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

(11) **EP 2 088 051 B1**

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
20.04.2011 Patentblatt 2011/16

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

(21) Anmeldenummer: **08002440.9**

(22) Anmeldetag: **11.02.2008**

(54) **Verfahren und Vorrichtung zur sicheren Einstellung von einer Fahrstrasse für ein Schienenfahrzeug**

Method and device for secure setting of a route for a rail vehicle

Procédé et dispositif destinés au réglage sécurisé d'une voie de circulation pour un véhicule sur rail

(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

(43) Veröffentlichungstag der Anmeldung:
12.08.2009 Patentblatt 2009/33

(73) Patentinhaber: **Siemens Schweiz AG**
8047 Zürich (CH)

(72) Erfinder: **Felix, Jon**
8152 Opfikon (CH)

(74) Vertreter: **Fischer, Michael et al**
Siemens AG
Postfach 22 16 34
80506 München (DE)

(56) Entgegenhaltungen:
US-A1- 2002 173 884

- **MASCHEK U: "ELEKTRONISCHE STELLWERKE - EIN INTERNATIONALER UEBERBLICK" SIGNAL + DRAHT, TELZLAFF VERLAG GMBH. DARMSTADT, DE, Bd. 89, Nr. 3, 1. März 1997 (1997-03-01), Seiten 15/16,18-23, XP000779765 ISSN: 0037-4997**
- **WALTHER H ET AL: "EINSATZ VON ELEKTRONISCHEN STELLWERKEN BEI DER DEUTSCHEN BUNDESBAHN" ETR EISENBAHNTECHNISCHE RUNDSCHAU, HESTRA-VERLAG. DARMSTADT, DE, Bd. 34, Nr. 11, 1. Januar 1985 (1985-01-01), Seiten 789-796, XP001246968**

EP 2 088 051 B1

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren und eine Vorrichtung zur sicheren Einstellung einer Fahrstrasse für ein Schienenfahrzeug.

[0002] Eisenbahnnetze sind im besonderen im Bereich von Bahnhöfen und dabei im Besonderen im Bereich von grossen Bahnhöfen aufgrund der Vielzahl von eingesetzten Stellelementen, wie Weichen und Signalen etc., und eingesetzten Überwachungselementen, wie Gleisstromkreise, Achszähler etc., hochkomplexe Systeme, die zur Vermeidung von Personen- und Sachschäden mit einer auf sehr hohem Sicherheitniveau liegenden Stellwerktechnik betrieben werden müssen. Das Stellwerk hat dabei die Aufgabe, die im Leitsystem vorgesehenen Zugläufe (gemäss des Fahrplans) sowie die auch aufgrund von Verspätungen individuell zu steuernden Zugläufe durch die Einstellung von Fahrstrasse zu ermöglichten. Eine Fahrstrasse stellt dabei in der Regel ein Stück eines Fahrweges für das Schienenfahrzeug dar, das an einem Startsignalpunkt beginnt und mit dem Erreichen des in der Regel nächsten Startsignalpunktes endet. Für die Einstellung einer Fahrstrasse werden dann die daran beteiligten Stell- und Überwachungselemente sowie der ggfs. erforderliche Flankenschutz etc. eingestellt und temporär gesichert, wenn für die Stell- und Überwachungselement diese Einstellung zulässig ist. Eine diesbezügliche Diskussion verfügbarer elektronischer Stellwerke ist beispielsweise in dem Artikel von U. Maschek: "Elektronische Stellwerke - ein internationaler überblick", publiziert in der Zeitschrift SIGNAL + DRAHT, Telzlaff Verlag GmbH, Darmstadt, DE, Bd. 89, Nr. 3, 01. März 1997, Seiten 15/16, 18 bis 23, XP000779765 ISSN: 0037-4997, nachlesbar.

[0003] Aufgrund der hohen Sicherheitsanforderungen ist daher die in einem Stellwerk und seinen Aussenanlagen angeordnete Hardware vielfach hochgradig proprietär ausgeführt, um bestimmten besonders sicherheitsrelevante Einstellungen und Überwachungsroutinen für die Einstellung von Fahrstrassen in direkter Verbindung von dem Stellwerkrechner zu den Stell- und Überwachungselementen beispielsweise auf einem SIL4-Level (IEC / DIN EN 61508) ausführen zu können. SIL4 beschreibt dabei bei Systemen mit permanent hohen Sicherheitsanforderungen eine Ausfallwahrscheinlichkeit zwischen 10^{-9} und 10^{-8} pro Stunde.

[0004] Für den ordnungsgemässen Zuglauf müssen die vorstehend genannten Fahrstrasse daher aufgrund der vorhandenen Zugdichten sehr schnell aufgebaut, reserviert und wieder abgebaut werden. Zu jeder Zugstrasse werden die daran beteiligten Stell- und Überwachungselemente sowie deren gewünschte Position bzw. Aussage zugeordnet und mit der Anforderung der Fahrstrasse seitens des Stellwerks abgefragt und ggfs. eingestellt. Ist die Fahrstrasse eingestellt und gesichert, kann auch der zugehörige Signalbegriff "FAHRT" am Startsignal generiert bei herkömmlichen Zugsicherungssystemen angezeigt oder beim ETCS-Level 2 über ein Radio Block Center in den Führerstand des Schienenfahrzeugs übertragen werden.

[0005] Aufgrund der heutigen hierarchischen Segmentierung der Stellwerksaufgaben findet die Überprüfung das an einer angeforderten Fahrstrasse beteiligten Stell- und Überwachungselemente immer aus dem Stellwerk heraus statt, was bedingt, dass die zum Stellwerk gelangenden Informationen einerseits hochzuverlässig und sicher sein müssen und andererseits dann auch hochzuverlässig in das Stellwerk übertragen werden müssen, weil dann im Stellwerk entschieden werden wird, ob eine Fahrstrasse tatsächlich eingestellt werden kann. Diese Randbedingungen führen - wie schon weiter oben angeführt- dazu, dass im Besonderen die eingesetzte Hardware hochproprietär und dadurch in der Anschaffung und im Betrieb unter der Beachtung der geforderten RAMS (Reliability, Availability, Maintainability, Safety) vergleichsweise teuer ist. Besonders die Verwendung von sicheren Rechnerkerne, die in der Regel in einer höheren Programmiersprache kodiert sind, benötigen eine vergleichsweise aufwendige (komplexe) Projektierung im Bereich der Hard- und Software.

[0006] Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren und ein System zur sicheren Einstellung von einer Fahrstrasse anzugeben, die es ermöglichen, bei der Einstellung von sicheren Fahrstrasse unter Umverteilung der hierarchischen Segmentierung dezentraler und weniger proprietär vorgehen zu können.

[0007] Diese Aufgabe wird bezüglich des Verfahrens erfindungsgemäss durch ein Verfahren zur sicheren Einstellung einer Fahrstrasse für ein Schienenfahrzeug gelöst, wobei der Fahrstrasse an der Fahrstrasse beteiligte Stell- und Überwachungselemente sowie deren etwaige, zur Fahrstrasse korrespondierende Zustände zugeordnet sind und wobei jedem Stell- und Überwachungselement ein eindeutiger Hauptschlüssel und etwaige eindeutige zu den möglichen Zuständen korrespondierende Nebenschlüssel zugeordnet sind, mit den folgenden Verfahrensschritten:

a) die von dem Schienenfahrzeug zu befahrende Fahrstrasse wird angefordert;

b) eine Mitteilung an die an der angeforderten Fahrstrasse beteiligten Stell- und Überwachungselemente wird ausgesendet;

c) in Antwort auf die ausgesendete Mitteilung prüfen die Stell- und Überwachungselemente ihre jeweilige Verfügbarkeit für die Einstellung des für die Fahrstrasse vorgesehenen Zustands und stellen diesen Zustand im Falle ihrer jeweiligen Verfügbarkeit ein bzw. verifizieren das Vorliegen des für die Einstellung der Fahrstrasse erforderlichen Zustands;

d) im Falle des Vorliegens der genannten Verfügbarkeit wird ausserdem der Hauptschlüssel und etwaige weitere Nebenschlüssel von jedem der an der Fahrstrasse beteiligten Stell- und Überwachungselemente gesendet; und

d) ein mit der Anforderung der Fahrstrasse verbundener Signalbegriff für die angeforderte Fahrstrasse wird nur im Fall der vollständigen Übersendung der dieser Fahrstrasse zugeordneten Hauptschlüssel und etwaiger weiterer Nebenschlüssel erzeugt.

[0008] Bezüglich des Systems wird die vorstehend genannte Aufgabe erfindungsgemäss durch ein System zur sicheren Einstellung von einer Fahrstrasse für ein Schienenfahrzeug gelöst, wobei der Fahrstrasse an den Fahrstrassen beteiligte Stell- und Überwachungselemente sowie deren etwaige, zur jeweiligen Fahrstrasse korrespondierende Zustände zugeordnet sind und wobei jedem Stell- und Überwachungselement ein eindeutiger Hauptschlüssel und etwaige eindeutige zu den möglichen Zuständen korrespondierende Nebenschlüssel zugeordnet sind, mit:

a) einer Leitstelle, in der die von dem Schienenfahrzeug zu befahrende Fahrstrasse anforderbar ist;
b) einer Kommunikationseinheit, mit der über ein Kommunikationsnetzwerk eine Mitteilung an die an der angeforderten Fahrstrasse beteiligten Stell- und Überwachungselemente aussendbar ist;
c) die Stell- und Überwachungselemente mit Rechenmitteln ausgestattet sind, mit denen in Antwort auf die ausgesendete Mitteilung ihre jeweilige Verfügbarkeit für die Einstellung des für die Fahrstrasse vorgesehenen Zustands prüfbar ist, wobei die Rechenmittel im Falle der jeweiligen Verfügbarkeit den erforderlichen Zustand einstellen bzw. das Vorliegen des für die Einstellung der Fahrstrasse erforderlichen Zustands verifizieren und wobei mittels der Rechenmittel im Falle des Vorliegens der genannten Verfügbarkeit der Hauptschlüssel und etwaige weitere Nebenschlüssel von jedem der an der Fahrstrasse beteiligten Stell- und Überwachungselemente über das Kommunikationsnetzwerk aussendbar sind; und
d) einem Signalbegrifferzeuger, mit dem ein mit der Anforderung der Fahrstrasse verbundener-Signalbegriff für die angeforderte Fahrstrasse nur im Fall der vollständigen Übersendung der dieser Fahrstrasse zugeordneten Hauptschlüssel und etwaiger weiterer Nebenschlüssel erzeugbar ist.

[0009] Auf diese Weise wird zur sicheren Einstellung der Fahrstrasse eine Verlagerung bzw. Verteilung einer notwendigen Sicherungsebene auf die an der Fahrstrasse beteiligten Elemente erreicht. Jedes Stell- und Überwachungselement kann sozusagen selbst prüfen, ob es grundsätzlich für die Einstellung der angeforderten Fahrstrasse verfügbar ist und, wenn ja, ob es auch schon den richtigen Zustand aufweist. Mit Zustand ist hier beispielsweise die Lage einer Weiche oder die Blockierung einer Weiche für den Flankenschutz oder aber auch das Vorliegen des Freimelde-Zustands eines Gleisfreimelders gemeint. Die erforderliche Sicherheitsprüfung bzw. deren Nachweisführung wird so stark vereinfacht und kann generisch, beispielsweise für den Typ "Weiche" oder den "Gleisfreimelder", durchgeführt werden. Die weitere sicherheitsrelevante Prüfung wird hier dann nur noch seitens des Signalbegrifferzeugers erforderlich, der das Vorliegen der für den Fahrtbefehl (z.B. der Signalbegriff "Grüne Lampe AN; rote Lampe AUS) erforderlichen Haupt- und Nebenschlüssel prüft. Die Wahl der Nomenklatur "Hauptschlüssel" und "Nebenschlüssel" soll dabei implizieren, dass der Hauptschlüssel und der Nebenschlüssel eine eindeutige Datenmenge darstellen, die eindeutig einem Stell- oder Überwachungselement und seinem jeweiligen Zustand zugeordnet werden kann. Diese Schlüssel können beispielsweise ein Datenstring sein, der beispielsweise auch nur aus einer ID des Stell- und Überwachungselements und einer logischen "1" für die Verfügbarkeit des Stell- und Überwachungselements bestehen kann. Weitere Nebenschlüssel können dann beispielsweise als weitere logische "Einsen" mit den vorstehend genannten Daten übermittelt werden. Somit können der Hauptschlüssen und einer oder mehrere Nebenschlüsse auch in einem Datensatz zusammengefasst sein. Die Wahl des Bestandteils "Schlüssel" möchte hier weiter implizieren, dass der jeweilige Hauptschlüssel und der oder die etwaigen Nebenschlüssel eine eindeutige Datenmenge zur Kennzeichnung des jeweiligen Stell- und Überwachungselements sowie seines jeweiligen Zustands sind. Weiter kann in dem Begriff des Schlüssels auch ein gewisses Authentizitätsattribut gesehen werden, das es beispielsweise dem Signalbegrifferzeuger erlaubt, den Schlüssel als solchen und zu einem bestimmten Element zugehörig zu erkennen, was ebenfalls einen erheblichen Sicherheitszugewinn darstellt, der aber ebenfalls rein im Kontext der Signalbegrifferzeugung erzielt werden kann. Weiter erlauben es das vorstehende Verfahren und das vorstehende System Erweiterung und Modifizierungen an einer bestehende Fahrstrasse oder bei der Einrichtung einer neuen Fahrstrasse vergleichsweise einfach durchführen zu können, weil nur die neuen oder geänderten Stell- und Überwachungselemente mit neuen Schlüsseln ausgestattet und der Algorithmus auf dem Signalbegrifferzeuger an die neue Situation angepasst werden muss. Das im Signalbegrifferzeuger aber grundsätzlich implementierte Verfahren zur Erzeugung des Signalbegriffs bleibt als solches aber ebenfalls unverändert, weshalb auch die Validierung eines grösseren Netzbereichs erheblich vereinfacht ist.

[0010] In Summe ist daher auch festzuhalten, dass auch die eingesetzte Hardware überwiegend vom Typ SIL0 sein kann, da die signaltechnische Sicherheit einerseits auf den Stell- und Überwachungselementen selbst und andererseits in der Projektierung der Hauptschlüssel und der Nebenschlüssel sowie der Überprüfung auf das vollständige Vorliegen der Schlüssel im Signalbegrifferzeuger reduziert werden kann.

[0011] Eine vorteilhafte Ausgestaltung der Erfindung kann es vorsehen, dass für jede Fahrstrasse ein Signal-

begrifferzeuger definierbar ist, wobei den an der Fahrstrasse beteiligten Stell- und Überwachungselementen im Rahmen der Mitteilung mitteilbar ist, an welchen Signalbegrifferzeuger die jeweiligen Hauptschlüssel und ggfs. die jeweiligen Nebenschlüssel zu senden sind. Somit ist es möglich, den Vorgang der Signalbegrifferzeugung mit einer dem entsprechenden Startsignalpunkt zugeordneten Logikeinheit dort durchzuführen, wo die Fahrstrasse ihren Anfang nimmt. Auf diese Weise bleibt beispielsweise auch die gesamte Stellwerklogik unverändert, wenn beispielsweise innerhalb der Fahrstrasse neue Elemente eingebaut, geändert oder entfernt werden. Einzigallein in dem Algorithmus zur Fahrbegriffbildung muss dieser Vorgang abgebildet werden. Mit anderen Worten heisst dies, dass der Signalbegrifferzeuger vorteilhafterweise mit dem Stellelement assoziiert ist, das den jeweiligen Signalbegriff optisch an einem Signal ausgibt oder im Falle von ETCS Level 2 und höher der Signalbegrifferzeuger vorteilhafterweise mit dem Stellelement assoziiert ist, das den jeweiligen Signalbegriff zur drahtlosen Übersendung an einen Bordcomputer des Schienenfahrzeugs an eine übergeordnete Instanz übergibt.

[0012] Zur weiteren Erhöhung der Sicherheit können die Hauptschlüssel und die ggfs. vorhandenen Nebenschlüssel nach einem sicheren Codierverfahren (CRC, MD4) erzeugt und gesichert sind und so von dem Signalbegrifferzeuger auf Authenzität geprüft werden. Dann kann nicht nur eineindeutig geprüft werden, ob alle erforderlichen Schlüssel gesendet wurden, sondern es kann ebenfalls eineindeutig geprüft werden, ob diese gesendeten Schlüssel auch wirklich genau die Schlüssel sind, deren Übermittlung erwartet worden ist.

[0013] In einer weiteren bevorzugten Ausführungsform der Erfindung kann der Signalbegrifferzeuger den Stell- und Überwachungselementen den Erhalt eines authentizierbaren Hauptschlüssels und ggfs. weiterer authentizierbarer Nebenschlüssel quittieren. Die Stell- und Überwachungselemente erhalten so eine Rückkopplung, dass ihre Schlüssel auch tatsächlich am richtigen Signalbegrifferzeuger angekommen sind und von diesem authentifiziert werden konnten. Der Empfang dieser Quittung kann weiter beispielsweise dafür genutzt werden, das entsprechende Element für die weitere Versendung von Schlüsseln zu blockieren. Andersherum gesagt, können die Stell- und Überwachungselemente entweder bereits mit dem Senden ihres zugehörigen Hauptschlüssels oder dann nach dem Erhalt der Quittierung der Sendung zur erneuten Sendung ihres Hauptschlüssels blockiert sein. Somit ist es während dieser Zeit keinem anderen Signalbegrifferzeuger möglich, einen Hauptschlüssel dieser so blockierten Stell- und Überwachungselemente zu erhalten. Auf diese Weise kann die Reservierung einer Fahrstrasse einfach und ebenfalls wieder sicherheitstechnisch ausgelagert an die Stell- und Überwachungselemente gelöst werden.

[0014] Gelegentlich kann es vorkommen, dass entweder die Funktionalität eines Stell- oder Überwachungselements gestört ist oder eine Kommunikationsstörung zu einem Stell- oder Überwachungselement vorliegt, sodass die angeforderte Fahrstrasse nicht eingestellt werden kann, weil der Hauptschlüssel dieses Elements nicht an den entsprechenden Signalbegrifferzeuger gesendet wird. Ein derartiger Fehler kann beispielsweise auch durch einen Achszähler verursacht werden, bei dem aufgrund von ungünstigen EMV-Interferenzen eine unterschiedliche Anzahl von Waggonachsen in einem Abschnitt ein- und ausgezählt worden sind, obwohl alle Waggons des Zuges den Abschnitt nach dessen Befahrung verlassen haben. In einer vorteilhaften Ausgestaltung der Erfindung ist daher eine Überwachungsinstanz vorgesehen, die einen zur Erzeugung des mit der Anforderung der Fahrstrasse gewünschten Signalbegriffs fehlenden Hauptschlüssel sowie der etwaigen Nebenschlüssel durch einen explizit übermittelten Interventionsschlüssel ersetzen kann. Auf diese Weise kann in einem Störungsfall gezielt unter Beachtung der signaltechnischen Sicherheit eingegriffen werden, um dann unter definierten (auch definierbaren) Bedingungen eine Notzugfahrstrasse einzustellen bzw. weitere Umgehungen der gestörten Fahrstrasse (ggfs. auch das Ausweichen auf eine andere Fahrstrasse) anzustossen.

[0015] Eine weitere vorteilhafte Ausgestaltung der Erfindung kann es vorsehen, dass die Stell- und Überwachungselemente, die ihre jeweiligen Hauptschlüssel und ggfs. weitere Nebenschlüssen an den Signalbegriffgenerierer gesendet haben, dem Signalbegriffgenerierer zyklisch eine Zusicherung des gesendeten Hauptschlüssels und ggfs. weiterer Nebenschlüssel übermitteln. Auf diese Weise kann der Signalbegrifferzeuger immer sicher sein, dass alle erforderlichen Schlüssel immer noch von den Stell- und Überwachungselementen bei ihm reserviert sind. Zugleich könnte diese zyklische Bestätigung auch als Anfrage genutzt werden werden, ob die an ihn übersendeten Hauptschlüssel und ggfs. auch übersendeten Nebenschlüssel tatsächlich noch gebraucht werden oder beispielsweise aufgrund einer temporären Leitungsstörung die Schlüssel eigentlich schon wieder zurückgegeben worden, aber eben noch nicht angekommen sind. Signalbegrifferzeuger und Stell- und Überwachungselemente triggern sich so gegenseitig, um eine möglichst prozessnahe Schlüsselpositionierung zu erzielen. Sobald das in der Fahrstrasse erstgelegene Überwachungselemente den Zustand "BELEGT" anzeigt, kann dieser Hauptschlüssel wieder vom Signalbegriffgenerierer an das Überwachungselement zurückgegeben werden. Sobald der Signalbegrifferzeuger einen Hauptschlüssel wieder zurückgegeben hat, ist dieser auch nicht mehr in der Lage den gewünschten Signalbegriff zu generieren. Ein Lichtsignal würde in diesem Fall sofort von "FAHRT" auf "HALT" umstellen.

[0016] Das Verfahren kann weiter so ausgestaltet sein, dass das Ausbleiben der Bestätigung der Zusicherung der gesendeten Haupt- und Nebenschlüssel zu einer Reaktion des Signalbegrifferzeugers führt. Eine mögliche Reaktion ist die sofortige Rücknahme des Fahrbe-

griffs. Gleiches kann gelten, wenn die Bestätigung auf dem Kommunikationsweg verloren geht. Es kann vorgesehen sein, dass die übergeordnete Instanz - ggfs. unter Beachtung einer gewissen Zeitsperre - den Signalbegrifferzeuger veranlasst, alle erhaltenen Haupt- und Nebenschlüssel zurück zu geben.

[0017] Grundsätzlich ist daher zweckmässig, wenn der Signalbegrifferzeuger die für die Einstellung einer Fahrstrasse gesendeten Hauptschlüssel und ggfs. weiteren Nebenschlüssel nach einer komplettierten Befahrung der eingestellten Fahrstrasse an die jeweiligen Stell- und Überwachungselemente zurückgibt oder wenn der Signalbegrifferzeuger die für die Einstellung einer Fahrstrasse gesendeten Hauptschlüssel und ggfs. weiteren Nebenschlüssel nach Fortschritt der Fahrt des Schienenfahrzeugs auf der eingestellten Fahrstrasse abschnittweise an die jeweiligen Stell- und Überwachungselemente zurückgibt.

[0018] Wie schon mehrfach weiter vorangehend angedeutet kann der Signalbegriffgenerierer in einer weiteren bevorzugten Ausführungsform einen für die angeforderte Fahrstrasse spezifizierten Algorithmus ausführen, der das Vorhandensein der für die Erteilung einer Fahrerlaubnis über die angeforderte Fahrstrasse erforderlichen Hauptschlüssel sowie etwaiger Nebenschlüssel überprüft.

[0019] Weitere vorteilhafte Ausgestaltungen der Erfindung sind den übrigen Unteransprüchen zu entnehmen.

[0020] Die Erfindung wird nachfolgend anhand der Zeichnung beispielsweise näher erläutert. Dabei zeigen:

Figur 1 eine einfaches Eisenbahnsystem in einer Ausgangskonfiguration, bei der keine Fahrstrasse eingestellt ist; und

Figur 2 das Eisenbahnsystem nach Figur 1 nach der Einstellung einer Fahrstrasse.

[0021] Figur 1 zeigt ein einfaches Eisenbahnsystem 2 in einer Ausgangskonfiguration, bei der keine Fahrstrasse FS eingestellt ist. Das System 2 weist eine Leitstelle 4, eine Servereinheit 6 und entlang einer einfachen Gleistopologie angeordnete Stell- und Überwachungselemente 8 bis 24 auf. Weiter umfasst das System 2 zwei Signale 26, 28, denen jeweils eine Signaleinheit 30 bzw. 32 zugeordnet ist. Wie unten links in der Legende zur Figur 1 dargestellt, weist jedes der Stell- und Überwachungselemente 8 bis 24 Mittel M zum Erfassen des Zustandes auf einem Sicherheitslevel SIL4 auf, was im unteren Drittel des Symbols S dargestellt. Im oberen Teil des Symbols S befindet sich eine zugehörige, innerhalb des Eisenbahnsystems 2 eineindeutige Adresse AD. Im mittleren Bereich auf der rechten Seite sind zur Verfügung stehende Schlüssel KA gezeigt; entsprechend befinden sich auf der linken Seite die momentan nicht verfügbaren (verschlossenen) Schlüssel KL. Auf die Schlüssel wird dann nachstehend noch im Detail eingegangen werden. Hier an dieser Stelle ist hervorzuheben, dass einzigallein die Mittel M zum Erfassen des Zustands des Stell- und Überwachungselements 8 bis 24 und zur Freigabe der Schlüssel auf SIL4 befindlicher Sicherheitsstufe arbeiten müssen. Für die Genehmigung derartig aufgebauter Eisenbahnsysteme 2 sind daher an dieser Stelle nur die Mittel M generisch zu überprüfen und zuzulassen.

[0022] In der gezeigten Topologie sind die Stell- und Überwachungselemente 8 bis 24 generisch in zwei Funktionalitäten unterteilbar. Mit 14 und 22 sind zwei tatsächliche Stellelemente gezeigt, die nur die Stellung einer Weiche überwachen, sondern diese auch verstellen können. Alle übrigen Elemente 8, 10, 12, 16, 18, 20 und 24 sind zur Feststellung der Gleisbelegung vorgesehen und können beispielsweise Achszählsysteme, Gleisstromkreise oder ähnliches sein. Diese Elemente haben in der Regel nur einen im Kontext dieser Anmeldung Hauptschlüssel genannten Schlüssel mit den elementseitigen Bezeichnungen A, B, D, Q, N, X und Y, der für ihre Verfügbarkeit steht. Eine Verfügbarkeit derartiger Elemente ergibt sich dann nur, wenn der von ihnen überwachte Gleisabschnitt nicht belegt, also frei, ist. Die Stellelemente 14 und 22 unterscheiden sich hiervor in dem Sinne, dass sie zwar auch über je einen Hauptschlüssel C und E, erweitert jedoch auch über weitere Nebenschlüssel C_{li}, C_{re}, E_{li} und E_{re} verfügen, die jeweils einem bestimmten Zustand des Stellelements repräsentieren, also bei den Weichen zum Beispiel die Stellzustände "Abgelenkt" oder "Nicht abgelenkt" oder auch "Lage links" oder "Lage rechts". Die Haupt- und die ggfs. weiter vorhandenen Nebenschlüssel sind eineindeutig und im vorliegenden Ausführungsbeispiel im Anhang mittels CRC32 gesichert. Eine mögliche alternative Sicherung könnte beispielsweise auch MD4 sein. Eineindeutig bedeutet im hier vorhandenen Kontext, dass jeder Schlüssel (Hauptwie Nebenschlüssel) im gesamten zu sichernden Bereich nur exakt einmal vorkommt.

[0023] Figur 2 zeigt nun den Zustand nach der Einstellung der Fahrstrasse FS, die vom Signal 26 bis zum Signal 28 reicht. Hierzu wurde in der Leitstelle 4 ein entsprechender Befehl zur Einstellung der Fahrstrasse FS an die Servereinheit 6 übermittelt. Ein erster Client-Server-Prozess R-1 nimmt diesen Einstellbefehl entgegen. Dieser erste Client-Server-Prozess R-1 besitzt zudem immer ein aktelles Abbild vom Zustand der Stell- und Überwachungselemente 8 bis 24 sowie der Signaleinheiten 30 und 32. Bevor nun versucht wird die Fahrstrasse einzustellen, verifiziert der erste Client-Server-Prozess R-1 das Vorhandensein und die Freigabe aller notwendigen Haupt- und Nebenschlüssel.

[0024] Der erste Client-Server-Prozess R-1 kommuniziert hierbei direkt mit den beteiligten Stell- und Überwachungselementen 8 bis 24 und stellt so bereits einleitende Abklärungen hinsichtlich der Einstellbarkeit der Fahrstrasse FS an. Er prüft weiter, ob die Signaleinheit 30 des Startsignals 26 im vorliegenden Fall leer ist, also keine Schlüssel beinhaltet. Der erste Client-Server-Prozess R-1 benötigt an dieser Stelle keinerlei Kenntnisse

zur Art und Beschaffenheit der Haupt- und ggfs. vorhandener Nebenschlüssel. Mit einem erfolgreichen Abschluss dieser Klärungen übergibt der erste Client-Server-Prozess R-1 die weitere Einstellroutine an einen zweiten Client-Server-Prozess R-2. Dieser zweite Client-Server-Prozess R-2 veranlasst nun die beteiligten Stell- und Überwachungselemente, hier 10, 12, 14, 16, 18 und 22, dazu, die für diese Fahrstrasse benötigten Haupt- und Nebenschlüssel, hier A, B, C, C_{li} (Nebenschlüssel), D und E, E_{li} (Nebenschlüssel) an die Signaleinheit 30 zu senden. Dabei sind diese Schlüssel nicht nur die direkt dem Fahrweg zugeordneten Elemente, sondern auch solche im Falle des Elements 22, die den Flankenschutz für die einzustellende Fahrstrasse FS bereitstellen. Auch dieser zweite Client-Server-Prozess R-2 muss keinerlei Kenntnisse von der Art und Beschaffenheit der Haupt- und Nebenschlüssel haben. Die beteiligten Stell- und Überwachungselemente 10 bis 18 und 22 senden in Antwort auf die Aufforderung ihre diesbezüglichen Haupt- und Nebenschlüssel an die Signaleinheit 30. Die Signaleinheit 30 verifiziert (authentiziert), ob es sich bei den erhaltenen Schlüsseln um gültige Schlüssel handelt. Damit dies hier mit der geforderten Sicherheit nach SIL4 gefolgert werden kann, werden hochsichere Prüfverfahren nach CRC oder MD4 angewendet. Kommt der zweite Client-Server-Prozess R-2 zu dem verifizierten Ergebnis, dass alle beteiligten Stell- und Überwachungselemente 10 bis 18 und 22 ihre Hauptschlüssel, hier A, B, C, D, E und X, sowie die zugehörigen Nebenschlüssel, hier C_{li} und E_{li}, abgegeben haben, wird die weitere Verarbeitung an einen dritten Client-Server-Prozess R-3 übergeben.

[0025] Dieser dritte Client-Server-Prozess R-3 liefert der betroffenen Signaleinheit 30 einen letzten Freigabeschlüssel R-3io zur Freigabe der entsprechenden Fahrstrasse FS. Bildlich ist dies in Figur 2 anhand der in der Signaleinheit 30 eingetragenen Haupt- und Nebelschlüssel sowie anhand den im rechten mittleren Bereich der Stell- und Überwachungselemente eingetragenen Buchstaben Re (=reserviert) dargestellt. Ausserdem zeigt das Signal 26 nun grünes Licht, sodass ein Zugführer in die Fahrstrasse einfahren kann.

[0026] In der Signaleinheit 30 läuft für die Darstellung des Signalbegriffs "Grünes Licht = FAHRT" noch einmal ein mit SIL4 ausgeführter Prozess zur Bildung dieses Signalbegriffs ab. Mit Hilfe der Haupt- und Nebenschlüssel ermittelt der in der Signaleinheit 30 ausgeführte Algorithmus den gültigen Signalbegriff. Während dieser Phase bis zur Auflösung der Fahrstrasse sichern bzw. überwachen hier an dieser Stelle so genannte Überlebenstelegramme die Sicherung der Fahrstrasse in vorteilhafter Weise. Die Überlebenstelegramme werden dabei zwischen den an der Fahrstrasse beteiligten Stell- und Überwachungselementen 10 bis 18 und 22 und der Signaleinheit 30 ausgetauscht. Die Stell- und Überwachungselemente 10 bis 18 und 22 bestätigen der Signaleinheit 30 im Grunde genommen auf diese Weise die Vergabe ihrer Hauptschlüssel. Gleichzeitig kann mann diese Bestätigung aber auch dahingendend interpretieren, dass die Stell- und Überwachungselemente auf diese Weise quasi auch zyklisch bei der Signaleinheit 30 die Rückgabe ihrer Hauptschlüssel sowie der ggfs. involvierten Nebenschlüssel anfragen. Der Prozess kann dabei so ausgestaltet sein, dass die Stell- und Überwachungselemente entweder erstmalig nach ihrer Belegung (also der tatsächlichen Zugüberfahrt) bei der Signaleinheit 30 die Rückgabe des entsprechenden nicht mehr benötigten Schlüssel anfragen. Hierbei kann die Signaleinheit 30 bereits der erstmaligen Anfrage die nun nicht mehr benötigten Hauptschlüssel und allfällige Nebenschlüssel an die anfragenden Stell- und Überwachungselemente zurückgeben. Mit der Rückgabe des ersten der zuvor noch benötigten Schlüssel ist aber die Signaleinheit 30 nicht mehr in der Lage den Signalbegriff "FAHRT" aufrechtzuerhalten. Das Signal 26 zeigt entsprechend rotes Licht; Fahrbegriff "HALT".

[0027] Bei einer Verwendung von Transparent-Datenbalisen als Stellelemente kann dabei die Syntax der Hauptschlüssel und allfälliger Nebenschlüssel so konzipiert sein, dass mit einer einfachen Verarbeitung (beispielsweise einer Addition aller notwendigen Schlüssel) in der Signaleinheit 30 ein gültiges Balisentelegramm sozusagen als Fahrbegriff generiert wird. Zusätzlich bzw. auch alterniv kann das aus den Schlüsseln abgeleitete Balisentelegramm zur Ansteuerung der optischen Signale verwendet werden.

[0028] In einer weiteren alternativen Ausgestaltung der Erfindung können die Haupt- und Nebenschlüssel auch direkt auf dem Bordrechner des Schienenfahrzeugs ausgewertet werden. Die Haupt- und Nebenschlüssel werden in diesem Fall drahtlos (beispielsweise mit einer Transparentdaten-Balise) auf das Fahrzeug übertragen. Da die Übermittlung von Zugbeeinflussungsdaten mittels Transparentdaten-Balisen, beispielsweise im Rahmen von ETCS Level 1, sowieso ein besonders hohes Sicherheitsniveau erreichen muss (auch hier ist SIL4 gefordert), wäre für diese Lösung nicht einmal ein zusätzlicher Aufwand hinsichtlich der Sicherheitsprüfung erforderlich. Enthalten die Hauptschlüssel und die Nebenschlüssel auch noch weitere Informationen bezüglich der Topologie der Fahrstrasse, kann mit dem Bordrechner nicht nur die Fahrerlaubnis, sondern auch das Geschwindigkeitsprofil für die vor dem Schienenfahrzeug liegende Fahrstrasse generiert werden.

[0029] Im Falle einer Störung, also wenn beispielsweise einzelne Elemente der Fahrstrasse gestört sind oder wenn korrekt abgesendete Haupt- und Nebenschlüssel nicht ankommen, erfolgt eine Meldung an eine übergeordnete Instanz, beispielsweise die Leitstelle 2. Diese Störung hat somit zur Folge, dass auf der Sicherungsebene der Fahrstrasse die erforderlichen Schlüssel nicht ordnungsgemäss abgegeben werden können, weshalb der Fahrbegriff in der Signaleinheit 30 nicht generiert werden kann. Um nun hier doch eine Fahrerlaubnis erteilen zu können, ist hier ein gezielter Eingriff der übergeordneten Instanz insofern ermöglicht, dass die übergeordnete Instanz einen Interventionsschlüssel, nachfol-

gend vereinfacht Notschlüssel genannt, generieren und an die betroffene Signaleinheit übermitteln kann. In Kombination mit den auf der Signaleinheit vorhandenen (regulären) Haupt- und Nebenschlüssel kann dann zusammen mit dem Notschlüssel der ursprünglich vorgesehene Fahrbegriff oder aber auch nur ein Hilfssignalbegriff oder andere tieferwertigere Signalbegriffe generiert werden. Mit Hilfe dieser Notschlüssel können beispielsweise auch temporär vorgesehene Umfahrungen realisiert werden, wie dies beispielsweise bei Bau- oder Wartungsarbeiten der Fall sein kann.

[0030] Wie schon vorstehend erläutert können diese Grundprinzipien mit einer derartigen Verteilung der Haupt- und Nebenschlüssel auf die Stell- und Überwachungselemente auch für das moderne europäische Zugsicherungssystem ETCS übernommen. Bei einer Anwendung nach Level 2, bei der die Fahrbegriffe nicht mehr mittels Lichtsignalen angezeigt werden, wird anstelle der Generierung der optischen Fahrbegriffe von der Signaleinheit entsprechende Fahrberechtigungsschlüssel generiert, welche eine temporäre Gültigkeit besitzen. Die Fahrberechtigungsschlüssel werden zyklisch erneuert und dem RBC-Interface-Rechner zur weiteren Verarbeitung und Übermittlung auf den Fahrzeugführerstand übergeben. Grundsätzlich bleibt aber auch hier die gesamte vorstehend beschriebene Philosophie der dezentral verteilten Sicherheitprüfung komplett erhalten.

[0031] Aufgrund der dezentral in den Signaleinheiten vorhandenen Fahrstrasseninformationen können mit diesen vorstehend beschriebenen Verfahren auch neue Konzepte zur Automatisierung realisiert werden, indem beispielsweise auf dezentraler Ebene eine starre Zuglenkung mittels Kommunikation zwischen den Signaleinheiten realisiert werden kann. Das würde bedeuten, dass die Signaleinheit, deren Fahrstrassen gerade aktuell befahren wird, ggfs. unter Berücksichtigung der voraussichtlichen Fahrdauer die Stell- und Überwachungselemente der nachfolgenden Fahrstrasse anweist, die für die Einstellung der nachfolgenden Fahrstrasse erforderlichen Haupt- und Nebenschlüssel an die der nachfolgenden Fahrstrasse zugeordneten Signaleinheit zu senden. Aus diese Weise kann sich quasi ein selbst fortschreibendes System von eingestellten Fahrstrassen ergeben, ohne dass die übergeordnete Instanz im Regelbetrieb eingreifen muss. Die übergeordnete Instanz kann sich so ganz auf die Aspekte der Konfliktlösung beschränken. Eine derartige Lösung setzt es natürlich weiter voraus, dass die Signaleinheit, deren Fahrstrasse aktuell befahren wird, die nachfolgend einzustellende Fahrstrasse kennt. Auch dieser Vorgang ist vergleichsweise einfach automotisierbar, indem beispielsweise anhand der Zugnummer des in eingestellte Fahrstrasse einlaufenden Zuges durch Zugriff auf eine dezentrale oder auch zentrale Datenbank die nachfolgende Fahrstrasse ermittelt wird. Weiter wäre es auch möglich, in der Signaleinheit die fahrplanmässige Abfolge der die Fahrstrasse befahrenden Züge mit einem Hinweis auf die nachfolgende Fahrstrasse zu speichern. Natürlich wäre es auch möglich, der übergeordneten Instanz einen Vorschlag für die nachfolgend einzustellende Fahrstrasse zu machen und diesen Vorschlag dort quittieren zu lassen, bevor die entsprechenden Stell- und Überwachungselemente zur Übersendung ihrer Haupt- und Nebenschlüssel aufgefordert werden.

Patentansprüche

1. Verfahren zur sicheren Einstellung einer Fahrstrasse (FS) für ein Schienenfahrzeug, wobei der Fahrstrasse (FS) an der Fahrstrasse (FS) beteiligte Stell- und Überwachungselemente (8 bis 24) sowie deren etwaige, zur Fahrstrasse (FS) korrespondierende Zustände zugeordnet sind,
   dadurch gekennzeichnet, dass
   jedem Stell- und Überwachungselement (8 bis 24) ein eindeutiger Hauptschlüssel (A bis E, N, X, Y) und etwaige eindeutige zu den möglichen Zuständen korrespondierende Nebenschlüssel (C_{li}, C_{re}, E_{li}, E_{re}) zugeordnet sind, mit den folgenden Verfahrensschritten:

   a) die von dem Schienenfahrzeug zu befahrende Fahrstrasse (FS) wird angefordert;
   b) eine Mitteilung an die an der angeforderten Fahrstrasse (FS) beteiligten Stell- und Überwachungselemente (10 bis 18, 22) wird ausgesendet;
   c) in Antwort auf die ausgesendete Mitteilung prüfen die Stell- und Überwachungselemente (10 bis 18, 22) ihre jeweilige Verfügbarkeit für die Einstellung des für die Fahrstrasse (FS) vorgesehenen Zustands und stellen diesen Zustand im Falle ihrer jeweiligen Verfügbarkeit ein bzw. verifizieren das Vorliegen des für die Einstellung der Fahrstrasse (FS) erforderlichen Zustands;
   d) im Falle des Vorliegens der genannten Verfügbarkeit wird ausserdem der Hauptschlüssel (A bis E, N, X, Y) und etwaige weitere Nebenschlüssel (C_{li}, C_{re}, E_{li}, E_{re}) von jedem der an der Fahrstrasse (FS) beteiligten Stell- und Überwachungselemente (10 bis 18, 22) gesendet; und
   e) ein mit der Anforderung der Fahrstrasse (FS) verbundener Signalbegriff für die angeforderte Fahrstrasse (FS) wird nur im Fall der vollständigen Übersendung der dieser Fahrstrasse (FS) zugeordneten Hauptschlüssel (A bis E, N, X, Y) und etwaiger weiterer Nebenschlüssel (C_{li}, C_{re}, E_{li}, E_{re}) erzeugt.

2. Verfahren nach Anspruch 1,
   dadurch gekennzeichnet, dass für jede Fahrstrasse (FS) ein Signalbegrifferzeuger (30, 32) definiert wird, wobei den an der Fahrstrasse (FS) beteiligten Stell- und Überwachungselementen (10 bis 18, 22)

im Rahmen der Mitteilung mitgeteilt wird, an welchen Signalbegrifferzeuger (30, 32) die jeweiligen Hauptschlüssel (A bis E, N, X, Y) und ggfs. die jeweiligen Nebenschlüssel (C_{li}, C_{re}, F_{li}, E_{re}) zu senden sind.

3. Verfahren nach Anspruch 1 oder 2,
dadurch gekennzeichnet, dass
die Hauptschlüssel (A bis E, N, X, Y) und die ggfs. vorhandenen Nebenschlüssel (C_{li}, C_{re}, E_{li}, E_{re}) nach einem sicheren Codierverfahren (CRC, MD4) erzeugt werden und von dem Signalbegrifferzeuger (30, 32) auf Authenzität geprüft werden.

4. Verfahren nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet, dass
die Signalbegrifferzeuger (30, 32) den Stell- und Überwachungselementen (8 bis 24) den Erhalt eines authentizierbaren Hauptschlüssels und ggfs. weiterer Nebenschlüssel quittieren.

5. Verfahren nach einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet, dass
die Stell- und Überwachungselemente (8 bis 24) mit dem Senden ihres zugehörigen Hauptschlüssels (A bis E, N, X, Y) und ggfs. mit der Quittierung der Sendung zur erneuten Sendung ihres Hauptschlüssels (A bis E, N, X, Y) blockiert sind.

6. Verfahren nach einem der Ansprüche 1 bis 5,
dadurch gekennzeichnet, dass
ein zur Erzeugung des Signalbegriffs fehlender Hauptschlüssel (A bis E, N, X, Y) durch einen von einer Überwachungsinstanz explizit übermittelten Interventionsschlüssel ersetzbar ist.

7. Verfahren nach einem der Ansprüche 1 bis 6,
dadurch gekennzeichnet, dass
die Stell- und Überwachungselemente (8 bis 24), die ihre jeweiligen Hauptschlüssel (A bis E, N, X, Y) und ggfs. weitere Nebenschlüssel (C_{li}, C_{re}, E_{li}, E_{re}) an den Signalbegriffgenerierer (30, 32) gesendet haben, dem Signalbegriffgenerierer (30, 32) zyklisch die Zusicherung des gesendeten Hauptschlüssels (A bis E, N, X, Y) und ggfs. weiterer Nebenschlüssel (C_{li}, C_{re}, E_{li}, E_{re}) bestätigen.

8. Verfahren nach einem der Ansprüche 1 bis 7,
dadurch gekennzeichnet, dass
die für die Einstellung einer Fahrstrasse (FS) gesendeten Hauptschlüssel (A bis E, N, X, Y) und ggfs. weiterer Nebenschlüssel (C_{li}, C_{re}, E_{li}, E_{re}) nach einer komplettierten Befahrung der eingestellten Fahrstrasse (FS) zurückgegeben werden.

9. Verfahren nach einem der Ansprüche 1 bis 7,
dadurch gekennzeichnet, dass
die für die Einstellung einer Fahrstrasse (FS) gesendeten Hauptschlüssel (A bis E, N, X, Y) und ggfs. weiterer Nebenschlüssel (C_{li}, C_{re}, E_{li}, E_{re}) nach Fortschritt der Fahrt des Schienenfahrzeugs auf der eingestellten Fahrstrasse (FS) abschnittweise an die jeweiligen Stell- und Überwachungselemente (10 bis 18, 22) zurückgegeben werden.

10. Verfahren nach einem der Ansprüche 1 bis 9,
dadurch gekennzeichnet, dass
der Signalbegriffgenerierer (30, 32) einen für die angeforderte Fahrstrasse (FS) spezifizierten Algorithmus ausführt, der das Vorhandensein der erforderlichen Hauptschlüssel (A bis E, N, X, Y) sowie etwaiger Nebenschlüssel (C_{li}, C_{re}, E_{li}, E_{re}) überprüft.

11. System zur sicheren Einstellung von einer Fahrstrasse für ein Schienenfahrzeug, wobei der Fahrstrasse an den Fahrstrassen beteiligte Stell- und Überwachungselemente sowie deren etwaige, zur jeweiligen Fahrstrasse korrespondierende Zustände zugeordnet sind,
dadurch gekennzeichnet, dass
jedem Stell- und Überwachungselement ein eindeutiger Hauptschlüssel und etwaige eindeutige zu den möglichen Zuständen korrespondierende Nebenschlüssel zugeordnet sind, mit:

a) einer Leitstelle, in der die von dem Schienenfahrzeug zu befahrende Fahrstrasse anforderbar ist;
b) einer Kommunikationseinheit, mit der über ein Kommunikationsnetzwerk eine Mitteilung an die an der angeforderten Fahrstrasse beteiligten Stell- und Überwachungselemente aussendbar ist;
c) die Stell- und Überwachungselemente mit Rechenmitteln ausgestattet sind, mit denen in Antwort auf die ausgesendete Mitteilung ihre jeweilige Verfügbarkeit für die Einstellung des für die Fahrstrasse vorgesehenen Zustands prüfbar ist, wobei die Rechenmittel im Falle der jeweiligen Verfügbarkeit den erforderlichen Zustand einstellen bzw. das Vorliegen des für die Einstellung der Fahrstrasse erforderlichen Zustands verifizieren und wobei mittels der Rechenmittel im Falle des Vorliegens der genannten Verfügbarkeit der Hauptschlüssel und etwaige weitere Nebenschlüssel von jedem der an der Fahrstrasse beteiligten Stell- und Überwachungselemente über das Kommunikationsnetzwerk aussendbar sind; und
d) einem Signalbegrifferzeuger, mit dem ein mit der Anforderung der Fahrstrasse verbundener Signalbegriff für die angeforderte Fahrstrasse nur im Fall der vollständigen Übersendung der dieser Fahrstrasse zugeordneten Hauptschlüssel und etwaiger weiterer Nebenschlüssel erzeugbar ist.

12. System nach Anspruch 11,
dadurch gekennzeichnet, dass
für jede Fahrstrasse ein Signalbegrifferzeuger definierbar ist, wobei den an der Fahrstrasse beteiligten Stell- und Überwachungselementen im Rahmen der Mitteilung mitteilbar ist, an welchen Signalbegrifferzeuger die jeweiligen Hauptschlüssel und ggfs. die jeweiligen Nebenschlüssel zu senden sind.

13. System nach Anspruch 12,
dadurch gekennzeichnet, dass
der Signalbegrifferzeuger mit dem Stellelement assoziiert ist, das den jeweiligen Signalbegriff optisch an einem Signal ausgibt.

14. System nach Anspruch 12
dadurch gekennzeichnet, dass
der Signalbegrifferzeuger mit dem Stellelement assoziiert ist, das den jeweiligen Signalbegriff zur drahtlosen Übersendung an einen Bordcomputer des Schienenfahrzeugs an eine übergeordnete Instanz übergibt.

15. System nach einem der Ansprüche 11 bis 14,
dadurch gekennzeichnet, dass
die Hauptschlüssel und die ggfs. vorhandenen Nebenschlüssel nach einem sicheren Codierverfahren (CRC, MD4) erzeugt werden und von dem Signalbegrifferzeuger auf Authenzität geprüft werden..

16. System nach einem der Ansprüche 11 bis 15,
dadurch gekennzeichnet, dass
die Signalbegrifferzeuger den Stell- und Überwachungselementen den Erhalt eines authentizierbaren Hauptschlüssels und ggfs. weiterer authentizierbarer Nebenschlüssel quittiert.

17. System nach einem der Ansprüche 11 bis 16,
dadurch gekennzeichnet, dass
die Stell- und Überwachungselemente mit dem Senden ihres zugehörigen Hauptschlüssels und ggfs. mit der Quittierung der Sendung zur erneuten Sendung ihres Hauptschlüssels blockiert sind.

18. System nach einem der Ansprüche 11 bis 17,
dadurch gekennzeichnet, dass
eine Überwachungsinstanz einen zur Erzeugung des mit der Anforderung der Fahrstrasse gewünschten Signalbegriffs fehlenden Hauptschlüssel sowie einen etwaigen Nebenschlüssel durch einen explizit übermittelten Interventionsschlüssel ersetzt.

19. System nach einem der Ansprüche 11 bis 18,
dadurch gekennzeichnet, dass
die Stell- und Überwachungselemente, die ihre jeweiligen Hauptschlüssel und ggfs. weitere Nebenschlüssen an den Signalbegriffgenerierer gesendet haben, den Signalbegriffgenerierer zyklisch die Zusicherung des gesendeten Hauptschlüssels und ggfs. weiterer Nebenschlüssel bestätigen.

20. System nach einem der Ansprüche 11 bis 19,
dadurch gekennzeichnet, dass
der Signalbegrifferzeuger die für die Einstellung einer Fahrstrasse gesendeten Hauptschlüssel und ggfs. weiteren Nebenschlüssel nach einer komplettierten Befahrung der eingestellten Fahrstrasse an die jeweiligen Stell- und Überwachungselemente zurückgibt.

21. System nach einem der Ansprüche 11 bis 20,
dadurch gekennzeichnet, dass
der Signalbegrifferzeuger die für die Einstellung einer Fahrstrasse gesendeten Hauptschlüssel und ggfs. weiteren Nebenschlüssel nach Fortschritt der Fahrt des Schienenfahrzeugs auf der eingestellten Fahrstrasse abschnittweise an die jeweiligen Stell- und Überwachungselemente zurückgibt.

22. System nach einem der Ansprüche 11 bis 21,
dadurch gekennzeichnet, dass
der Signalbegriffgenerierer einen für die angeforderte Fahrstrasse spezifizierten Algorithmus ausführt, der das Vorhandensein der für die Erteilung einer Fahrerlaubnis über die angeforderte Fahrstrasse erforderlichen Hauptschlüssel sowie etwaiger Nebenschlüssel überprüft.

Claims

1. Method for secure setting of a route (FS) for a rail vehicle, wherein the route (FS) is assigned control and monitoring elements (8 to 24) involved in the route (FS) as well as any of their states corresponding to the route (FS), **characterised in that**
each control and monitoring element (8 to 24) is assigned a unique master key (A to E, N, X, Y) and any unique subsidiary keys (C_{li}, C_{re}, E_{li}, E_{re}) corresponding to the possible states, said method comprising the following steps:

a) the route (FS) to be travelled by the rail vehicle is requested;
b) a message is transmitted to the control and monitoring elements (10 to 18, 22) involved in the requested route (FS);
c) in response to the transmitted message the control and monitoring elements (10 to 18, 22) check their respective availability for setting the state provided for the route (FS) and in the event of their respective availability set said state or, as the case may be, verify the presence of the state required for setting the route (FS);
d) if the said availability is present the master key (A to E, N, X, Y) and any further subsidiary

keys (C_{li}, C_{re}, E_{li}, E_{re}) are also sent by each of the control and monitoring elements (10 to 18, 22) involved in the route (FS); and
e) a signal aspect for the requested route (FS) associated with the request for the route (FS) is generated only if the master keys (A to E, N, X, Y) assigned to said route (FS) and any further subsidiary keys (C_{li}, C_{re}, E_{li}, E_{re}) are transmitted in full.

2. Method according to claim 1,
characterised in that
a signal aspect generator (30, 32) is defined for each route (FS), wherein within the scope of the message it is communicated to the control and monitoring elements (10 to 18, 22) involved in the route (FS) to which signal aspect generator (30, 32) the respective master keys (A to E, N, X, Y) and where applicable the respective subsidiary keys (C_{li}, C_{re}, E_{li}, E_{re}) are to be sent.

3. Method according to claim 1 or 2,
characterised in that
the master keys (A to E, N, X, Y) and any subsidiary keys (C_{li}, C_{re}, E_{li}, E_{re}) present are generated in accordance with a secure coding method (CRC, MD4) and checked for authenticity by the signal aspect generator (30, 32).

4. Method according to one of claims 1 to 3,
characterised in that
the signal aspect generators (30, 32) acknowledge the receipt of an authenticatable master key and any further subsidiary keys to the control and monitoring elements (8 to 24).

5. Method according to one of claims 1 to 4,
characterised in that
with the transmission of their associated master key (A to E, N, X, Y) and where applicable with the acknowledgement of the transmission the control and monitoring elements (8 to 24) are blocked for a new transmission of their master key (A to E, N, X, Y).

6. Method according to one of claims 1 to 5,
characterised in that
a missing master key (A to E, N, X, Y) required for generating the signal aspect can be replaced by an intervention key explicitly transmitted by a monitoring entity.

7. Method according to one of claims 1 to 6,
characterised in that
the control and monitoring elements (8 to 24) which have sent their respective master keys (A to E, N, X, Y) and any further subsidiary keys (C_{li}, C_{re}, E_{li}, E_{re}) to the signal aspect generator (30, 32) cyclically confirm the acknowledgement of the transmitted master key (A to E, N, X, Y) and any further subsidiary keys (C_{li}, C_{re}, E_{li}, E_{re}) to the signal aspect generator (30, 32).

8. Method according to one of claims 1 to 7,
characterised in that
the master keys (A to E, N, X, Y) sent for the purpose of setting a route (FS) and any further subsidiary keys (C_{li}, C_{re}, E_{li}, E_{re}) are returned after travel over the set route (FS) has been completed.

9. Method according to one of claims 1 to 7,
characterised in that
the master keys (A to E, N, X, Y) sent for the purpose of setting a route (FS) and any further subsidiary keys (C_{li}, C_{re}, E_{li}, E_{re}) are returned to the respective control and monitoring elements (10 to 18, 22) section by section according to the rail vehicle's progress in travelling on the set route (FS).

10. Method according to one of claims 1 to 9,
characterised in that
the signal aspect generator (30, 32) executes an algorithm which is specified for the requested route (FS) and which checks the presence of the requisite master keys (A to E, N, X, Y) as well as any subsidiary keys (C_{li}, C_{re}, E_{li}, E_{re}).

11. System for secure setting of a route for a rail vehicle, wherein the route is assigned control and monitoring elements involved in the routes as well as any of their states corresponding to the respective route,
characterised in that
each control and monitoring element is assigned a unique master key and any unique subsidiary keys corresponding to the possible states, said system comprising:

a) a control centre in which the route to be travelled by the rail vehicle can be requested;
b) a communication unit by means of which a message can be transmitted over a communication network to the control and monitoring elements involved in the requested route;
c) control and monitoring elements which are equipped with computing means with the aid of which, in response to the transmitted message, their respective availability for setting the state provided for the route can be checked,
wherein in the event of the respective availability the computing means set the requisite state or, as the case may be, verify the presence of the state required for setting the route and wherein if the said availability is present the master key and any further subsidiary keys can be transmitted with the aid of the computing means over the communication network by each of the control and monitoring elements involved in the

route; and
d) a signal aspect generator by means of which a signal aspect for the requested route associated with the request for the route can be generated only if the master keys assigned to said route and any further subsidiary keys are transmitted in full.

12. System according to claim 11,
characterised in that
a signal aspect generator can be defined for each route, wherein within the scope of the message it can be communicated to the control and monitoring elements involved in the route to which signal aspect generator the respective master keys and where applicable the respective subsidiary keys are to be sent.

13. System according to claim 12,
characterised in that
the signal aspect generator is associated with the control element which outputs the respective signal aspect visually at a signal.

14. System according to claim 12,
characterised in that
the signal aspect generator is associated with the control element which passes on the respective signal aspect to a higher-ranking entity for wireless transmission to an onboard computer of the rail vehicle.

15. System according to one of claims 11 to 14,
characterised in that
the master keys and any subsidiary keys present are generated in accordance with a secure coding method (CRC, MD4) and checked for authenticity by the signal aspect generator.

16. System according to one of claims 11 to 15,
characterised in that
the signal aspect generator acknowledges the receipt of an authenticatable master key and any further authenticatable subsidiary keys to the control and monitoring elements.

17. System according to one of claims 11 to 16,
characterised in that
with the transmission of their associated master key and where applicable with the acknowledgement of the transmission the control and monitoring elements are blocked for a new transmission of their master key.

18. System according to one of claims 11 to 17,
characterised in that
a monitoring entity replaces a missing master key required for generating the signal aspect desired with the request for the route as well as any subsidiary key with an explicitly transmitted intervention key.

19. System according to one of claims 11 to 18,
characterised in that
the control and monitoring elements which have sent their respective master keys and any further subsidiary keys to the signal aspect generator cyclically confirm the acknowledgement of the transmitted master key and any further subsidiary keys to the signal aspect generator.

20. System according to one of claims 11 to 19,
characterised in that
the signal aspect generator returns the master keys sent for the purpose of setting a route and any further subsidiary keys to the respective control and monitoring elements after travel over the set route has been completed.

21. System according to one of claims 11 to 20,
characterised in that
the signal aspect generator returns the master keys sent for the purpose of setting a route and any further subsidiary keys to the respective control and monitoring elements section by section according to the rail vehicle's progress in travelling on the set route.

22. System according to one of claims 11 to 21,
characterised in that
the signal aspect generator executes an algorithm which is specified for the requested route and which checks the presence of the master keys required for the granting of a permit to travel over the requested route as well as any subsidiary keys.

Revendications

1. Procédé de réglage sécurisé d' un trajet (FS) d'un véhicule ferroviaire, dans lequel on affecte au trajet (FS) des éléments (8 à 24) de réglage et de contrôle participant au trajet ainsi que des états éventuels correspondants au trajet (FS),
caractérisé en ce que
on affecte, à chaque élément (8 à 24) de réglage et de contrôle, une clé (A à E, N, X, Y) principale univoque et éventuellement des clés (Cli, Cre, Eli, Ere) auxiliaires univoques correspondant aux états possibles, comprenant les stades de procédé suivantes:

a) le trajet (FS) à parcourir par le véhicule ferroviaire est demandé ;
b) on envoie une communication aux éléments (10 à 18, 22) de réglage et de contrôle participant au trajet (FS) demandé ;
c) en réponse à la communication envoyée, les

éléments (10 à 18, 22) de réglage et de contrôle vérifient leur disponibilité respective pour le réglage de l'état prévu pour le trajet (FS) et règlent cet état dans le cas où ils sont respectivement disponibles ou vérifient la présence de l'état nécessaire pour le réglage du trajet (FS) ;
d) dans le cas de la présence de ladite disponibilité, la clé (A à E, N, X, Y) principale et d'éventuelles autres clés (Cli, Cre, Eli, Ere) auxiliaires sont en outre envoyées par chaque élément (10 à 18, 22) de réglage et de contrôle participant au trajet (FS); et
e) une position de signal, en liaison avec la demande du trajet (FS) pour le trajet (FS) demandé, n'est produite que dans le cas de la transmission complète de la clé (A à E, N, X, Y) principale et d'éventuelles autres clés (Cli, Cre, Eli, Ere) auxiliaires éventuelles affectées à ce trajet (FS).

2. Procédé suivant la revendication 1, **caractérisé en ce que**
on définit pour chaque trajet (FS) un producteur (30, 32) de position de signal, en indiquant, dans le cadre de la communication aux éléments (10 à 18, 22) de réglage et contrôle faisant partie du trajet (FS), les producteurs (30, 32) de position de signal auxquels doivent être envoyées les clés (A à E, N, X, Y) respectives et éventuellement les clés (Cli, Cre, Eli, Ere) auxiliaires respectives.

3. Procédé suivant la revendication 1 ou 2, **caractérisé en ce que**
l'on produit les clés (A à E, N, X, Y) principales et les clés (Cli, Cre, Eli, Ere) auxiliaires éventuellement présentes par un procédé (CRC, MD4) de codage sécurisé et on en contrôle l'authenticité par le producteur (30, 32) de position de signal.

4. Procédé suivant l'une des revendications 1 à 3, **caractérisé en ce que**
les producteurs (30, 32) de position de signal accusent réception aux éléments (8 à 24) de réglage et de contrôle de la réception d'une clé principale et éventuellement d'autres clés auxiliaires pouvant être authentifiées.

5. Procédé suivant l'une des revendications 1 à 4, **caractérisé en ce que**
les éléments (8 à 24) de réglage et de contrôle sont empêchés de renouveler l'envoi de leur clé (A à E, N, X,) principale par l'envoi de leur clé (A à E, N, X, Y) principale associée et, éventuellement, par l'accusé de réception de l'envoi.

6. Procédé suivant l'une des revendications 1 à 5, **caractérisé en ce qu'**une clé (A à E, N, X, Y) principale manquante pour la production de la production de signal peut être remplacée par une clé d'intervention transmise explicitement par une instance de contrôle.

7. Procédé suivant l'une des revendications 1 à 6, **caractérisé en ce que**
les éléments (8 à 24) de réglage et de contrôle envoient aux producteurs (30, 32) de position de signal, leur clé (A à E, N, X, Y) principale respective et, le cas échéant, d'autres clés (Cli, Cre, Eli, Ere) auxiliaires confirment au producteur (30, 32) de position de signal cycliquement l'assurance de l'émission de la clé (A à E, N, X, Y) principale et le cas échéant d'autres clés (Cli, Cre, Eli, Ere) auxiliaires.

8. Procédé suivant l'une des revendications 1 à 7, **caractérisé en ce que**
les clés (A à E, N, X, Y) principales et le cas échéant d'autres clés (Cli, Cre, Eli, Ere) auxiliaires émises pour le réglage d'un trajet (FS) sont retournées après que le parcours du trajet (FS) réglé a été effectué complètement.

9. Procédé suivant l'une des revendications 1 à 7, **caractérisé en ce que**
les clés (A à E, N, X, Y) principales et le cas échéant d'autres clés (Cli, Cre, Eli, Ere) auxiliaires émises pour le réglage d'un trajet (FS) sont, après la progression du déplacement du véhicule sur le trajet (FS) réglé, retournées tronçon par tronçon aux éléments (10 à 18, 22) de réglage et de contrôle respectifs.

10. Procédé suivant l'une des revendications 1 à 9, **caractérisé en ce que**
le producteur (30, 32) de position de signal exécute un algorithme spécifié pour le trajet (FS) demandé, algorithme qui contrôle la présence de la clé (A à E, N, X, Y) principale nécessaire ainsi que d'éventuelles clés (Cli, Cre, Eli, Ere) auxiliaires.

11. Système de réglage sécurisé d'un trajet d' un véhicule ferroviaire, dans lequel il est affecté au trajet des éléments de réglage et de contrôle participant au trajet, ainsi que d'éventuels états correspondants au trajet respectif, **caractérisé en ce que**
il est affecté à chaque élément de réglage et de contrôle une clé principale univoque et d'éventuelles clés auxiliaires univoques correspondants aux états possibles,
comprenant:

a) un poste de pilotage dans lequel le trajet à parcourir par le véhicule ferroviaire peut être demandé ;
b) une unité de communication par laquelle, par l'intermédiaire d'un réseau de communication, une communication peut être envoyée aux élé-

ments de réglage et de contrôle faisant partie du trajet demandé ;
c) les éléments de réglage et de contrôle sont équipés de moyens informatiques par lesquels, en réponse à la communication envoyée, leur disponibilité respective pour le réglage de l'état prévu pour le trajet peut être contrôlé, les moyens informatiques réglant, dans les cas de la disponibilité respective, l'état nécessaire ou vérifiant la présence de l'état nécessaire pour le réglage du trajet, et dans lequel, à l'aide des moyens informatiques dans le cas de la présence de ladite disponibilité, la clé principale et d'éventuelles autres clés auxiliaires peuvent être envoyées par l'intermédiaire du réseau de communication par chacun des éléments de réglage et de contrôle participant au trajet ; et
d) un producteur de position de signal par lequel une position de signal pour le trajet exigé, position de signal qui est reliée à la demande du trajet, ne peut être produite que dans le cas de la transmission complète de la clé principale affectée à ce trajet et d'éventuelles autres clés auxiliaires.

12. Système suivant la revendication 11,
caractérisé en ce que
pour chaque trajet un producteur de position de signal peut être défini, dans lequel aux éléments de réglage et de contrôle participant au trajet peuvent être communiqués, dans le cadre de la communication, les producteurs de position de signal auxquels les clés principales respectives et le cas échéant les clés auxiliaires respectives doivent être envoyées.

13. Système suivant la revendication 121,
caractérisé en ce que
le producteur de position de signal est associé à l'élément de réglage, qui émet la position de signal respective visuellement sur un signal.

14. Système suivant la revendication 12,
caractérisé en ce que
le producteur de position de signal est associé à l'élément de réglage, qui transmet, à une instance supérieure hiérarchiquement, la position de signal respective pour la transmission sans fil à un ordinateur de bord du véhicule ferroviaire.

15. Système suivant l'une des revendications 11 à 14,
caractérisé en ce que
les clés principales et les clés auxiliaires éventuellement présentes sont produites suivant un procédé de codage sécurisé (CRC, MD4) et leur authenticité est contrôlée par le producteur de position de signal.

16. Système suivant l'une des revendications 11 à 15,
caractérisé en ce que
le producteur de signal accuse réception, aux éléments de réglage et de contrôle, de la réception d4une clé principale authentifiable et le cas échéant d'autres clés auxiliaires authentifiables.

17. Système suivant l'une des revendications 11 à 16,
caractérisé en ce que
les éléments de réglage et de contrôle sont empêchés de renouveler l'envoi de leur clé principale par l'envoi de leur clé principale associée le cas échéant par l'accusé de réception de l'envoi.

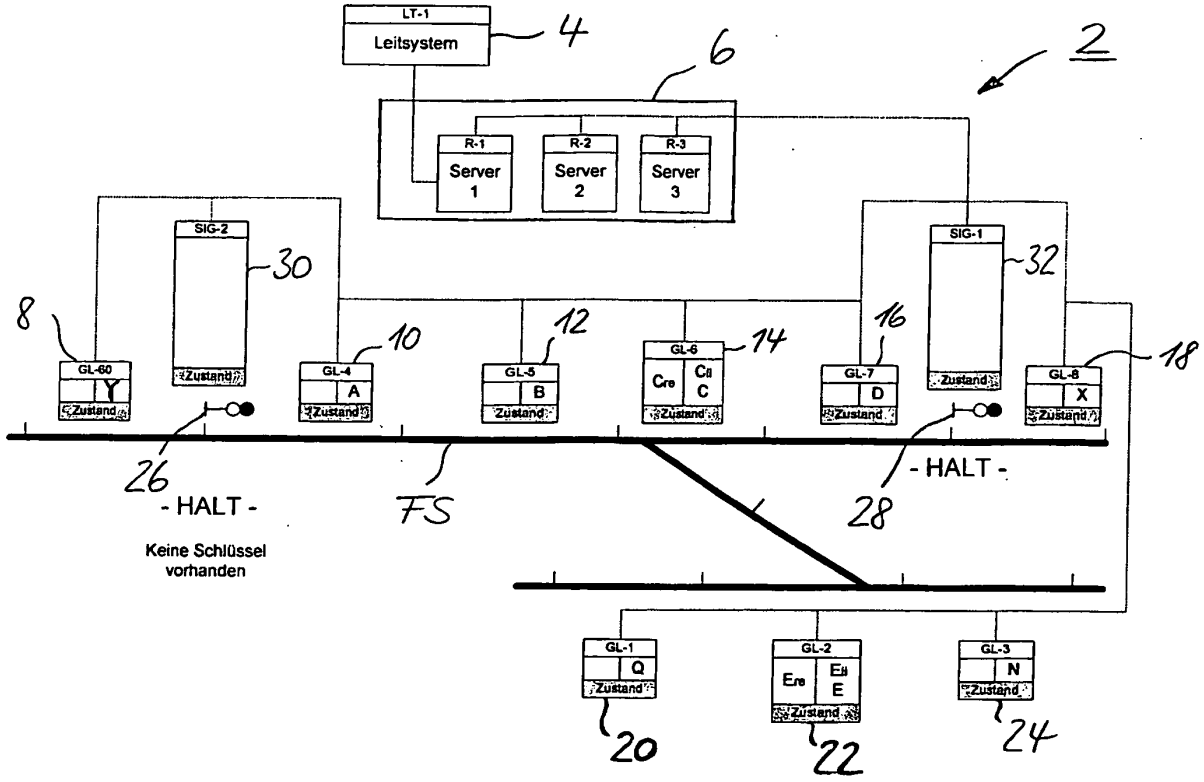
18. Système suivant l'une des revendications 11 à 17,
caractérisé en ce qu'une instance de contrôle remplace une clé principale manquante pour la production de la position de signal souhaitée par la demande de trajet, ainsi que d'éventuelles clés auxiliaires par une clé d'intervention transmise explicitement.

19. Système suivant l'une des revendications 11 à 18,
caractérisé en ce que
les éléments de réglage et de contrôle, qui ont envoyés leur clé principale et le cas échéant d'autres clés auxiliaires aux producteurs de position de signal, confirment aux producteurs de position de signal cycliquement l'assurance que la clé principale et éventuellement d'autres clés auxiliaires ont été envoyées.

20. Système suivant l'une des revendications 11 à 19,
caractérisé en ce que
le producteur de position de signal retourne, aux éléments respectifs de réglage et de contrôle, de la clé principale envoyée pour réglage d'un trajet et le cas échéant d'autres clés auxiliaires, après que le trajet réglé a été parcouru complètement.

21. Système suivant l'une des revendications 11 à 20,
caractérisé en ce que
le producteur de position de signal retourne, aux éléments respectifs de réglage et de contrôle, par tronçon sur le trajet réglé, la clé principale et le cas échéant d'autres clés auxiliaires envoyées pour le réglage d'un trajet après que le véhicule a progressé.

22. Système suivant l'une des revendications 11 à 21,
caractérisé en ce que
le producteur de position de signal exécute pour le trajet demandé un algorithme spécifié qui contrôle la présence de la clé principale ainsi que d'éventuelles clés auxiliaires nécessaires pour l'accord d'un permis de parcourir le trajet demandé.



Legende:

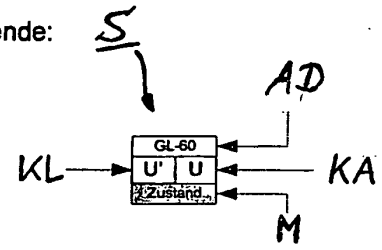


Fig. 1

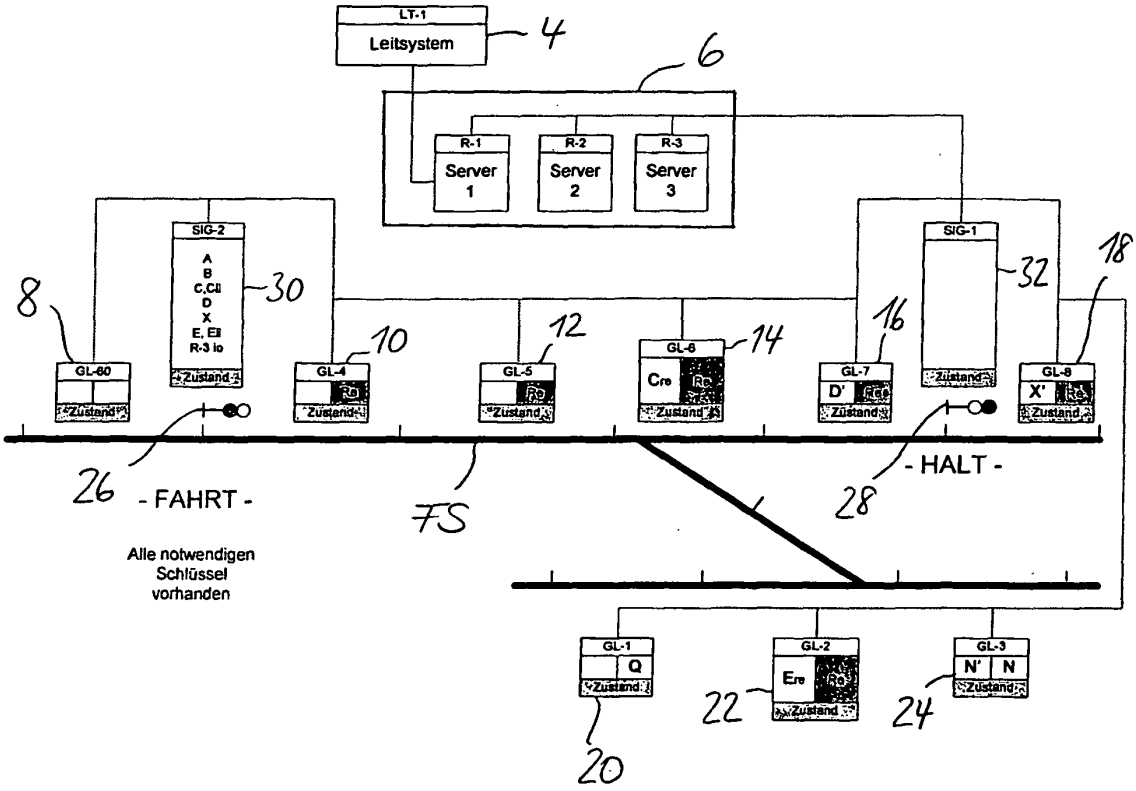

LT-1
Leitsystem
4
6
R-1
Server 1
R-2
Server 2
R-3
Server 3
SIG-2
A
B
C,CII
D
X
E, EII
R-3 io
30
SIG-1
32
18
8
GL-60
Zustand
GL-4
10
GL-5
12
GL-6
Cre
14
GL-7
D'
16
GL-8
X'
26
- FAHRT -
FS
28
- HALT -
Alle notwendigen Schlüssel vorhanden
GL-1
Q
GL-2
Ere
GL-3
N' N
22
24
20

Fig. 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 Nicht-Patentliteratur

- Elektronische Stellwerke - ein internationaler überblick. **U. Maschek.** Zeitschrift SIGNAL + DRAHT. Telzlaff Verlag GmbH, 01. Marz 1997, vol. 89, 15, 16, 18-23 **[0002]**