übertragenen Daten auf digitale Ein-/Ausgabe-Bits verfahrensgesichert umsetzen. Grundsätzlich setzt das dezentrale Prozesselement lediglich Netzwerk-Telegramme des sicheren Stellwerkskerns in digitale Ausgaben um und meldet Änderungen der digitalen Eingänge ereignisgesteuert oder auf Anfrage vom sicheren Stellwerkskern, ebenfalls über das Kommunikations-Netzwerk.

[0045] Sowohl die Kommunikation in der gesamten Verfahrenskette als auch die Funktion der dezentralen, im Allgemeinen nicht sicheren Elemente der Prozessebene müssen gemäß Anspruch 6 ständig überprüft werden. Bei den vom sicheren Stellwerkskern initiierten Aktionen geschieht dies über dialogorientierte Verfahrenssicherung.

[0046] Hierzu müssen von der Sicherungsebene getriggerte und überwachte Mechanismen zyklisch die Kommunikation in der Verfahrenskette sowie die Funktion der Elemente in der Prozessebene überprüfen. Im

Fehlerfall wird von der Sicherungsebene zumindest die Stromversorgung zum zugehörigen Element der Prozessebene sicher abgeschaltet.

[0047] Gegebenenfalls wird zusätzlich die Signalversorgungsspannung derart separiert, dass im Fehlerfall nur die zum Signalbegriff "Halt" gehörenden Elemente mit Spannung versorgt werden.

[0048] In Anspruch 7 ist eine Vorrichtung beschrieben, die das in Anspruch 1 genannte Verfahren umsetzt.

[0049] Die Systemarchitektur orientiert sich am bewährten industriellen Ebenenmodell, bestehend aus einer Bedien- und Beobachtungsebene, einer Sicherungsebene und einer Prozessebene.

[0050] Erfindungsgemäß stellt ein vollgrafisches, auf Marktstandards basierendes System die Bedien- und Beobachtungsebene dar.

[0051] Die Sicherungsebene wird von einem sicheren Rechnersystem gebildet.

[0052] In der Prozessebene befinden sich die anzusteuernden Elemente der Außenanlage sowie andere signaltechnische Einrichtungen, wie Nachbarstellwerke, Blockeinrichtungen, Bahnübergänge, etc.

[0053] Die Komponenten der verschiedenen Ebenen kommunizieren über entsprechende Datenübertragungseinrichtungen.

[0054] Ein sicheres Rechnersystem befindet sich nur in der Sicherungsebene. Es leistet die sicherheitsgerichteten Prüfungen und Algorithmen zur Gewährleistung der Verfahrenssicherheit, wohingegen die Rechner beziehungsweise sonstigen Komponenten der Bedien- und Beobachtungsebene sowie der Prozessebene geringeren Sicherheitsansprüchen genügen.

[0055] Die Vorrichtung basiert sicherheitstechnisch auf einer Variante der bekannten Verfahrenssicherung, wobei erfindungsgemäß die Sicherungsprozeduren zwar jeweils konsequent an den Endpunkten (Quelle und Senke) der Aktionen greifen, die Zwischen- und Ergebnisse jedoch nur im sicheren Stellwerkskern geprüft werden. Somit sind alle Komponenten außerhalb des sicheren Stellwerkskerns, das heißt sowohl für die Kommunikation als auch für die Prozessebene, Komponenten nach Industriestandard, die einem geringeren Sicherheitslevel genügen.

[0056] Die aufwändige sichere Programmierung und Prüfung sowie teure Hardware ist nur an der einen Stelle im sicheren Stellwerkskern erforderlich.

[0057] Durch Anwendung der CENELEC-Normen ist eine quantitative Betrachtung des Fehlverhaltens einzelner Module, Programme und Datenverbindungen möglich, so dass sich unterschiedliche Arten der Verfahrenssicherung hinsichtlich der geforderten SIL berechnen lassen.

[0058] In Anspruch 8 ist beschrieben, wie die Vorrichtung Befehle zur Ansteuerung von Elementen der Prozessebene sicher auslöst. Dabei wird unterschieden, auf welchem Weg Befehle an die Prozessebene erteilt werden.

[0059] Wenn mindestens ein Befehl von der Bedienereingabe auf der Bedien- und Beobachtungsebene eingegeben wird, so überträgt eine Datenübertragungseinrichtung den Befehl an das sichere Rechnersystem in der Sicherungsebene. Das sichere Rechnersystem überprüft den Befehl auf Plausibilität. Plausible Befehle werden neu codiert und an die Bedien- und Beobachtungsebene zurück übertragen. In dem mindestens einen Rechner der Bedien- und Beobachtungsebene wird der neu codierte Befehl des sicheren Rechnersystems ebenfalls auf Plausibilität überprüft und das Ergebnis der Plausibilitätsprüfung in final codierter Form an das sichere Rechnersystem in der Sicherungsebene übertragen.

[0060] Zusätzlich gewährleistet im Allgemeinen bei solchen sicherheitsrelevanten manuellen Bedieneingaben ein separater Kommunikationsweg, dass die Bedienung in dieser Form explizit gewünscht ist. Hierfür muss vom Bediener insbesondere ein gedoppelter oder antivalenter Kontakt geschlossen werden, und/oder werden zusätzlich codierte digitale Adressen eingelesen und geprüft.

[0061] Sind diese Bedingungen erfüllt, so ist mit ausreichender Sicherheit davon auszugehen, dass eine Elementansteuerung von der Bedien- und Beobachtungsebene einerseits tatsächlich gewünscht ist und andererseits der Befehl plausibel ist sowie die Kommunikation mit dem Element in der Prozessebene einwandfrei funktioniert. Dementsprechend löst der sichere Rechner den Befehl zur Ansteuerung des Elements aus.

[0062] Sobald jedoch mindestens eine der zuvor genannten Plausibilitätsüberprüfungen der verwendeten Befehle in mindestens einem der beteiligten Rechner negativ ausfällt, bricht das sichere Rechnersystem die Ansteuerung von Elementen der Prozessebene mit einer entsprechenden Fehlermeldung sicher ab.

[0063] Werden die Befehle zur Ansteuerung von mindestens einem Element der Prozessebene aufgrund des internen Programmablaufs im sicheren Rechnersystem der Sicherungsebene erteilt, so löst das sichere Rechnersystem der Sicherungsebene die Ansteuerung direkt aus.

[0064] In Anspruch 9 ist beschrieben, wie das sichere Rechnersystem das von dem gemäß Anspruch 8 ausgelösten Befehl erzeugte Ansteuerungsereignis signaltechnisch sicher überwacht.

[0065] Nachdem der Befehl zur Ansteuerung eines Elements der Prozessebene vom sicheren Rechnersystem der Sicherungsebene ausgelöst wurde, wird er über eine Datenübertragungseinrichtung an das passende Element in der Prozessebene übertragen. Die Wirkung dieses Befehls führt zu mindestens einem Ansteuerungsereignis, dessen Ergebnis von einer geeigneten Sensorik überwacht und an das sichere Rechnersystem in der Sicherungsebene zurückgemeldet wird. Als Endergebnisse der Ansteuerungsereignisse kommen beispielsweise die Rückmeldung von optischen Sensoren bei der Anschaltung von Lichtsignalen oder die Verwendung von magnetischen Sensoren, wie z.B. industrieller Beros zum Überwachen des mechanisch korrekten Um-

laufs einer Weiche in Frage.

[0066] Die Ergebnisse eines jeden Ansteuerungsereignisses müssen mehrfach hinsichtlich der geforderten logischen und zeitgerechten Abfolge überprüft werden. Da nur ein sicheres Rechnersystem im sicheren Stellwerkskern zur Verfügung steht, müssen alle Prüfungen auch dort erfolgen. Deshalb prüft die Software im sicheren Rechnersystem die Ergebnisse mehrfach, aber zeitversetzt, so dass für jedes Ergebnis Mehrfachdialoge entstehen, die bis hin zum Endergebnis geführt werden.

[0067] Nach positiver Prüfung aller Ergebnisse zu den Ansteuerungsereignissen geht das sichere Rechnersystem von einer erfolgreichen Elementansteuerung aus und offenbart dies. Ergibt die Prüfung von mindestens einem Ergebnis der Ansteuerungsereignisse einen Widerspruch zur geforderten logischen und zeitgerechten Abfolge, so geht das sichere Rechnersystem von einer fehlerhaften Elementansteuerung aus und offenbart auch dies.

[0068] Die mehrfache, zeitversetzte Prüfung der unterschiedlichen Ereignisse an nur einer Stelle im sicheren Stellwerkskern erfordert eine leistungsfähige Rechnerarchitektur. Sie stellt sicher, dass der Zeitaufwand für die je nach gewünschtem Sicherheitslevel erforderlichen Prüfungen und das anschließende Stellen der Elemente der Prozessebene nicht mehr Zeit aufgewendet wird, als die von der Zulassungsbehörde geforderte Maximalzeit, innerhalb der der Signalbegriff "Halt" gezeigt werden muss (Haltfallzeit).

[0069] Die heute zur Verfügung stehenden, erprobten Prozessoren und Kommunikationssysteme machen dies möglich.

[0070] Gemäß Anspruch 10 besteht eine vorteilhafte Ausgestaltung der Erfindung darin, dass das sichere Rechnersystem der Sicherungsebene aus einer fehlersicheren speicherprogrammierbaren Steuerung (SPS) besteht.

[0071] Die auf der SPS realisierte Logik wird nach DIN EN 61131 programmiert und ist somit aufwandsarm auf andere SPS Systeme portierbar.

[0072] In Anspruch 11 ist eine dezentralisierbare Prozessebene beschrieben, die über ein LAN (Local Area Network) mit der Sicherungsebene verbunden ist. Hierbei agieren Standard-ET (elektronische Trennleiste) oder kleine SPS-Systeme verfahrensgesichert als logisch passive Umsetzer für die über Ethernet oder eine andere standardisierte Datennetztechnologie übertragenen Daten, so dass hinter den Umsetzern digitale Ein-/Ausgabebits vorliegen.

[0073] Die Prozessebene macht als Multiplikator für die LST den Hauptkosten- und LCC-Anteil aus.

[0074] ETs sind Standardprodukte der Industrieautomatisierung und werden mit ähnlichem Leistungsspektrum von vielen Firmen angeboten.

[0075] Durch neutrale Netzwerk-Adressierung und vergleichbare Leistungsmerkmale der Hersteller ergibt sich hier eine einfache Substituierbarkeit des gewählten Lieferanten.

[0076] Darüber hinaus sind mittlerweile kompakte kleine SPS-Systeme auf dem Markt. Auch diese können ET-Funktionen ausführen. Deren Einsatz ist ebenfalls möglich, bedingt jedoch eine CENELEC-konforme "Code Inspection".

[0077] Erfindungsgemäß werden durch konsequente Dezentralisierung Standardkomponenten nah am Zielobjekt platziert und über LAN-Verbindungen (Kupferkabel oder LWL) vom sicheren Stellwerkskern gesteuert. Daraus resultieren sehr kurze Kabellängen und geschützte Kabelwege innerhalb der Außenanlage. Somit sind deutlich geringere induzierte Spannungen für Scherheits- und Schutzbetrachtungen auf den Kabeln anzunehmen.

[0078] Sowohl die Kommunikation in der gesamten Verfahrenskette als auch die Funktion der dezentralen, im Allgemeinen nicht sicheren Elemente der Prozessebene müssen gemäß Anspruch 12 ständig überprüft werden.

[0079] Hierzu prüfen von der Sicherungsebene getriggerte und überwachte Watchdogs zyklisch die Kommunikation in der Verfahrenskette sowie die Funktion der Elemente in der Prozessebene. Im Fehlerfall schaltet die Sicherungsebene zumindest die Stromversorgung zum zugehörigen Element der Prozessebene sicher ab. Gegebenenfalls wird zusätzlich die Signalversorgungsspannung derart separiert, dass im Fehlerfall nur die zum Signalbegriff "Halt" gehörenden Elemente mit Spannung versorgt werden.

[0080] Die Erfindung ist nachfolgend anhand einer Zeichnung mit zwei Figuren und eines Beispiels in einer vorteilhaften Ausführungsform näher erläutert.

[0081] Die Zeichnung zeigt in

Fig. 1: die Darstellung der dialogorientierten Sicherungskette zwischen sicherem Stellwerkskern und Prozessebene, inkl. Watchdog,

Fig. 2: die Prinzipschaltung des Prozesselements "Signal" mit Ethernet-Schnittstelle, Elektronischer Trennleiste, Stromversorgung und Überwachung des Lichtstroms mit einem optischen Sensor.

[0082] Die Systemarchitektur eines Elektronischen Stellwerks zum Durchführen des Fahrbetriebs von Schienenfahrzeugen gliedert sich in die drei Ebenen der Bedienung/Beobachtung, der Sicherung und der Prozesselemente

[0083] Ein vollgrafisches, auf Marktstandards basierendes System, findet sich in der Bedien- und Beobachtungsebene (1).

[0084] Die Sicherungsebene (2) wird von einem sicheren Rechnersystem gebildet, das als fehlersichere SPS, wie z.B. einer SIMATIC S7-F ausgebildet ist.

[0085] In der Prozessebene (4) befinden sich die anzusteuernden Elemente der Außenanlage sowie andere signaltechnische Einrichtungen, wie Nachbarstellwerke, Bahnübergänge, etc. Aus Gründen der Übersichtlichkeit

ist nur das Prozesselement "Signal" benannt. Die anderen Prozesselemente der Prozessebene sind durch die gestrichelte Darstellung des Ethernets nur angedeutet.

[0086] Über Kupferkabel werden die Daten beispielsweise in einem Ethernet-LAN (5) zwischen der Sicherungsebene (2) und den dezentral platzierten Elementen (6) der Prozessebene (4) ausgetauscht. Daraus resultieren sehr kurze Kabellängen und geschützte Kabelwege innerhalb der Außenanlage. Somit sind deutlich geringere induzierte Spannungen auf den Kabeln anzunehmen. Kabelfehler können einfach offenbart werden, da nur geringe ohmsche Widerstände bei den kurzen Kabelwegen anzunehmen sind. Erdschlüsse sind durch galvanische Trennung der Speisespannung erst als Doppelfehler relevant und offenbaren sich hardwaremäßig und in der Verfahrenssicherung. Darüber hinaus können einfache Erdschlüsse durch Erdschlussmelder erkannt werden.

[0087] Als Schnittstelle zu den Elementen der Prozessebene werden elektronische Trennleisten (ET, 7) eingesetzt. Als logisch passive Komponenten setzen die ET (7) die über Ethernet (5) übertragenen Daten in digitale Ein-/ Ausgabebits um.

[0088] Soll beispielsweise im Rahmen des automatischen, internen Programmablaufs der Fahrstraßeneinstellung eine Signalglühlampe (20) eingeschaltet werden, so sieht die Verfahrenskette zur sicheren Ansteuerung und Rückmeldung des Lampenfadens folgendermaßen aus:

[0089] Der Stellwerkskern (3) löst im ersten SPS-Zyklus ein Daten-Telegramm aus, welches von der ET (7) des angesprochenen Signal-Prozesselements einen Digitalausgang (DA, 9) rücksetzt. Diese Rücksetzung steuert ein zwangsgeführtes Relais K1 (16) ab. K1 (16) hat einen Öffner im Stromkreis der Signallampe. Damit wird an den Schließerkontakt des elektronischen Relais (ELR, 17) das Potential der Signallampenspannung geleitet.

[0090] Dieses Potential wird nun von einem digitalen Eingang (8) des Prozesselementes detektiert und über die ET (7) per Netzwerk (5) an die sichere SPS (3) übermittelt. Die sichere SPS (3) erwartet eben diese Reaktion (Änderung des Status des entsprechenden DE-Bits von 0 auf 1) für das Auslösen des nächsten Prozess-Schrittes, nämlich der Ansteuerung eines weiteren digitalen Ausganges (9) des Prozesselementes. Dieser DA (9) steuert nun das ELR (17) an. Das ELR schließt den Stromkreis bestehend aus Stromquelle (10), Öffnerkontakt Relais K1 (16), Schließer des ELR (17) und Lampenfaden (20). Da der Relaiskontakt des K1 (16) bereits geschlossen ist, wird dieser geschont, was die Lebensdauer des Relais deutlich erhöht. Eine entsprechende Abfolge beim Löschen des Signalbegriffes dient ebenfalls zur Schonung des Relaiskontaktes. Die Lebensdauer des ELR (17) wird hingegen nicht durch die Anzahl der Schaltvorgänge beeinflusst.

[0091] Durch mindestens einen optischen Sensor (15) an der entsprechenden Signallampe wird nun erkannt, dass die Signalglühlampe korrekt leuchtet. Über einen digitalen Eingang (8) an der ET (7) wird diese Information an den sicheren Stellwerkskern (3) übermittelt. Damit ist die erwartete Reaktion (Änderung des Status des entsprechenden DE-Bits von 0 auf 1) zeitgerecht eingetreten. Der Stellwerkskern (3) kann auf logische Abfolge prüfen und auch das zeitgerechte Resultat der optischen Rückmeldung in einem definierten Zeitfenster auswerten. Nach positiver Prüfung kann die sichere Stellwerkslogik von einem korrekten Vorgang ausgehen und die bestimmungsgemäß arbeitende Signaloptik (20) in der zentralen Fahrstraßenlogik berücksichtigen.

[0092] Es ist anzunehmen, dass die nicht signaltechnisch sicheren Komponenten die unzeitige Anzeige eines Fahrt gebenden Signalbildes lediglich mit einer THR von>10 exp -4 pro Stunde beherrschen.

[0093] Die mögliche Fehlfunktion der Kommunikation, z.B. mit der Konsequenz dass ein anstehendes Grün nicht ausgeschaltet wird, ist zu überwachen. Ebenfalls die mögliche Fehlfunktion der ET.

[0094] Hierfür wird ein Watchdog (11) eingesetzt. Dieser muss in einem definierten Puls-/ Pausenverhältnis von einem digitalen Ausgang (9) der ET (7) angesteuert werden. Bleibt der Impuls in einem definierten Zeitfenster aus, so passiviert der Watchdog (11) die Stromersorgung (10). Der Impuls wird vom sicheren Stellwerkskern generiert.

[0095] Steht der zyklische Impuls beim Watchdog (11) an, so funktioniert die ET (7) und die Kommunikation zum sicheren Stellwerkskern (3).

[0096] Fällt die Kommunikation aus, wird der digitale Ausgang (9) der ET (7) nicht zyklisch zur Ausgabe des Watchdog-Impulses aufgefordert. Der Impuls bleibt aus, und der Watchdog (11) unterbricht die Stromversorgung (10).

[0097] Fällt die ET (7) aus, wird mit sehr hoher Wahrscheinlichkeit der zyklische Impuls und das erforderliche Puls-/ Pausenverhältnis, welches der Watchdog (11) erwartet, ausbleiben oder in einer anderen Pulsfolge anstehen. Der Watchdog (11) erkennt dies und unterbricht die Stromversorgung (10).

[0098] Der Watchdog (11) selbst schaltet über den Schließer eines zwangsgeführten Kleinrelais (12) die Versorgungsspannung der ET (7). Bleibt der Impuls aus, so fällt das zwangsgeführte Relais (12) ab, und die Versorgungsspannung wird unterbrochen. Der sichere Stellwerkskern (3) erkennt dies am Ausbleiben der Ethernet Telegramme.

[0099] Zur Prüfung des zwangsgeführten Relais (12) und der gesamten Watchdog-Funktion wird der Watchdog-Impuls vom sicheren Stellwerkskern (3) kurz ausgesetzt. Über den Öffnerkontakt des zwangsgeführten Relais (12) wird dann die Versorgungsspannung an einem DE der ET erwartet. Sollten die Relaiskontakte verschweißt sein oder ein sonstiger Fehler in der Kommunikationskette des Watchdog-Impulses vorliegen, so offenbart sich dieser im Prüfzyklus. Für die Dauer der Unterbrechung der Versorgungsspannung wird die ET-Versorgungsspannung hinter dem Watchdog Relais über ei-

nen Kondensator (13) gepuffert.

[0100] Durch weitere Kontakte des zwangsgeführten Relais können bedarfsweise die Signalspannungen fahrtgebender Begriffe ab- (18) und die Signalspannung haltgebender Begriffe angeschaltet (19) werden.

[0101] Durch die Prozesskette der sicheren Software des Stellwerkskerns (3) werden weitere Fehler eines jeden Elementes und auch Zweitfehler offenbart:

Defekt der ET (7):

[0102] Jede Aktion an einem Element (6) der Prozessebene (4) wird über die zugehörige ET (7) initiiert. Bei einem Defekt der ET wird das Absteuern des DA (9) für Relais 16 nicht ausgeführt. Also kommt auch keine Rückmeldung des anstehenden Potentials am ELR (17) an. Der sichere Stellwerkskern (3) erkennt den Fehler.

Defekt am DA (9) in der ET (7):

[0103]

1. Durchlegiertes Relais (16):

   Das Relais ist ständig angezogen. Die zugehörige Rückmeldung über DE (8) kommt nicht zustande. Der sichere Stellwerkskern (3) erkennt den Fehler.

2. Hochohmiges Relais (16):

   Das Relais ist bereits im Grundzustand abgefallen. Die zugehörige Rückmeldung des Potentials am ELR (17) ist zur Unzeit da. Der sichere Stellwerkskern (3) erkennt den Fehler.

Defekt am DE (8) in der ET (7):

[0104] Rückmeldungen kommen nicht oder zur Unzeit an. Der sichere Stellwerkskern (3) erkennt den Fehler.

[0105] Eine weitere Zweitfehleroffenbarung ergibt sich durch die nachfolgende, identische Prozedur mit dem ELR (17), und zusätzlich durch das Rücklesen des Lichtes:

Defekt bei der Rückmeldung des Lichts:

[0106] Lichtsensorik DE/ Sensor (15):

1. Durchlegiert:

   Licht wird ständig detektiert. Die zugehörige Rückmeldung über DE (8) steht zur Unzeit an. Der sichere Stellwerkskern (3) erkennt den Fehler.

2. Hochohmig:

   Licht wird nach Ansteuern des ELR (17) nicht detektiert. Der sichere Stellwerkskern (3) erkennt den Fehler.

[0107] Auch bei korrekt arbeitender Rückmeldung des Lichts können Fehler durch Fremdlichteinfall auftreten.

[0108] Ein Fremdlichteinfall wirkt sich nur als Zweitfehler in Verbindung mit dem Erstfehler "defekte Ansteuerung/Ausleuchtung" aus. Eine Auswirkung entsteht nur dann, wenn exakt in dem Zeitfenster, in dem die optische Rückmeldung einer Ansteuerung der Signaloptik (20) ansteht, Fremdlicht einfällt und trotz nicht vorhandener Signalausleuchtung für eine positive Rückmeldung durch den optischen Sensor (15) sorgt.

[0109] Steht bereits vorher Fremdlicht an, erkennt dies der sichere Stellwerkskern (3), da der optische Sensor (15) zur Unzeit eine positive Rückmeldung bringt.

[0110] Der Fall des Fremdlichteinfalls genau im Zeitfenster der Begriffsansteuerung ist durch geeignete Positionierung und Schutz des Sensors (15) vor Fremdlicht ausreichend beherrschbar.

[0111] Zur Fehleroffenbarung von Signaloptiken, die den Zustand über lange Zeit nicht wechseln, sind vom sicheren Stellwerkskern kurze Prüfzyklen durchzuführen, z.B. einmal pro 24h, wenn mehrere Gleisabschnitte vor dem Element frei sind.

Defekt in der Kommunikation:

[0112] Durch Mehrfachtelegramme (14) zur Auslösung einer Aktion ergibt sich eine hohe rechnerische Fehlerbeherrschung. Im sicheren Stellwerkskern (3) wird über eine Plausibilitätsprüfung ein Kommunikationsfehler offenbart. Bei Unplausibilität eines Telegramms passiviert der sichere Stellwerkskern das System.

[0113] Da bei defekter Kommunikation keine zeitgerechte Abarbeitung des Vorgangs erfolgen kann, ist eine zusätzliche Sicherung gegeben.

[0114] Darüber hinaus ist der Watchdog (11) in die Gesamtkette der Kommunikation eingebunden. Dadurch offenbaren sich Fehler in der Kommunikation zeitnah.

[0115] Berücksichtigt man die Mehrfachdialoge, die gegenläufige Ansteuerung von Relais (spannungslos durchgeschaltet) und ELR (angesteuert durchgeschaltet) in Kombination mit der dialogorientierten Prüfung des Verfahrens in der sicheren Stellwerkslogik, so sind Kommunikationsfehler mit einer Wahrscheinlichkeit, die SIL 4 entsprechen, auszuschließen.

Defekt im Lampensockel:

[0116] Ein Sockelschluss (Haupt und Nebenfaden brennen) wird über das Auslösen der Sicherung (22) und durch den DE (8) am ELR (17) detektiert.

Defekt am Hauptfaden:

[0117] Der optische Sensor (15) gibt nach Anschal-

tung keine positive Rückmeldung. Es kann eine Umschaltung auf den Nebenfaden ausgelöst werden. Zusätzlich erfolgt eine Information an den Fahrdienstleiter (Hauptfaden z.B. "Rot N1" defekt).

[0118] Durch zeitversetzte, unabhängige Prozeduren im sicheren Stellwerkskern (3), deren Plausibilitätsprüfungen und das zeitgerechte Prüfen der Lichtemission der adressierten Lichtquelle (20) in der sicheren Software entsteht Verfahrenssicherheit, auch unter Einbeziehung der nicht sicheren Komponenten der Prozessebene (4).

[0119] Bei einer sicherheitsgerichteten manuellen Bedienung des Signals in der Bedien- und Beobachtungsebene (1) anstelle der oben beschriebenen automatischen Ansteuerung ist es im Allgemeinen erforderlich, dass vor der Auslösung des Befehls die manuelle Bedienung explizit bestätigt wird. Hierfür ist in diesem Beispiel ein dezentrales Prozesselement KF (Kommando Freigabe nicht eingezeichnet) über einen separaten Kommunikationsweg in Verbindung mit einem Taster/Schlüsseltaster mit einem gedoppelten Kontakt am Bedienplatz-System installiert. Dadurch wird der KF Bediendialog mit dem sicheren Stellwerkskern abgebildet.

Bezugszeichenliste

[0120]

1	Bedien- und Beobachtungsebene
2	Sicherungsebene
3	Sicheres Rechnersystem (sicherer Stellwerkskern)
4	Prozessebene
5	Ethernet
6	Prozesselement
7	Elektronische Trennleiste
8	Digitaler Eingang
9	Digitaler Ausgang
10	Stromversorgung
11	Watchdog
12	zwangsgeführtes Kleinrelais
13	Pufferkondensator
14	Mehrfachdialoge
15	Optischer Sensor
16	Zwangsgeführtes Relais K1
17	Elektronisches Relais (ELR)
18	Schalter für fahrtzeigende Begriffe
19	Schalter für Haltbegriffe (rot)
20	Signalglühlampe
21	Watchdog-Relais
22	Sicherung

Patentansprüche

1. Verfahren zur signaltechnisch sicheren elektronischen Elementansteuerung zum Durchführen eines Fahrbetriebs von Schienenfahrzeugen, bestehend aus einer signaltechnisch sicheren Bedien- und Beobachtungsebene, einer Sicherungsebene und einer die anzusteuernden Elemente enthaltenden Prozessebene sowie Datenübertragungseinrichtungen zwischen den Komponenten dieser Ebenen, wobei entweder durch Bedienereingabe auf der Bedien- und Beobachtungsebene oder durch internen Programmablauf im sicheren Rechnersystem der Sicherungsebene Befehle zur Ansteuerung von mindestens einem Element der Prozessebene gegeben werden können, **dadurch gekennzeichnet, dass** die sicherheitsgerichteten Prüfungen und Algorithmen zur Gewährleistung der Verfahrenssicherheit vom sicheren Rechnersystem der Sicherungsebene geleistet werden, wohingegen die Rechner bzw. sonstigen Komponenten der Bedien- und Beobachtungsebene sowie der Prozessebene geringeren Sicherheitsansprüchen genügen können.

2. Verfahren zur signaltechnisch sicheren elektronischen Elementansteuerung zum Durchführen eines Fahrbetriebs von Schienenfahrzeugen nach Anspruch 1, **dadurch gekennzeichnet, dass**

- von dem sicheren Rechnersystem der Sicherungsebene die sicherheitsrelevante Ansteuerung von Elementen der Prozessebene ausgelöst wird, wenn

  i. bei Befehlen, die durch die Bedienereingabe auf der Bedien- und Beobachtungsebene eingegeben werden, die Befehle mit einer Datenübertragungseinrichtung an das sichere Rechnersystem in der Sicherungsebene übertragen, dort positiv auf Plausibilität überprüft und in neu codierter Form an die Bedien- und Beobachtungsebene zurück übertragen werden, die Software des mindestens einen Rechners der Bedien- und Beobachtungsebene den neu codierten Befehl des sicheren Rechnersystems ihrerseits positiv auf Plausibilität überprüft und das Ergebnis in final codierter Form erfolgreich an das sichere Rechnersystem in der Sicherungsebene überträgt, und wenn zusätzlich über einen separaten Kommunikationsweg des zugeordneten Prozesselementes für sicherheitsrelevante Bedienungen ein gedoppelter oder anti-valenter Kontakt und/oder zusätzlich codierte digitale Adressen eingelesen und positiv geprüft wurden.
  ii. durch internen Programmablauf im sicheren Rechnersystem der Sicherungsebene ein Befehl zur Ansteuerung von mindestens einem Element der Prozessebene erteilt wird,

- die Ansteuerung von Elementen der Prozes-

sebene mit einer entsprechenden Fehlermeldung sicher abgebrochen wird, sobald mindestens eine der zuvor genannten Plausibilitätsüberprüfungen der verwendeten Befehle in mindestens einem der beteiligten Rechner negativ ausfällt.

3. Verfahren zur signaltechnisch sicheren elektronischen Elementansteuerung zum Durchführen eines Fahrbetriebs von Schienenfahrzeugen nach mindestens einem der vorigen Ansprüche, **dadurch gekennzeichnet, dass**

- der Auslösebefehl zur Ansteuerung von Elementen der Prozessebene über eine Datenübertragungseinrichtung vom sicheren Rechnersystem der Sicherungsebene an das passende Element der Prozessebene übertragen wird und dort zu mindestens einem Ansteuerungsereignis führt, dessen Ergebnis von einer geeigneten Sensorik überwacht und an das sichere Rechnersystem in der Sicherungsebene zurückgemeldet wird,
- die Ergebnisse der Ansteuerungsereignisse über Mehrfachdialoge im sicheren Rechnersystem der Sicherungsebene auf die geforderte logische und zeitgerechte Abfolge hin geprüft werden,
- nach positivem Prüfungsergebnis aller Ergebnisse der Ansteuerungsereignisse im sicheren Rechnersystem von einer erfolgreichen Elementansteuerung ausgegangen wird und dies offenbart wird,
- bei negativem Prüfungsergebnis von mindestens einem Ergebnis der Ansteuerungsereignisse von einer fehlerhaften Elementansteuerung ausgegangen und dies offenbart wird.

4. Verfahren zur signaltechnisch sicheren elektronischen Elementansteuerung zum Durchführen eines Fahrbetriebs von Schienenfahrzeugen nach mindestens einem der vorigen Ansprüche, **dadurch gekennzeichnet, dass** das sichere Rechnersystem der Sicherungsebene aus einem modularen System für Industrie-Automatisierungsanlagen besteht.

5. Verfahren zur signaltechnisch sicheren elektronischen Elementansteuerung zum Durchführen eines Fahrbetriebs von Schienenfahrzeugen nach mindestens einem der vorigen Ansprüche, **dadurch gekennzeichnet, dass** die dezentralisierbare Prozessebene über ein Daten-Netzwerk mit der Sicherungsebene verbunden ist, wobei von logisch passiven Komponenten die übertragenen Daten auf digitale Ein-/ Ausgabebits verfahrensgesichert umgesetzt werden.

6. Verfahren zur signaltechnisch sicheren elektronischen Elementansteuerung zum Durchführen eines Fahrbetriebs von Schienenfahrzeugen nach mindestens einem der vorigen Ansprüche, **dadurch gekennzeichnet, dass** durch von der Sicherungsebene getriggerte und überwachte Mechanismen zyklisch die Kommunikation in der gesamten Verfahrenskette sowie die Funktion der dezentralen, im Allgemeinen nicht sicheren Elemente der Prozessebene geprüft wird, und von der Sicherungsebene mindestens die Stromversorgung zum zugehörigen Element der Prozessebene im Fehlerfall abgeschaltet und gegebenenfalls zusätzlich die Signalversorgungsspannung derart separiert wird, dass im Fehlerfall nur die zum Signalbegriff "Halt" gehörenden Elemente mit Spannung versorgt werden.

7. Vorrichtung zur signaltechnisch sicheren elektronischen Elementansteuerung zum Durchführen eines Fahrbetriebs von Schienenfahrzeugen, bestehend aus einer signaltechnisch sicheren Bedien- und Beobachtungsebene, einer Sicherungsebene und einer die anzusteuernden Elemente enthaltenden Prozessebene sowie Datenübertragungseinrichtungen zwischen den Komponenten dieser Ebenen, wobei entweder durch Bedienereingabe auf der Bedien- und Beobachtungsebene oder durch internen Programmablauf im sicheren Rechnersystem der Sicherungsebene Befehle zur Ansteuerung von mindestens einem Element der Prozessebene gegeben werden können, **dadurch gekennzeichnet, dass** die sicherheitsgerichteten Prüfungen und Algorithmen zur Gewährleistung der Verfahrenssicherheit im sicheren Rechnersystem der Sicherungsebene erfolgen, wohingegen die Rechner bzw. sonstigen Komponenten der Bedien- und Beobachtungsebene sowie der Prozessebene geringeren Sicherheitsansprüchen genügen können.

8. Vorrichtung zur signaltechnisch sicheren elektronischen Elementansteuerung zum Durchführen eines Fahrbetriebs von Schienenfahrzeugen nach Anspruch 7, **dadurch gekennzeichnet, dass**

- das sichere Rechnersystem der Sicherungsebene die sicherheitsrelevante Ansteuerung von Elementen der Prozessebene auslöst, wenn

  i. bei Befehlen, die durch die Bedienereingabe auf der Bedien- und Beobachtungsebene eingegeben werden, die Befehle mit einer Datenübertragungseinrichtung an das sichere Rechnersystem in der Sicherungsebene übertragen, dort positiv auf Plausibilität überprüft und in neu codierter Form an die Bedien- und Beobachtungsebene zurück übertragen werden, die Software des mindestens einen Rechners der

Bedien- und Beobachtungsebene den neu codierten Befehl des sicheren Rechnersystems ihrerseits positiv auf Plausibilität überprüft und das Ergebnis in final codierter Form erfolgreich an das sichere Rechnersystem in der Sicherungsebene überträgt, und wenn zusätzlich über einen separaten Kommunikationsweg des zugeordneten Prozesselementes für sicherheitsrelevante Bedienungen ein gedoppelter oder antivalenter Kontakt und/oder zusätzlich codierte digitale Adressen eingelesen und positiv geprüft wurden.

ii. durch internen Programmablauf im sicheren Rechnersystem der Sicherungsebene ein Befehl zur Ansteuerung von mindestens einem Element der Prozessebene erteilt wird,

- die Ansteuerung von Elementen der Prozessebene mit einer entsprechenden Fehlermeldung sicher abgebrochen wird, sobald mindestens eine der zuvor genannten Plausibilitätsüberprüfungen der verwendeten Befehle in mindestens einem der beteiligten Rechner negativ ausfällt.

9. Vorrichtung zur signaltechnisch sicheren elektronischen Elementansteuerung zum Durchführen eines Fahrbetriebs von Schienenfahrzeugen nach mindestens einem der vorigen Ansprüche, **dadurch gekennzeichnet, dass**

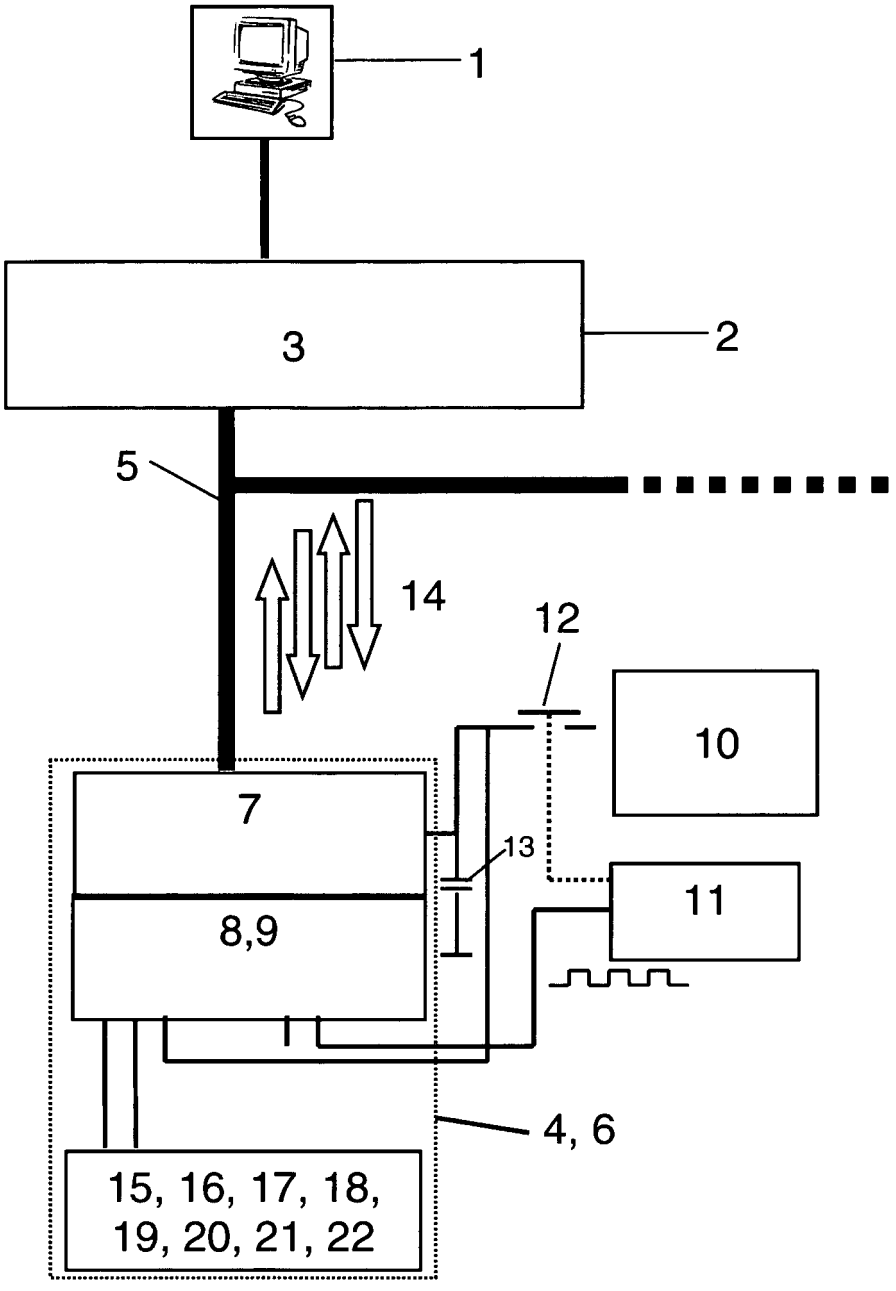
- der Auslösebefehl zur Ansteuerung von Elementen der Prozessebene über eine Datenübertragungseinrichtung vom sicheren Rechnersystem der Sicherungsebene an das passende Element der Prozessebene übertragen wird und dort zu mindestens einem Ansteuerungsereignis führt, dessen Ergebnis eine geeigneten Sensorik überwacht und an das sichere Rechnersystem in der Sicherungsebene zurückgemeldet,
- das sichere Rechnersystem der Sicherungsebene die Ergebnisse der Ansteuerungsereignisse über Mehrfachdialoge auf die geforderte logische und zeitgerechte Abfolge hin prüft,
- das sichere Rechnersystem nach positivem Prüfungsergebnis aller Ergebnisse der Ansteuerungsereignisse von einer erfolgreichen Elementansteuerung ausgeht und dies offenbart,
- das sichere Rechnersystem bei negativem Prüfungsergebnis von mindestens einem Ergebnis der Ansteuerungsereignisse von einer fehlerhaften Elementansteuerung ausgeht und dies offenbart.

10. Vorrichtung zur signaltechnisch sicheren elektronischen Elementansteuerung zum Durchführen eines Fahrbetriebs von Schienenfahrzeugen nach mindestens einem der vorigen Ansprüche, **dadurch gekennzeichnet, dass** das sichere Rechnersystem der Sicherungsebene aus einer fehlersicheren Speicherprogrammierbaren Steuerung (SPS) besteht.

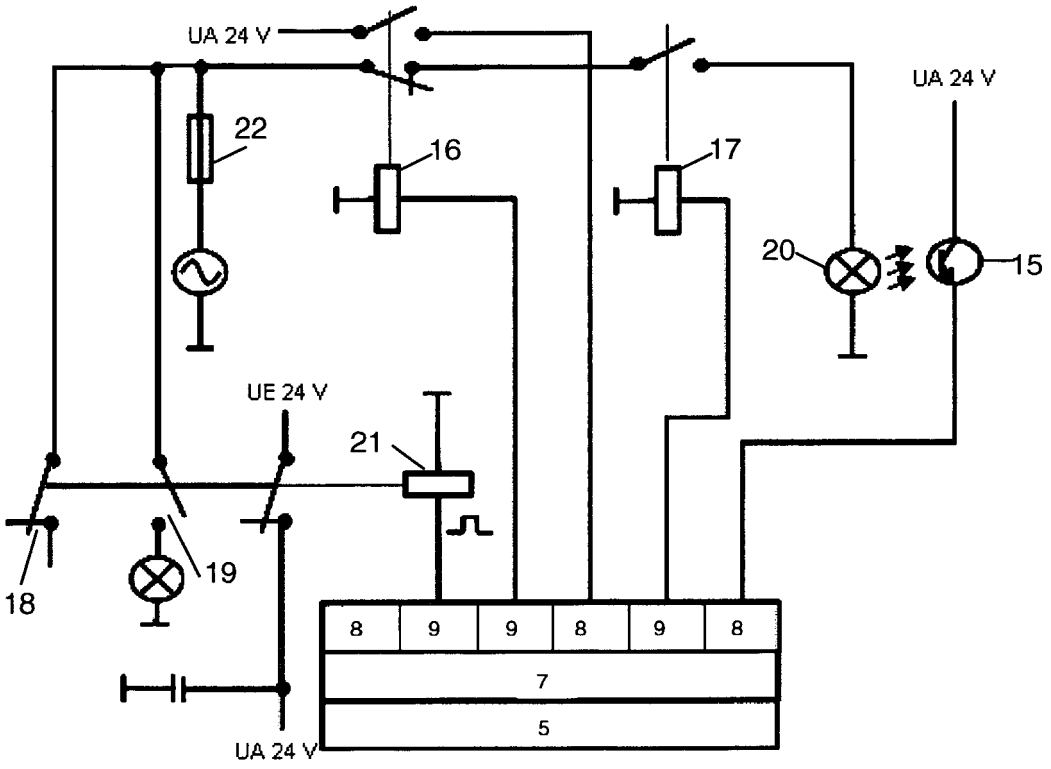
11. Vorrichtung zur signaltechnisch sicheren elektronischen Elementansteuerung zum Durchführen eines Fahrbetriebs von Schienenfahrzeugen nach mindestens einem der vorigen Ansprüche, **dadurch gekennzeichnet, dass** die dezentralisierbare Prozessebene über LAN (Local Area Network) mit der Sicherungsebene verbunden ist, wobei Standard-ET (elektronische Trennleiste) oder kleine SPS-Systeme als logisch passive Umsetzer der über Ethernet oder eine andere Datennetztechnologie übertragenen Daten auf digitale Ein-/ Ausgabebits verfahrensgesichert agieren.

12. Vorrichtung zur signaltechnisch sicheren elektronischen Elementansteuerung zum Durchführen eines Fahrbetriebs von Schienenfahrzeugen nach mindestens einem der vorigen Ansprüche, **dadurch gekennzeichnet, dass** von der Sicherungsebene getriggerte und überwachte Watchdogs zyklisch die Kommunikation in der gesamten Verfahrenskette sowie die Funktion der dezentralen, im Allgemeinen nicht sicheren Elemente der Prozessebene prüfen und die Sicherungsebene mittels zwangsgeführter Kontakte des Watchdog-Relais mindestens die Stromversorgung zum zugehörigen Element der Prozessebene im Fehlerfall abschaltet und gegebenenfalls zusätzlich die Signalversorgungsspannung derart separiert, dass im Fehlerfall nur die zum Signalbegriff "Halt" gehörenden Elemente mit Spannung versorgt werden.

Figur 1



Figur 2



IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- DE 102005043305 A1 **[0013]**
- DE 19606894 C2 **[0014]**
- DE 10053023 C1 **[0015]**