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

(11) **EP 1 669 824 B1**

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
09.01.2008 Patentblatt 2008/02

(51) Int Cl.:
G05B 19/05 *(2006.01)*

(21) Anmeldenummer: **05110582.3**

(22) Anmeldetag: **10.11.2005**

(54) **Verfahren und Vorrichtung zur Vorgabe einer Betriebsartennummer**

Method and apparatus for setting an operation mode number

Procédé et dispositif pour la sélection d'un numéro mode d'opération

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

(30) Priorität: **08.12.2004 DE 102004059717**

(43) Veröffentlichungstag der Anmeldung:
14.06.2006 Patentblatt 2006/24

(73) Patentinhaber: **SIEMENS AKTIENGESELLSCHAFT**
80333 München (DE)

(72) Erfinder: **Temming, Rudolf**
38154, Königslutter (DE)

(56) Entgegenhaltungen:
DE-A1- 4 114 921
DE-A1- 10 040 866
US-A- 5 485 590
US-A- 5 659 705

- **LENNARTZ K: "SIGNALTECHNISCH SICHERE DATENUEBERTRAGUNG IM RAHMEN VON CIRNET" 1. April 1993 (1993-04-01), SIGNAL + DRAHT, TELZLAFF VERLAG GMBH. DARMSTADT, DE, PAGE(S) 96-101 , XP000380305 ISSN: 0037-4997 * Absatz [03.4] ***
- **RIVEST R L ED - MENEZES A J ET AL INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH: "THE MD4 MESSAGE DIGEST ALGORITHM" 30. Dezember 1991 (1991-12-30), ADVANCES IN CRYPTOLOGY - PROCEEDINGS OF CRYPTO. SANTA BARBARA, AUG. 11, PAGE(S) 303-311 , XP000260021 * Zusammenfassung * * Seite 304, Absatz 3 ***
- **"ST24C04, ST25C04, ST24W04, ST25W04, 4kBit Serial I2C Bus EEPROM with user defined Block Write Protection" Februar 1999 (1999-02), ANNOUNCEMENT ST MICROELECTRONICS, PAGE(S) 1-16 , XP002206612 * das ganze Dokument ***

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist. (Art. 99(1) Europäisches Patentübereinkommen).

EP 1 669 824 B1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Vorgabe einer Betriebsartennummer gemäß dem Oberbegriff des Anspruchs 1 und eine diesbezügliche Vorrichtung gemäß dem Oberbegriff des Anspruchs 2.

[0002] Sicherheitsrelevante Bahnbetriebsprozesse betreffen insbesondere die Ansteuerung von Feldelementen, beispielsweise Weichen und Signale. Dazu dienen Stellwerkselemente, über die unter anderem auch Betriebsartennummern, beispielsweise für Normalbetrieb oder Antriebsersatz, vorgegeben werden. Mit der Betriebsartennummer wird die Verarbeitungssoftware der Stellwerkselemente in bestimmter Weise initialisiert, d. h. zu einem bestimmten Verhalten gezwungen. Die Betriebsartennummer muss daher signaltechnisch sicher vorgegeben werden.

[0003] Bekannt sind Betriebsartenstecker, die durch Brücken im Stecker das Verhalten der Verarbeitungssoftware bestimmen. Nachteilig bei diesen Betriebsartensteckern ist vor allem deren erheblicher Hardwareaufwand.

[0004] Aus der US-A-5 659 705 ist eine speicherprogrammierbare Steuerung mit einem herausnehmbaren Programmspeicher bekannt, wodurch eine Anpassung an andere Parameter möglicht ist. Bei der Implementierung eines Datensatzes in die speicherprogrammierbare Steuerung ist eine Prüfsummenbildung vorgesehen.

[0005] Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren und eine Vorrichtung gattungsgemäßer Art anzugeben, die sich durch geringeren Hardwareaufwand auszeichnen, wobei die Betriebsartenwahl die Sicherheitsanforderungsstufe SIL 4 nach CENELEC erfüllt.

[0006] Die Aufgabe wird verfahrensgemäß mit den kennzeichnenden Merkmalen des Anspruches 1 und vorrichtungsgemäß mit den kennzeichnenden Merkmalen des Anspruches 2 gelöst. Durch das Einschreiben der Betriebsartennummer und der Teilnehmeradresse zusammen mit einem Sicherungsanhang in einen nichtflüchtigen Speicher ist eine sehr hohe Sicherheit bezüglich der Korrektheit der Betriebsartennummer und damit der entsprechenden Auswirkungen auf den sicherheitsrelevanten Bahnbetriebsprozess gegeben. Ein weiterer Vorteil gegenüber dem bekannten Betriebsartenstecker mit Brücken besteht darin, dass neben der Betriebsartennummer zusätzlich weitere Daten gespeichert werden können. Darüber hinaus ist bei geringem Volumen des Speichermoduls nur minimaler Hardwareaufwand erforderlich. Der Datensatz, bestehend aus Betriebsartennummer, Teilnehmeradresse, gegebenenfalls weiteren Daten und Sicherungsanhang, lässt sich über eine serielle I2C-Schnittstelle sehr einfach und mit besonders geringem Aufwand in den nichtflüchtigen Speicher einlesen. Da üblicherweise mehrere Komponenten parallel an einem I2C-Bus hängen, ist es nötig, auch die Teilnehmeradresse zu speichern. Der I2C-Bus ist ein sehr häufig eingesetzter 2-Draht-Bus und wurde speziell für die Kommunikation zwischen einzelnen Komponenten innerhalb eines Gerätes entwickelt. Vorteilhafterweise wird auch zwischen dem Speicher und einem Frontplattenmodul der Verarbeitungssoftware ein I2C-Bus eingesetzt, wobei das Frontplattenmodul den Datensatz zweikanalig mittels des Sicherungsanhangs auf Datenintegrität überprüft.

[0007] Vorzugsweise ist der Sicherungsanhang gemäß Anspruch 3 als MD4-Signatur (Message Digest) ausgebildet. Durch die kryptografische MD4-Funktion wird der Eingabedatensatz in einen kurzen Wert fester Länge, den Hashwert, umgewandelt. Bei diesem Algorithmus verändern sich Variablen mittels nichtlinearer Transformationen anhand der Eingabedaten, d. h. des auf Datenintegrität zu prüfenden Datensatzes, und bilden dadurch einen eindeutigen Hashwert. Bei einer guten Hashfunktion gibt es kaum zwei Datensätze, die denselben Hashwert besitzen. Weiterhin beeinflussen geringe Änderungen des Eingabedatensatzes bei einer guten Hashfunktion den Hashwert sehr stark. Bei dem MD4-Algorithmus sind vier Variablen vorgesehen, die in drei Runden in die Berechnung des Hashwertes eingehen. Um noch größere Sicherheit hinsichtlich des Nachweises der Datenintegrität zu erreichen, kann auch eine höhere Version des MD-Algorithmus, beispielsweise MD5 eingesetzt werden. Es können auch andere Verfahren zur Sicherung genutzt werden, beispielsweise CRC16 oder CRC32. Der Sicherungsanhang wird über den gesamten Datensatz gebildet.

[0008] Als nichtflüchtiger Speicher wird gemäß Anspruch 4 vorzugsweise ein EEPROM (electrically erasable programmable read only memory) eingesetzt. Dieser Festwertspeicher zeichnet sich dadurch aus, dass der Programmiervorgang und auch der Löschvorgang sehr einfach mittels eines Computers oder eines Peripheriegerätes möglich sind.

[0009] Der Speicher selbst ist gemäß Anspruch 5 in einem Betriebsartenstecker integriert. Der Betriebsartenstecker ist vorzugsweise äußerlich mit der Betriebsartennummer beschriftet und wird bedarfsweise in ein Frontplattenmodul eines Mikro-Controllers, der die Verarbeitungssoftware enthält, eingesetzt.

[0010] Nachfolgend wird die Erfindung anhand figürlicher Darstellungen naher erläutert.

[0011] Es zeigen:

- Figur 1 Betriebsartenstecker im Zusammenwirken mit einem Frontplattenmodul und
- Figur 2 eine Architekturspezifikation des Betriebsartensteckers.

[0012] Figur 1 zeigt beispielhaft zwei Betriebsartenstecker 1 und 2, wobei der erste Betriebsartenstecker 1 für Normalbetrieb und der zweite Betriebsartenstecker 2 für Antriebsersatz bei der Ansteuerung einer Weichenbaugruppe vorgesehen sind. Die Betriebsartenstecker 1 und 2 sind jeweils mit einem EEPROM 3 (Fig. 2) zur Speicherung der zugeordneten Betriebsartennummer 4a, einer Teilnehmernummer 4b, einer Teilnehmeradres-

se 5 und einer MD4-Signatur 6 ausgestattet (Figur 2). Damit der Betriebsartenstecker 1 bzw. 2 in ein Frontplattenmodul 7, das mit einem Mikro-Controller 8 (Figur 2) verbunden ist, auf einfache Weise eingesteckt und abgezogen werden kann, ist ein Griff 9 an den Betriebsartenstecker 1 bzw. 2 angeformt. Der Betriebsartenstecker 1 bzw. 2 ist dabei derart gestaltet, dass ein kontaktsicheres Einstecken in eine Steckerbuchse 10 des Frontplattenmoduls 7 möglich ist, wobei der Betriebsartenstecker 1 bzw. 2 bündig mit der Oberfläche des Frontplattenmoduls 7 abschließt und sich nicht durch Erschütterungen lösen kann. Wird kein Betriebsartenstecker 1 bzw. 2 genutzt, kann auch eine Blindplatte ohne jede elektrische Funktionalität gesteckt werden. Mit dem Betriebsartenstecker 1 bzw. 2 wird der Verarbeitungssoftware in dem Mikro-Controller 8 mitgeteilt, wie sie sich zu verhalten hat. Der Betriebsartenstecker 1 bzw. 2 ist mit der Nummer der Betriebsart deutlich beschriftet. Diese Nummer wird blinkend in einem Diagnosedisplay 11 auf dem Frontplattenmodul 7 angezeigt. Der signaltechnisch sicher aufgebaute Mikro-Controller 8 liest zyklisch über das Frontplattenmodul 7 den Datensatz aus dem Betriebsartenstecker 1 bzw. 2. Auf dem Frontplattenmodul 7 sind neben der Steckerbuchse 10 und dem Diagnosedisplay 11 verschiedene Schalter 12 und 13, eine Diagnosebuchse 14 sowie Statusanzeigen 15 und eine LED-Matrix 16 zur Prozessanzeige vorgesehen.

[0013] Figur 2 veranschaulicht den Datenfluss von dem Betriebsartenstecker 1 bzw. 2 über dass Frontplattenmodul 7 zum Mikro-Controller 8. Der Datensatz für den Betriebsartenstecker 1 bzw. 2 wird über eine I2C-Schnittstelle 17 geladen. Dabei muss sichergestellt sein, dass die Daten des Betriebsartensteckers 1 bzw. 2 im gesteckten Zustand nicht verändert werden können. Weiterhin ist der Betriebsartenstecker 1 bzw. 2 mit einer Stromversorgung 18 und einem seriellen I2C-Bus 19 verbunden. Über den 12C-Bus 19 liest das Frontplattenmodul 7 den Datensatz und überprüft diesen zweikanalig anhand der MD4-Signatur auf Datenintegrität. Danach wird die Betriebsartennummer ohne MD4-Signatur an die Abbildspeicher des zweikanaligen Mikro-Controllers 8 weitergeleitet. Wird der Betriebsartenstecker 1 bzw. 2 gezogen oder hat die Betriebsartennummer 4a sich geändert, wird auf dem Diagnosedisplay 11 des Frontplattenmoduls 7 ein Fehler angezeigt. Da die Betriebsartennummer 4a auf dem EEPROM 3 durch die MD4-Signatur 6 abgesichert ist, kann die Datenintegrität auf sehr hohem Sicherheitsniveau gemäß der Sicherheitsanforderungsstufe SIL 4 nach CENELEC überwacht werden.

Patentansprüche

1. Verfahren zur Vorgabe einer Betriebsartennummer (4a) für sicherheitsrelevante Bahnbetriebsprozesse,
   dadurch gekennzeichnet,
   dass ein Datensatz, bestehend aus der Betriebsartennummer (4a), einer Teilnehmeradresse (5) und gegebenenfalls weiteren Daten, gebildet wird, wobei ein Sicherungsanhang über dem gesamten Datensatz gebildet wird und der Datensatz samt Sicherungsanhang über eine serielle I2C-Schnittstelle (17) in einen nichtflüchtigen Speicher eingelesen wird und dass ein Frontplattenmodul (7) den Datensatz über einen I2C-Bus (19) liest und zweikanalig mittels des Sicherungsanhangs auf Datenintegrität überprüft.

2. Vorrichtung zur Durchführung des Verfahrens nach Anspruch 1,
   dadurch gekennzeichnet,
   dass ein nichtflüchtiger Speicher mit einer seriellen I2C-Schnittstelle (17) vorgesehen ist, wobei die Betriebsartennummer (4a), eine Teilnehmeradresse (5) und gegebenenfalls weitere Daten, als Datensatz mit einem Sicherungsanhang über die I2C-Schnittstelle (17) in den Speicher einlesbar sind, dass der Speicher über einen I2C-Bus (19) mit einem Frontplattenmodul (7) verbunden ist und
   dass das Frontplattenmodul (7) Mittel zur zweikanaligen Überprüfung des Datensatzes auf Datenintegrität mittels des Sicherungsanhangs aufweist.

3. Vorrichtung nach Anspruch 2,
   dadurch gekennzeichnet,
   dass der Sicherungsanhang als MD4-Signatur (6) über den gesamten Datensatz ausgebildet ist.

4. Vorrichtung nach Anspruch 2 oder 3,
   dadurch gekennzeichnet,
   dass der Speicher als EEPROM (3) ausgebildet ist.

5. Vorrichtung nach einem der Ansprüche 2 bis 4,
   dadurch gekennzeichnet,
   dass der Speicher in einem Betriebsartenstecker (1, 2) integriert ist.

Claims

1. Method for prescribing an operating mode number (4a) for safety-related rail operating processes,
   characterized
   in that a data record, comprising the operating mode number (4a), a subscriber address (5) and possibly further data, is formed, with a backup attachment being formed over the entire data record and the data record together with the backup attachment being read into a non-volatile memory via a serial I2C interface (17), and in that a front panel module (7) reads the data record via an I2C bus (19) and checks for data integrity over two channels using the backup attachment.

2. Apparatus for carrying out the method according to Claim 1,

characterized
in that a non-volatile memory having a serial 12C interface (17) is provided, with the operating mode number (4a), a subscriber address (5) and possibly further data being able to be read into the memory via the I2C interface (17) as a data record with a backup attachment, in that the memory is connected to a front panel module (7) via an I2C bus (19), and **in that** the front panel module (7) has means for checking the data record for data integrity over two channels using the backup attachment.

3. Apparatus according to Claim 2, **characterized** **in that** the backup attachment is in the form of an MD4 signature (6) relating to the entire data record.

4. Apparatus according to Claim 2 or 3, **characterized** **in that** the memory is in the form of an EEPROM (3).

5. Apparatus according to one of Claims 2 to 4, **characterized** **in that** the memory is integrated in an operating mode connector (1, 2).

Revendications

1. Procédé pour prescrire un numéro de mode d'opération (4a) pour des processus d'exploitation ferroviaire déterminants pour la sécurité, **caractérisé par le fait que** l'on forme un bloc de données constitué du numéro de mode d'opération (4a), d'une adresse d'utilisateur (5) et éventuellement d'autres données, un supplément de sécurité étant formé sur l'ensemble du bloc de données et le bloc de données étant écrit conjointement avec le supplément de sécurité dans une mémoire non volatile par l'intermédiaire d'une interface I2C sérielle (17), et **par le fait qu'**un module frontal d'entrée (7) lit le bloc de données par l'intermédiaire d'un bus I2C (19) et vérifie l'intégrité des données sur deux canaux au moyen du supplément de sécurité.

2. Dispositif pour la mise en oeuvre du procédé selon la revendication 1, **caractérisé par le fait que** il est prévu une mémoire non volatile avec une interface I2C sérielle (17), le numéro de mode d'opération (4a), une adresse d'utilisateur (5) et éventuellement d'autres données pouvant être écrites comme bloc de données avec un supplément de sécurité dans la mémoire par l'intermédiaire de l'interface I2C (17), la mémoire est reliée à un module frontal d'entrée (7) par l'intermédiaire d'un bus I2C (19), et le module frontal d'entrée (7) comporte des moyens pour la vérification sur deux canaux de l'intégrité des données du bloc de données au moyen du supplément de sécurité.

3. Dispositif selon la revendication 2, **caractérisé par le fait que** le supplément de sécurité est conçu comme une signature MD4 (6) sur l'ensemble du bloc de données.

4. Dispositif selon la revendication 2 ou 3, **caractérisé par le fait que** la mémoire est conçue comme une EEPROM (3).

5. Dispositif selon l'une des revendications 2 à 4, **caractérisé par le fait que** la mémoire est intégrée dans un connecteur de mode d'opération (1, 2).

FIG 1

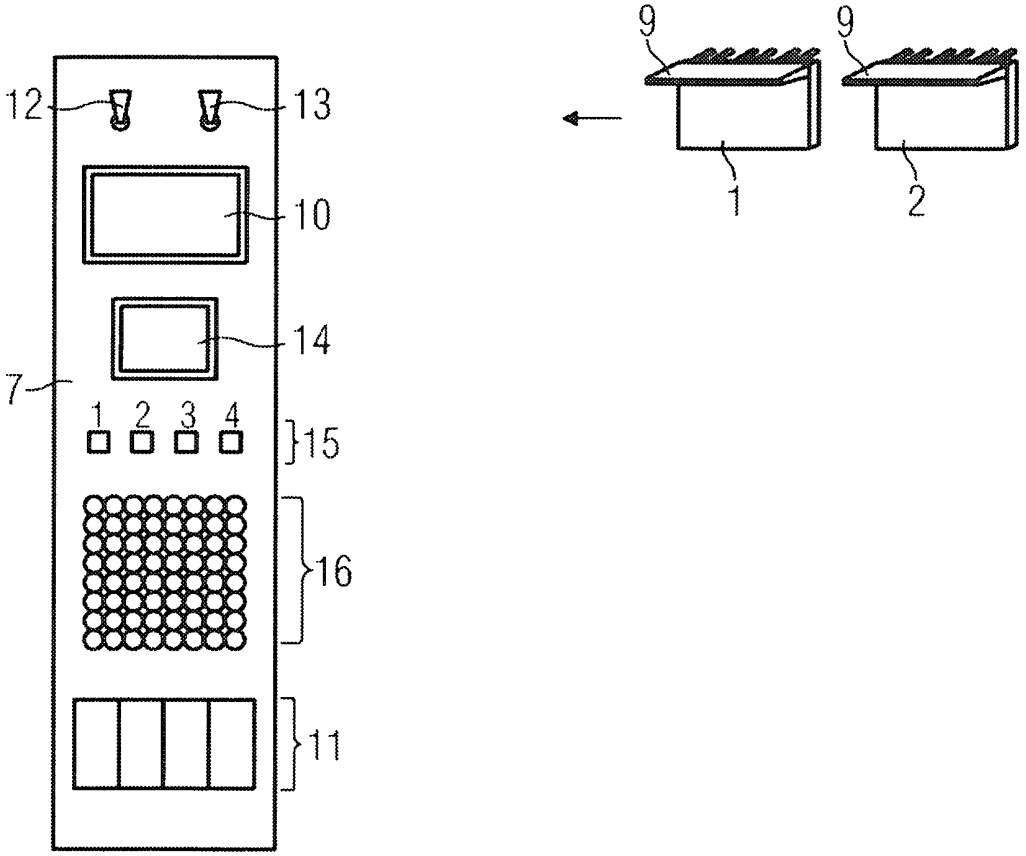
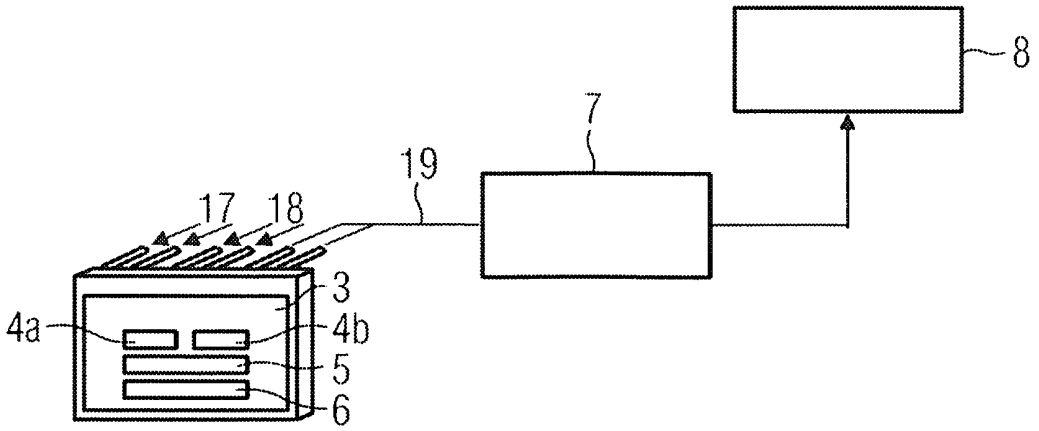


FIG 2



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 Patentdokumente

- US 5659705 A **[0004]**