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

(11) **EP 3 549 842 B2**

(12) **NEW EUROPEAN PATENT SPECIFICATION**
After opposition procedure

(45) Date of publication and mention of the opposition decision:
12.02.2025 Bulletin 2025/07

(45) Mention of the grant of the patent:
11.05.2022 Bulletin 2022/19

(21) Application number: **18177217.9**

(22) Date of filing: **12.06.2018**

(51) International Patent Classification (IPC):
B61L 19/06 *(2006.01)* ***B61L 21/06*** *(2006.01)*
B61L 27/00 *(2022.01)* ***B61L 25/06*** *(2006.01)*

(52) Cooperative Patent Classification (CPC):
B61L 19/06; B61L 21/06; B61L 25/06; B61L 27/20; B61L 27/30; B61L 27/50; B61L 2019/065

(54) **TRAIN TRAFFIC CONTROL SYSTEM AND METHOD FOR SAFE DISPLAYING A STATE INDICATION OF A ROUTE AND TRAIN CONTROL SYSTEM**

ZUGVERKEHRSLEITSYSTEM UND VERFAHREN ZUR SICHEREN ANZEIGE EINER ZUSTANDSANZEIGE EINER STRECKE UND ZUGVERKEHRSLEITSYSTEM

SYSTÈME DE CONTRÔLE DU TRAFIC FERROVIAIRE ET PROCÉDÉ DE SÉCURISATION DE L'AFFICHAGE D'UNE INDICATION D'ÉTAT D'UNE ROUTE ET SYSTÈME DE COMMANDE DE TRAIN

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

(30) Priority: **06.04.2018 DE 102018205235**
06.04.2018 EP 18166202

(43) Date of publication of application:
09.10.2019 Bulletin 2019/41

(73) Proprietor: **Hitachi Rail GTS Deutschland GmbH**
71254 Ditzingen (DE)

(72) Inventors:
- **SCHÄFER, Michael**
  70806 Kornwestheim (DE)
- **TIPLÉ, Abhay**
  70188 Stuttgart (DE)

(74) Representative: **Kohler Schmid Möbus Patentanwälte**
Partnerschaftsgesellschaft mbB
Gropiusplatz 10
70563 Stuttgart (DE)

(56) References cited:

EP-A1- 2 244 188
EP-A1- 2 551 787
EP-A1- 3 040 862
EP-A2- 1 942 041
EP-B1- 1 750 988
EP-A1- 2 551 787
EP-A1- 3 040 862
EP-A1- 3 082 127
EP-A2- 1 942 041
EP-B1- 1 750 988
WO-A2-03/093999
DE-A1- 102011 005 188
DE-A1- 102014 201 551
DE-A1- 102015 209 448
US-A1- 2009 254 986
US-A1- 2010 271 194
US-A1- 2011 157 222
US-A1- 2014 088 802
US-A1- 2016 267 885
US-A1- 2016 379 381
WO-A2-03/093999
DE-A1- 102012 207 439
DE-A1- 102014 201 551
DE-A1- 4 306 470
US-A1- 2009 254 986
US-A1- 2011 057 951
US-A1- 2011 199 308
US-A1- 2015 277 838
US-A1- 2016 379 331

- **LAUMEN HEINZ, HENNING STEFFEN: "Das Stellwerk ZSB2000 für die Anwendung ESZB", SIGNAL + DRAHT, EURALPRESS, HAMBURG, vol. 96, 1 January 2004 (2004-01-01), pages 32 - 36, XP093028931**
- **INA BLEICHER: "Herausforderungen des neuen integrierten Bediensystems bei der DB Netz AG", SIGNAL UND DRAHT: SIGNALLING & DATACOMMUNICATION, EURAILPRESS, DE, vol. 106, no. 4, 1 April 2014 (2014-04-01), DE , pages 30 - 33, XP001587950, ISSN: 0037-4997**
- **SPEISER NORBERT: "Ein Bedien-kommando im ESTW mit besonderer Bedeutung", BAHNPRAXIS, 1 May 2007 (2007-05-01), pages 6 - 9, XP093028937**
- **RUDOLF GANZ: "Sichere Anzeige und Bediensysteme Sicherheit schafft Vertrauen", EB- ELEKTRISCHE BAHNEN, DIV-DEUTSCHER INDUSTRIEVERLAG, DE, vol. 109, no. 3, 1 March 2011 (2011-03-01), DE , pages 131 - 134, XP001526115, ISSN: 0013-5437**

Processed by Luminess, 75001 PARIS (FR)

(Cont. next page)

- VIEIRA PAULO, QUARESMA MANUEL, JERONYMO, OSVALDO-SENIOR: "An Ergonomic Design for a HMI of Locomotives in a CBTC System", 9111 INTERNATIONAL HEAVY HAUL CONFERENCE, 1 January 2009 (2009-01-01), pages 689 - 695, XP093028948
- BÜCKER CHRISTOPH, HEUER VOLKMAR: "Traffic Management System (TMS) in großen Betriebszentralen Traffic Management System (TMS) in large operations control centres", SIGNALLING + DATACOMMUNICATION, vol. 108, no. 1-2, 1 February 2016 (2016-02-01), pages 51 - 57, XP093119205
- ENGELBART PATRICK: "Hochrüsten von ESTW Hochrüsten von ESTW für die Anbindung an eine Betriebszentrale", SIGNAL + DRAHT, vol. 93, no. 7-8, 1 August 2001 (2001-08-01), pages 22 - 26, XP093119208
- HEUER VOLKMAR, BRECKEL HEIKO, HOWE NORBERT: "Digitale, mobile Verkehrssteuerung im Baustellenbereich für ETCS-L2-Strecken Digital, mobile traffic control and possession management for ETCS L2 lines", SIGNAL + DRAHT, vol. 113, 1 September 2021 (2021-09-01), pages 52 - 59, XP093182937
- BSI: "Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Part 1: Generic RAMS Process", BSEN 50126-1:2017, 1 November 2017 (2017-11-01), XP093182938
- SCHUBATH STEFAN, GROTHEER ULF: "Neues SIMIS-W-Stellwerk in Polen", SIGNAL + DRAHT, vol. 94, 1 June 2002 (2002-06-01), pages 27 - 31, XP093189443
- ANONYMOUS: "EN 50128", WIKIPEDIA, XP093189448, Retrieved from the Internet <URL:https://de.wikipedia.org/w/index.php?title=EN%2050128&oldid=240766907>
- "Systementwicklungsprojekt Integration eines X-Servers in VR-Systemen", Georgi Nachev, Dimitar Marinov, Technische Universität München, 18.November 2005, Kapitel 6.2.1.3 X-Protokoll basierte Kommunikation
- Nachev/XinCAVE_2005.pdfAVE_2005.pdf WaybackMachine - Screenshot dated 10.08.2017 https://campar.in.tum.de/twiki/pub/Students/SepMarinoy
- Robert W. Scheifler, Jim Gettys : "The X Window System" ACM Transactions on Graphics, Vol. 5, No. 2, April 1986, Pages 79-109

Description

Background of the invention

[0001] The invention concerns a train traffic control system comprising a route and train control system, an operator workstation with a display, and a safe state indication component with safety level SIL>0, in particular SIL4, for indicating safety-related information concerning the state of elements of the route and train control system on the display of the operator workstation. The invention further concerns a method for safe displaying a state indication of a route and train control system.

[0002] An according train traffic control system is known from [1]

[0003] Route and train control systems are adapted to manage safely routes and movement-authorities in railway networks for running trains and to control protect and protect trains from running to fast or beyond their end of movement-authority. Typical route and train control systems are for example interlocking systems, radio-block-centers or similar systems.

[0004] Remote control for controlling interlocking systems and other route and train control systems via traffic management systems getting increasingly important. Traffic management systems comprise human machine interfaces for operating route and train control systems by a human operator. The route and train control system receives commands from the traffic management system concerning regular operation as well as concerning safety critical operations. Safety critical operations are carried out by using the route and train control system in special operational situations or in case of disturbances. In contrast to regular operations for which the admissibility can be checked at any time by the route and train control system, safety critical operations are instructed by the operator while bypassing elements of the route and train control system (e.g. the radio block center or the interlocking system). I.e. safety critical operations are operator actions, e.g. safety critical route clearing, safety critical point change, etc. with which the operator can circumvent a safe setting of the system.

[0005] For controlling safety critical operations, high safety requirements have to be fulfilled. In some cases customers require not only a safety critical operation of a route and train control system, but also a safe state indication of the states of the route and train control system, e.g. in case of safety critical operations which bypass the interlocking system, such as "schriftlicher Befehl" and operation of a "Ersatzsignal". "Schriftlicher Befehl" is an order from the operator to bypass a route and train control system manually, which has to be given to the train staff or recorded in written form in case of e.g. an operational failure. "Ersatzsignal" is an additional signal, which replaces the order for passing a stop sign. By executing such safety critical operations, the operator can circumvent a safe setting of the system. The basis for decision of the operator whether to execute such a safety critical operation is the state of the route and train control system indicated at the display of the operator workstation. It is therefore an essential requirement that the state of the route and train control system is displayed correctly. According operator workstations, which fulfill the required safety integrity level (typically SIL2, sometimes even SIL4), have been developed [1], [2], [3].

[0006] Customers now require more and more the integration of additional non-safety related functionality or SIL0 functions in operator workstations [4]. Yet, this results in large efforts, because it must be ensured that the SIL0 components are non-intrusive ("ruckwirkungsfrei") to the SIL>0 environment of the operator workstation. This however results in high hardware costs for this dedicated computer and also in high costs for software development, integration and test, because all these components have to developed according a high safety integrity level (typically SIL4) according the standard EN 50128 [5].

[0007] Existing solutions provide only low flexibility and do not meet the customer's requirements. In particular customers request for a flexible operation web-based user interfaces. Users should have the possibility not only to operate the RTCS from central operator workstation but also from mobile devices. A web-based user interface is an adaptable solution that provides the necessary flexibility.

[0008] A method for secure transmission of data is disclosed in [2]. A method for verifying correct data transfer is disclosed in [3].

[0009] Document EP 3 040 862 A1 discloses a train traffic control system comprising: route and train control system, an operator workstation with a display, wherein the operator workstation comprises at least one basic integrity indication component, with safety level SIL0 for indicating information with a basic integrity on the display, wherein the operator workstation is adapted to generate graphical data of information with basic integrity, safe state indication component with safety level SIL>0 configured to transform state data concerning the state of elements of the route and train control system into graphical data and thereby generating indication data indicating safety-related information concerning the state of elements of the route and train control system on the display of the operator workstation, wherein the basic integrity indication component and the safe state indication component are software components, wherein the safe state indication component is functionally separated from the basic integrity indication component, safe channel connecting the safe state indication component and the display for safe transmission of safety-related information about the state of elements of the route train control system.

Object of the invention

[0010] It is an object of the invention to suggest a train traffic control system, which on the one hand realizes the

required high safety level for safe state indication and on the other hand allows considerable cost reduction and flexibility.

Description of the invention

[0011] This object is solved by a train traffic control system according to claim 1 and a method according to claim 9.

[0012] According to the invention, the operator workstation comprises at least one basic integrity indication component with safety level SIL0 for indicating information with a basic integrity on the display. An indication server is provided comprising a safe state indication component with safety level SIL>0, in particular SIL4, for indicating safety-related information concerning the state of elements of the route and train control system on the display of the operator workstation, wherein the safe state indication component is functionally independent of the operator workstation. Further, a safe channel is provided connecting the safe state indication server and the display for safe transmission of safety-related information about the state of elements of the route train control system.

[0013] The basic integrity indication components and the safe state indication component are software components, i.e. encapsulated building blocks of software.

[0014] The basic integrity indication component indicates any type of information with basic integrity, such as delay of a train or the weather conditions, of a train traffic control system on a display to inform an operator about the respective conditions of the train traffic control system, the controlled route and train control system and their elements with a safety-integrity-level SIL0. Elements of the route and train control system can be e.g. field elements (points, signals, track vacancy detection systems, level crossings, etc.), logical elements (routes, movement authorities, line block systems, etc.), train related elements (train parameters like speed or length of a train, etc.) or area related elements (zones for temporary speed restrictions, working areas of maintenance staff, responsibility areas of a specific operator etc.).

[0015] The safe state indication component generates graphical data (indication data) in order to indicate safety related states of the train traffic control system, the controlled route and train control system and their elements with a safety-integrity-level SIL>0, in particular SIL4 to inform an operator reliably about these states. Safety related operations can be executed based on these indications.

[0016] According to the invention, the basic integrity indication component is integrated in the operator workstation, whereas the safe state indication component is functionally independent of the operator workstation. In other words, the function for generating indication data of safety-related information concerning the state of elements of the route train control system (state data) is outsourced from the operator workstation, i.e. the safe state indication component is functionally separated from the basic integrity indication component and can (but doesn't have to) be installed in separate locations. Thus, non-intrusiveness of the SIL0 basic integrity indication components on the safe state indication component can be ensured more easily. Since the operator workstation comprises only low safety components the operator workstation can be designed with basic integrity (in particular SIL0), which is much cheaper compared to the high safety operator workstation known from the state of the art. Thus, the inventive traffic control system enables safe indication of states of elements of the route and train control system on the display of the operator workstation at low cost.

[0017] The transmission of safety-related information about the state of elements of the route train control system between the safe state indication component and the display is realized by providing a safe channel (communication channel between the indication server and the display) that transmits graphical indication data to the display and checksum information to the safe state indication component. The procedures to ensure safe communications via this channel are implemented according the relevant standards (e.g. EN 50159) and the required safety integrity level.

[0018] At the display of the operator workstation both, information with basic integrity as well as safety-related information, in particular safe state indication of the route and train control system is displayed to the operator.

[0019] According to the invention, the safe state indication component is integrated in the route and train control system, i.e. in a sub-center of the train traffic control system. No further computer is required in this case, which makes this embodiment cost effective. Yet, an additional function has to be integrated in all route and train control systems, which are to be controlled by the train traffic, control system.

[0020] The safe state indication component can be integrated in an indication server. The indication server can be part of the route and train control system. This is in particular advantageous in case no overall Control Centre exists and only one (small) route and train control system has to be controlled.

[0021] In an alternative embodiment, the system comprises a control center, wherein the indication server is integrated in the control center. This embodiment is advantageous in cases where existing route and train control system (for example from different suppliers) shall be controlled, since no further functions have to be integrated in the route and train control system. Control centers are known e.g. from DB "Betriebszentrale" or "Steuerzentrale" respectively and handle the tasks of controlling, securing and dispositioning of railway operations.

[0022] In a further alternative embodiment, the indication server is integrated in a remote computer center (remote from the display). This allows the usage of thin-

clients for the operator workstation (to reduce the amount of needed energy, noise and space in the control center). The remote computer center can be part of the control center.

[0023] Preferably, the indication server is procedure-protected, i.e. the necessary safety integrity level is achieved by a procedure that, on the one hand, integrates the human user (operator) and, on the other hand, is controlled by a component of the route and train control system. Common industrial computer can be used as indication server.

[0024] Alternatively, the indication server can be a composite fail-safety server. I.e. the indication server is a multi-channel server having a 2002 or 2003 architecture. Safety level SIL4 can be achieved with this embodiment.

[0025] Preferably, the operator workstation is integrated in a traffic management system. The traffic management system may comprise further functions for managing train operation, e.g. delay detection, detection of train occupancy conflicts, (automatic) conflict resolution, management of resources such as maintenance area staff along the route, integration of telecommunications and video surveillance. By integrating the operator workstation in a traffic management system, only one set of input devices (mouse, keyboard etc.) is required for controlling the train traffic. So one operator is able to manage the top-level train operation as well as perform the safety critical operations that require the safe indication.

[0026] In a highly preferred embodiment, the safe channel is routed through the operator workstation. In this case, no further computer is required for transmission of the safety-related information. While, according to the state of the art, state data are transmitted and processed in the workstation leading to an overall safety integrity SIL>0 for the workstation itself, the present invention uses the workstation only as a "grey channel" which is secured by a procedure leading to no additional safety integrity needs for the workstation itself. This reduces the development costs.

[0027] In a highly preferred embodiment the safe state indication component is adapted to calculate a first checksum of the indication data generated by the safe state indication component and is further adapted to carry out a checksum comparison and/or a pixel comparison of pixmap data.

[0028] The safe state indication component is preferably adapted to download a read back component from a browser of the operator workstation.

[0029] The invention also concerns a method for safe displaying safety-related information concerning the state indication of a route and train control system at an operator workstation of a train traffic control system as described above, having the steps of claim 9.

[0030] Safety-related information is transmitted from the route and train control system to the indication server. The indication server generates graphical data (indication data) from the safety-related information, which are then sent to the display of the operator workstation via the safe channel.

[0031] Graphical data of information with basic integrity however are generated within the operator workstation. The graphical data of information with basic integrity are then transmitted within the operator workstation to the display.

[0032] In a highly preferred variant, the safe channel is routed through operator workstation. In this case, the safe channel is at least partially part of the operator workstation.

[0033] Preferably, the state data is transformed to pixmap indication data and the pixmap indication data are transmitted to the display by using a method for verifying correct transfer of pixmap data. The method for verifying correct transfer of pixmap data preferably comprises:

a) modifying at least one property of a fixed number of pixels selected from the pixmap indication data in a first memory, the selection being performed in a random way,

b) transferring the pixmap indication data comprising the modified pixels from the first memory to a second memory,

c) reading back the modified pixels from the second memory, and

d) comparing the read-back modified pixels to the modified pixels of the first memory for verifying the correct transfer of the pixmap indication data, wherein the at least one property is modified in such a way that the modification is not observable when displaying the modified pixels on the graphical display. An according method is described in [3].

[0034] In a highly preferred variant the indication data generated by the safe state component is displayed in a web-browser of the operator workstation to provide the necessary flexibility.

[0035] In order to verify that the visualization of the indication data in the browser is indeed what was intended to be displayed, a preferred variant provides that the displayed indication data are read back, in particular by generating pixmap data.

[0036] In a highly preferred variant the safe state indication component generates a first checksum of the indication data, the browser generates a second checksum of the read back data and transmits the second checksum to the safe state indication component via the safe channel, and the safe state indication component compares the first checksum and the second checksum. Thus, it can be checked whether the transmission of the indication data to the browser and the displaying of the transmitted indication data has been correct. According to this embodiment the checksum comparison is

carried out remote from the operator workstation to separate the safety related comparison from the SIL0 operator workstation.

[0037] Alternatively or in addition the browser transmits the read back data to the safe state indication component via the safe channel and the safe state indication component compares the read back data with the indication data (pixel comparison).

[0038] To avoid a false-positive error comparison, algorithms that check only a few pixels (e.g. according to [3]) or morphological comparison algorithms (e.g. according to [6]) are used.

[0039] The present invention realizes a procedure based safe graphical indication of a route and train control system state in a SIL0 traffic management system. Thus, safety related route and train control systems, e.g. interlockings, signaling systems can be controlled from SIL0 traffic management systems.

[0040] The inventive traffic control system enables execution of safety critical operations in a safety critical system with reduced cost, in particular the execution of safety critical operations which require a safe display of the state of the route and train control system, e.g. because the route and train control system is bypassed by executing the respective safety critical operation.

[0041] Further advantages can be extracted from the description and the enclosed drawing. The embodiments mentioned are not to be understood as exhaustive enumeration but rather have exemplary character for the description of the invention.

Drawings

[0042] The invention is shown in the drawing.

Fig. 1 shows the architecture of a traffic control system according to the state of the art.

Fig. 2 shows the architecture of a traffic control system which does not belong to the invention with an indication server integrated in a control center.

Fig. 3 shows the architecture of a traffic control system according to the invention with an indication server integrated in the route and train control system.

Fig. 4 shows the architecture of a traffic control system according to the invention, wherein a safe state indication component is integrated in the route and train control system without indication server.

Fig. 5 shows the architecture of a traffic control system which does not belong to the invention with an indication server integrated in a remote computer center.

Fig. 6 shows the architecture of a traffic control system which does not belong to the invention with a safe state integration component adapted to reveal error in transmission and/or display of the indication data and a web-based operator workstation.

[0043] **Fig. 1** shows an architecture of a traffic control system according to the state of the art. The traffic control system comprises a route and train control system **RTCS** and an operator workstation **OW'** with a display **D.** The operator workstation OW' comprises basic integrity indication components **BIC** with safety level SIL0 for indicating information on the display D with a basic integrity (railway traffic management data). The operator workstation OW' further comprises a safe state indication component **SSC** with safety level SIL>0 for processing state data (safety relevant information concerning states of elements of the route and train control system RTCS). The state data are transmitted from the route and train control system RTCS to the safe state indication component SSC of the operator workstation OW'. The safe state indication component SSC transforms the state data into graphical data and thus generates indication data, which is then displayed at the display D.

[0044] According to the invention, the traffic control system comprises an operator workstation **OW** which does not involve any components with safety level SIL>0, i.e. operator workstation only comprises components with safety level SIL0 or less, such as the basic integrity indication components BIC. Since the safe state indication component SSC is swapped out of the operator workstation OW and is functionally independent of the operator workstation OW, i.e. implemented in a different way, non-intrusiveness of the SIL=0 operator workstation to the SIL>0 safe state indication component SSC can be ensured.

[0045] Information with basic integrity is transmitted from the route and train control system RTCS to the operator workstation OW via channel C1. Safety relevant information (state data) however is transmitted to the safe state indication component SSC via a separate channel C2 in order to generate according graphical indication data. The transmission channel C2 is a secured channel, e.g. secured by means of a security gateway in order to avoid manipulation of the state data. The indication data is transferred from the safe state indication component SSC to the display D of the operator workstation. In order to avoid falsification of indication data due to malfunction of hardware or software, the data transfer is carried out via a safe channel **C3**.

[0046] The safe state indication component SSC can either be executed by an indication server **IS** as shown in Fig. 2, Fig. 3 and Fig. 5 (i.e. an additional computer is provided for executing the safe state indication component SSC) or by a secured partition of an already existing computer of the traffic control system, as shown in **Fig. 4.**

[0047] In anembodiment not belonging to the present invention, shown in **Fig. 2**, the safe state indication component SSC is integrated in a control center **CC**

together with the operator workstation OW. Non-intrusiveness between operator workstation OW and safe state indication component SSC is ensured by providing a separate computer (indication server IS) for executing the safe state indication component SSC.

[0048] Instead of integrating the safe state indication component SSC in the control center CC it is also possible to integrate the safe state indication component SSC in the route and train control system RTCS, either executable by the indication server **(Fig. 3)** or by an existing computer of the RTCS itself **(Fig. 4).** If several route and train control systems RTCS are operated by the traffic control system, each of the route and train control systems RTCS has to be equipped with an according safe state indication component SCC.

[0049] In an example, not belonging to the present invention, which is shown in **Fig. 5,** the indication server IS with the safe state indication component SSC is integrated in a computer center **RZ,** which can be located remote from the operator workstation OW.

[0050] **Fig. 6** shows the architecture of a traffic control system not belonging to the present invention using a web-based operator workstation. The operator workstation comprises a browser B and a read back component R. The safe state indication component SSC is adapted to download the read back component R from the operator workstation OW. By executing the read back component R the displayed indication data are read back (read back data) and transmitted to the safe state indication component SSC.

[0051] The steps below describe the realization of a highly preferred variant of the inventive method by means of the traffic control system shown in Fig. 6. The according method steps are preferably executed anytime the operator uses the browser to execute safety critical commands. The safety critical commands might also be executed explicitly on demand through a dedicated user interaction mechanism (button, drop down button etc.). The preferred method steps are as follows:

1. The safe state indication component has the functionality to convert the state data into graphical indication data. The safe state indication component sends this indication data via the safe channel to the browser of the operator workstation. The browser displays this indication data on the display. The displayed data are read back and the browser calculates a first checksum of the read back data.

2. The read back data (pixmap data) along with the first checksum is sent to the safe state indication component through the safe channel.

3. The safe state indication component then compares the first checksum generated by the browser with a second checksum calculated by the safe state indication component. The second checksum is the checksum of the indications data generated by the safe state indication component. Thereby, it is verified that the indication data sent to the browser and the resulting read back pixmap data sent from the browser through the safe channel were not corrupted in anyway *en route.*

4. The safe state indication component then does checksum comparison and (if applicable, in particular if the chesum comparison is successful) a pixel comparison between the read back data sent by the browser and the indication data the safe state indication component itself generated based on the state data. If the comparison is successful it sends a success notification to the operator workstation via the safe channel. If it is not, it will send a failure notification.

5. Based on the reply of the safe state indication component, the critical command that was initiated by the operator will be either continued or terminated.

[0052] The inventive solution is based on the idea of outsourcing the SIL>0 safe state indication component SSC from the operator workstation OW and to set-up a safe channel C3 (e.g. by applying remote desktop protocols) enhanced with safety measures, in particular according to EN50159. This safe channel C3 is preferably routed through the operator workstation OW wherein a method for verifying correct data transfer is used. Thus, the invention realizes safe graphical indication of states of elements of the railway control system (e.g. interlocking, RBC,...) in an operator workstation OW, in particular within a traffic management system TMS that provides (only) a SIL0 environment.

Cited Documents

[0053]

[1] EP 0 443 377 A2 (Lorenz)
[2] EP 2 683 589 B1 (Siemens)
[3] EP 2 244 188 A1 (Thales)
[4] Antweiler: "Bahn-Betriebsleitsystem ILTIS" Signal & Draht , 87 (1995) 10, Seiten 337 - 340
[5] EN 50128 "Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme" Ausgabe: 2012-03
[6] Mantere, Timo: "Electronic Imaging & Signal Processing - Image comparison based on morphological transforms" 29 November 2007, SPIE Newsroom. DOI: 10.1117/2.1200711.0926

List of Reference Signs

[0054]

BIC basic integrity indication component

C1	transmission channel for information with basic integrity
C2	transmission channel for safety relevant information (state data)
C3	safe transmission channel for graphical indication data
CC	control center
D	display
IS	indication server
OW	operator workstation
RTCS	route and train control system
RZ	computer center
SSC	safe state indication component
TMS	traffic management system

Claims

1. Train traffic control system comprising

a route and train control system (RTCS),
an operator workstation (OW) with a display (D), wherein the operator workstation (OW) comprises at least one basic integrity indication component (BIC) with safety level SILO for indicating information with a basic integrity on the display (D), wherein the operator workstation is adapted to generate graphical data of information with basic integrity, and wherein the operator workstation (OW) comprises only components with safety level SILO or less, and
a safe state indication component (SSC) with safety level SIL>0, in particular SIL4, configured to transform state data concerning the state of elements of the route and train control system (RTCS) into graphical data and thereby generating indication data indicating safety-related information concerning the state of elements of the route and train control system (RTCS) on the display of the operator workstation (OW), wherein the basic integrity indication component and the safe state indication component are software components, i.e. encapsulated building blocks of software,
wherein a channel (C1) connecting the route and train control system (RTCS) and the operator workstation (OW) is provided for transmitting information with basic integrity from the route and train control system (RTCS) to the operator workstation (OW),
wherein the safe state indication component (SSC) is functionally independent of the operator workstation (OW), and the safe state indication component (SSC) is functionally separated from the basic integrity indication component (BIC), wherein the function for generating indication data of safety-related information concerning the state of elements of the route train control system is outsourced from the operator workstation, and
in addition to the channel (C1), a safe channel (C3) connecting the safe state indication component (SSC) and the display (D) for safe transmission of safety-related information about the state of elements of the route train control system (RTCS),
wherein the safe state indication component (SSC) is integrated in the route and train control system (RTCS).

2. Train traffic control system according to claim 1 **characterized in that** the safe state indication component (SSC) is integrated in an indication server (IS).

3. Train traffic control system according to claim 2 **characterized in that** the system comprises a control center (CC), wherein the indication server (IS) is integrated in the control center.

4. Train traffic control system according to claim 2 or 3 **characterized in that** the indication server (IS) is integrated in a remote computer center (RZ).

5. Train traffic control system according to any one of the claims 2 through 4, **characterized in that** the indication server (IS) is procedure-protected.

6. Train traffic control system according to any one of the claims 2 through 4, **characterized in that** the indication server (IS) is a composite fail-safety server.

7. Train traffic control system according to one of the preceding claims, **characterized in that** the operator workstation (OW) is integrated in a traffic management system (TMS).

8. Train traffic control system according to one of the preceding claims, **characterized in that** the safe channel (C3) is routed through the operator workstation (OW).

9. Method for safe displaying safety-related information concerning the state of a route and train control system (RTCS) at an operator workstation (OW) of a train traffic control system comprising a route and train control system (RTCS), an operator workstation (OW) with a display (D), wherein the operator workstation (OW) comprises at least one basic integrity indication component (BIC) with safety level SILO for indicating information with a basic integrity on the display (D), wherein the operator workstation is adapted to generate graphical data of information with basic integrity; and wherein the operator workstation (OW) comprises only components with safety level SILO or less, and a safe state indication com-

ponent (SSC) with safety level SIL>0, in particular SIL4, for transforming state data concerning the state of elements of the route and train control system (RTCS) into graphical data and thereby generating indication data indicating safety-related information concerning the state of elements of the route and train control system (RTCS) on the display of the operator workstation (OW), wherein the basic integrity indication component and the safe state indication component are software components, i.e. encapsulated building blocks of software, wherein a channel (C1) connecting the route and train control system (RTCS) and the operator workstation (OW) is provided for transmitting information with basic integrity from the route and train control system (RTCS) to the operator workstation (OW), wherein the safe state indication component (SSC) is functionally independent of the operator workstation (OW), and the safe state indication component (SSC) is functionally separated from the basic integrity indication component (BIC), wherein the function for generating indication data of safety-related information concerning the state of elements of the route train control system is outsourced from the operator workstation; the train traffic control system further comprising an additional safe channel (C3) connecting the safe state indication component (SSC) and the display (D) for safe transmission of safety-related information about the state of elements of the route train control system (RTCS), wherein the safe state indication component (SSC) is integrated in the route and train control system (RTCS).

the method comprising
generation of graphical data of information with basic integrity within the operator workstation,
transformation of state data comprising the safety relevant information into graphical indication data within the safe state indication component (SSC) with safety level SIL>0 which is functionally independent from the basic integrity indication components (BIC) with safety level SILO of the operator workstation (OW), and
transmission of the indication data to a display (D) via the safe channel (C3).

10. Method according to claim 9, **characterized in that** the safe channel is routed through the operator workstation (OW).

11. Method according to claim 9 or 10, **characterized in that** indication data are pixmap data and wherein the indication data are transmitted to the display (D) by using a method for verifying correct transfer of pixmap data.

12. Method according to any one of the claims 9 through 11, **characterized in that** indication data are displayed in a web browser of the operator workstation.

13. Method according to claim 12, **characterized in that** the displayed indication data are read back.

14. Method according to claim 13, **characterized in**

that the safe state indication component generates a first checksum of the indication data;
that the browser generates a second checksum of the read back data and transmits the second checksum to the safe state indication component via the safe channel; and
that the safe state indication component compares the first checksum and the second checksum.

15. Method according to claim 13 or 14, **characterized in**

that the browser transmits the read back data to the safe state indication component via the safe channel; and
that the safe state indication component compares the read back data with the indication data.

Patentansprüche

1. Zugverkehrsteuerungssystem umfassend:

ein Strecken- und Zugsteuerungssystem (RTCS),
einen Bedienerarbeitsplatz (OW) mit einer Anzeige (D), wobei der Bedienerarbeitsplatz (OW) mindestens eine Komponente zur Anzeige mit Basisintegrität (BIC) mit Sicherheitsniveau SILO aufweist zum Anzeigen von Informationen mit einer Basisintegrität auf der Anzeige (D), wobei der Bedienerarbeitsplatz dazu eingerichtet ist, grafische Informationsdaten mit Basisintegrität zu erzeugen, und wobei der Bedienerarbeitsplatz (OW) nur Komponenten mit dem Sicherheitsniveau SIL0 oder weniger aufweist, und
eine Komponente zur Anzeige eines sicheren Zustands (SSC) mit Sicherheitsniveau SIL>0, insbesondere SIL4, die dazu eingerichtet ist, Zustandsdaten über den Zustand von Elementen des Strecken- und Zugsteuerungssystems (RTCS) in grafische Daten umzuwandeln und dadurch Anzeigedaten zu erzeugen, die sicherheitsrelevante Informationen über den Zustand von Elementen des Strecken- und Zugsteuerungssystems (RTCS) auf der Anzeige des Bedienerarbeitsplatzes (OW) anzeigen,
wobei die Komponente zur Anzeige mit Basisin-

tegrität und die Komponente zur Anzeige eines sicheren Zustands Softwarekomponenten sind, d.h. gekapselte Software-Bausteine,
wobei ein Kanal (C1), der das Strecken- und Zugsteuerungssystem (RTCS) und den Bedienerarbeitsplatz (OW) verbindet, zur Übertragung von Informationen mit Basisintegrität von dem Strecken- und Zugsteuerungssystem (RTCS) an den Bedienerarbeitsplatz (OW) vorgesehen ist,
wobei die Komponente zur Anzeige eines sicheren Zustands (SSC) von dem Bedienerarbeitsplatz (OW) funktional unabhängig ist und die Komponente zur Anzeige eines sicheren Zustands (SSC) von der Komponente zur Anzeige mit Basisintegrität (BIC) funktional getrennt ist, wobei die Funktion zur Erzeugung von Anzeigedaten sicherheitsrelevanter Informationen über den Zustand von Elementen des Streckenzugsteuerungssystems aus dem Bedienerarbeitsplatz ausgelagert ist, und
zusätzlich zu dem Kanal (C1), einen sicheren Kanal (C3), der die Komponente zur Anzeige eines sicheren Zustands (SSC) und die Anzeige (D) zur sicheren Übertragung sicherheitsrelevanter Informationen über den Zustand von Elementen des Streckenzugsteuerungssystems (RTCS) verbindet,
wobei die Komponente zur Anzeige eines sicheren Zustands (SSC) in das Strecken- und Zugsteuerungssystem (RTCS) integriert ist.

2. Zugverkehrsteuerungssystem nach Anspruch 1, **dadurch gekennzeichnet, dass** die Komponente zur Anzeige eines sicheren Zustands (SSC) in einen Anzeigeserver (IS) integriert ist.

3. Zugverkehrsteuerungssystem nach Anspruch 2, **dadurch gekennzeichnet, dass** das System eine Steuerzentrale (CC) umfasst, wobei der Anzeigeserver (IS) in die Steuerzentrale integriert ist.

4. Zugverkehrsteuerungssystem nach Anspruch 2 oder 3, **dadurch gekennzeichnet, dass** der Anzeigeserver (IS) in ein entferntes Rechenzentrum (RZ) integriert ist.

5. Zugverkehrsteuerungssystem nach einem der Ansprüche 2 bis 4, **dadurch gekennzeichnet, dass** der Anzeigeserver (IS) verfahrensgesichert ist.

6. Zugverkehrsteuerungssystem nach einem der Ansprüche 2 bis 4, **dadurch gekennzeichnet, dass** der Anzeigeserver (IS) ein Komposit-Server mit Ausfallsicherung ist.

7. Zugverkehrsteuerungssystem nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der Bedienerarbeitsplatz (OW) in ein Verkehrsmanagementsystem (TMS) integriert ist.

8. Zugverkehrsteuerungssystem nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der sichere Kanal (C3) über den Bedienerarbeitsplatz (OW) geleitet wird.

9. Verfahren zur sicheren Anzeige von sicherheitsrelevanten Informationen über den Zustand eines Strecken- und Zugsteuerungssystems (RTCS) an einem Bedienerarbeitsplatz (OW) eines Zugverkehrsteuerungssystems mit

einem Strecken- und Zugsteuerungssystem (RTCS),
einem Bedienerarbeitsplatz (OW) mit einer Anzeige (D), wobei der Bedienerarbeitsplatz (OW) mindestens eine Komponente zur Anzeige mit Basisintegrität (BIC) mit dem Sicherheitsniveau SILO zur Anzeige von Informationen mit einer Basisintegrität auf der Anzeige (D) aufweist, wobei der Bedienerarbeitsplatz dazu ausgebildet ist, grafische Daten von Informationen mit Basisintegrität zu erzeugen; und wobei der Bedienerarbeitsplatz (OW) nur Komponenten mit Sicherheitsniveau SILO oder weniger aufweist, und
einer Komponente zur Anzeige eines sicheren Zustands (SSC) mit Sicherheitsniveau SIL>0, insbesondere SIL4, zur Umwandlung von Zustandsdaten über den Zustand von Elementen des Strecken- und Zugsteuerungssystems (RTCS) in grafische Daten und dadurch zur Erzeugung von Anzeigedaten, die sicherheitsrelevante Informationen über den Zustand von Elementen des Strecken- und Zugsteuerungssystems (RTCS) auf der Anzeige des Bedienerarbeitsplatzes (OW) anzeigen, wobei die Komponente zur Anzeige mit Basisintegrität und die Komponente zur Anzeige eines sicheren Zustands Softwarekomponenten sind, d.h. gekapselte Software-Bausteine, wobei ein Kanal (C1), der das Strecken- und Zugsteuerungssystem (RTCS) und den Bedienerarbeitsplatz (OW) verbindet, zur Übertragung von Informationen mit Basisintegrität von dem Strecken- und Zugsteuerungssystem (RTCS) an den Bedienerarbeitsplatz (OW) vorgesehen ist,
wobei die Komponente zur Anzeige eines sicheren Zustands (SSC) funktional unabhängig von dem Bedienerarbeitsplatz (OW) ist, und die Komponente zur Anzeige eines sicheren Zustands (SSC) von der Komponente zur Anzeige mit Basisintegrität (BIC) funktional getrennt ist, wobei die Funktion zum Erzeugen von Anzeigedaten sicherheitsrelevanter Informationen über den Zustand von Elementen des Strecken-

zugsteuerungssystems vom Bedienerarbeitsplatz ausgelagert ist; wobei das Zugverkehrsteuerungssystem ferner einen zusätzlichen sicheren Kanal (C3) aufweist, der die Komponente zur Anzeige eines sicheren Zustands (SSC) und die Anzeige (D) zur sicheren Übertragung von sicherheitsrelevanten Informationen über den Zustand von Elementen des Streckenzugsteuerungssystems (RTCS) verbindet, wobei die Komponente zur Anzeige eines sicheren Zustands (SSC) in das Strecken- und Zugsteuerungssystem (RTCS) integriert ist,
wobei das Verfahren umfasst:

Erzeugung von grafischen Daten von Informationen mit Basisintegrität innerhalb des Bedienerarbeitsplatzes,
Umwandlung von Zustandsdaten, die die sicherheitsrelevanten Informationen enthalten, in grafische Anzeigedaten innerhalb der Komponente zur Anzeige eines sicheren Zustands (SSC) mit Sicherheitsniveau SIL>0, die funktional unabhängig ist von den Komponenten zur Anzeige mit Basisintegrität (BIC) mit Sicherheitsniveau SILO des Bedienerarbeitsplatzes (OW), und
Übertragung der Anzeigedaten an eine Anzeige (D) über den sicheren Kanal (C3).

10. Verfahren nach Anspruch 9, **dadurch gekennzeichnet, dass** der sichere Kanal über den Bedienerarbeitsplatz (OW) geleitet wird.

11. Verfahren nach Anspruch 9 oder 10, **dadurch gekennzeichnet, dass** die Anzeigedaten Pixmap-Daten sind und wobei die Anzeigedaten unter Verwendung eines Verfahrens zur Überprüfung der korrekten Übertragung von Pixmap-Daten an die Anzeige (D) übertragen werden.

12. Verfahren nach einem der Ansprüche 9 bis 11, **dadurch gekennzeichnet, dass** die Anzeigedaten in einem Webbrowser des Bedienerarbeitsplatzes angezeigt werden.

13. Verfahren nach Anspruch 12, **dadurch gekennzeichnet, dass** die angezeigten Anzeigedaten zurückgelesen werden.

14. Verfahren nach Anspruch 13, **dadurch gekennzeichnet,**

dass die Komponente zur Anzeige eines sicheren Zustands eine erste Prüfsumme der Anzeigedaten erzeugt;
dass der Browser eine zweite Prüfsumme der zurückgelesenen Daten erzeugt und die zweite Prüfsumme über den sicheren Kanal an die Komponente zur Anzeige eines sicheren Zustands überträgt; und
dass die Komponente zur Anzeige eines sicheren Zustands die erste Prüfsumme und die zweite Prüfsumme vergleicht.

15. Verfahren nach Anspruch 13 oder 14, **dadurch gekennzeichnet**

dass der Browser die zurückgelesenen Daten über den sicheren Kanal an die Komponente zur Anzeige eines sicheren Zustands sendet; und
dass die Komponente zur Anzeige eines sicheren Zustands die zurückgelesenen Daten mit den Anzeigedaten vergleicht.

Revendications

1. Système de contrôle de trafic ferroviaire comprenant :

un système de contrôle des itinéraires et des trains (RTCS) ;
un poste de travail d'opérateur (OW) qui est muni d'un affichage (D), dans lequel le poste de travail d'opérateur (OW) comprend au moins un composant d'indication d'intégrité de base (BIC) qui présente un niveau de sécurité SILO pour indiquer une information avec une intégrité de base sur l'affichage (D), dans lequel le poste de travail d'opérateur est adapté pour générer des données graphiques d'information avec intégrité de base, et dans lequel le poste de travail d'opérateur (OW) comprend seulement des composants qui présentent le niveau de sécurité SILO ou moins ; et
un composant d'indication d'état de sécurité (SSC) qui présente un niveau de sécurité SIL > 0, en particulier SIL4, lequel composant est configuré pour transformer des données d'état qui concernent l'état d'éléments du système de contrôle des itinéraires et des trains (RTCS) selon des données graphiques et par voie de conséquence, pour générer des données d'indication qui indiquent une information rapportée à la sécurité qui concerne l'état d'éléments du système de contrôle des itinéraires et des trains (RTCS) sur l'affichage du poste de travail d'opérateur (OW) ;
dans lequel le composant d'indication d'intégrité de base et le composant d'indication d'état de sécurité sont des composants logiciels, c'est-à-dire des blocs de construction encapsulés de logiciel,
dans lequel un canal (C1) qui connecte le système de contrôle des itinéraires et des trains (RTCS) et le poste de travail d'opérateur (OW)

est prévu pour transmettre l'information avec intégrité de base depuis le système de contrôle des itinéraires et des trains (RTCS) jusqu'au poste de travail d'opérateur (OW),
dans lequel le composant d'indication d'état de sécurité (SSC) est fonctionnellement indépendant du poste de travail d'opérateur (OW), et le composant d'indication d'état de sécurité (SSC) est fonctionnellement séparé du composant d'indication d'intégrité de base (BIC), dans lequel la fonction pour générer des données d'indication de l'information rapportée à la sécurité qui concerne l'état d'éléments du système de contrôle des itinéraires et des trains est extraite en termes de ressource externalisée au niveau du poste de travail d'opérateur ; et
en plus du canal (C1), un canal de sécurité (C3) qui connecte le composant d'indication d'état de sécurité (SSC) et l'affichage (D) pour une transmission en termes de sécurité de l'information rapportée à la sécurité qui concerne l'état d'éléments du système de contrôle des itinéraires et des trains (RTCS),
dans lequel le composant d'indication d'état de sécurité (SSC) est intégré dans le système de contrôle des itinéraires et des trains (RTCS).

2. Système de contrôle de trafic ferroviaire selon la revendication 1, **caractérisé en ce que** le composant d'indication d'état de sécurité (SSC) est intégré dans un serveur d'indication (IS).

3. Système de contrôle de trafic ferroviaire selon la revendication 2, **caractérisé en ce que** le système comprend un centre de commande (CC), dans lequel le serveur d'indication (IS) est intégré dans le centre de commande.

4. Système de contrôle de trafic ferroviaire selon la revendication 2 ou 3, **caractérisé en ce que** le serveur d'indication (IS) est intégré dans un centre informatique à distance (RZ).

5. Système de contrôle de trafic ferroviaire selon l'une quelconque des revendications 2 à 4, **caractérisé en ce que** le serveur d'indication (IS) est protégée en termes de procédure(s).

6. Système de contrôle de trafic ferroviaire selon l'une quelconque des revendications 2 à 4, **caractérisé en ce que** le serveur d'indication (IS) est un serveur composite défaillance - sécurité.

7. Système de contrôle de trafic ferroviaire selon l'une quelconque des revendications précédentes, **caractérisé en ce que** le poste de travail d'opérateur (OW) est intégré dans un système de gestion de trafic (TMS).

8. Système de contrôle de trafic ferroviaire selon l'une quelconque des revendications précédentes, **caractérisé en ce que** le canal de sécurité (C3) est routé par l'intermédiaire du poste de travail d'opérateur (OW).

9. Procédé pour l'affichage en termes de sécurité d'une information rapportée à la sécurité qui concerne l'état d'un système de contrôle des itinéraires et des trains (RTCS) au niveau d'un poste de travail d'opérateur (OW) d'un système de contrôle de trafic ferroviaire qui comprend un système de contrôle des itinéraires et des trains (RTCS), un poste de travail d'opérateur (OW) qui est muni d'un affichage (D), dans lequel le poste de travail d'opérateur (OW) comprend au moins un composant d'indication d'intégrité de base (BIC) qui présente un niveau de sécurité SILO pour indiquer une information avec une intégrité de base sur l'affichage (D), dans lequel le poste de travail d'opérateur est adapté pour générer des données graphiques d'information avec intégrité de base ; et dans lequel le poste de travail d'opérateur (OW) comprend seulement des composants qui présentent un niveau de sécurité SILO ou moins, et un composant d'indication d'état de sécurité (SSC) qui présente un niveau de sécurité SIL > 0, en particulier SIL4, pour transformer des données d'état qui concernent l'état d'éléments du système de contrôle des itinéraires et des trains (RTCS) selon des données graphiques et par voie de conséquence, pour générer des données d'indication qui indiquent une information rapportée à la sécurité qui concerne l'état d'éléments du système de contrôle des itinéraires et des trains (RTCS) sur l'affichage du poste de travail d'opérateur (OW), dans lequel le composant d'indication d'intégrité de base et le composant d'indication d'état de sécurité sont des composants logiciels, c'est-à-dire des blocs de construction encapsulés de logiciel, dans lequel un canal (C1) qui connecte le système de contrôle des itinéraires et des trains (RTCS) et le poste de travail d'opérateur (OW) est prévu pour transmettre l'information avec intégrité de base depuis le système de contrôle des itinéraires et des trains (RTCS) jusqu'au poste de travail d'opérateur (OW), dans lequel le composant d'indication d'état de sécurité (SSC) est fonctionnellement indépendant du poste de travail d'opérateur (OW), et le composant d'indication d'état de sécurité (SSC) est fonctionnellement séparé du composant d'indication d'intégrité de base (BIC), dans lequel la fonction pour générer des données d'indication de l'information rapportée à la sécurité qui concerne l'état d'éléments du système de contrôle des itinéraires et des trains est extraite en termes de ressource externalisée au niveau du poste de travail d'opérateur ; le système de contrôle de trafic ferroviaire comprenant en outre un canal de sécurité additionnel (C3) qui connecte le composant

d'indication d'état de sécurité (SSC) et l'affichage (D) pour une transmission en termes de sécurité de l'information rapportée à la sécurité qui concerne l'état d'éléments du système de contrôle des itinéraires et des trains (RTCS), dans lequel le composant d'indication d'état de sécurité (SSC) est intégré dans le système de contrôle des itinéraires et des trains (RTCS),
le procédé comprenant :

la génération de données graphiques d'information avec intégrité de base à l'intérieur du poste de travail d'opérateur ;
la transformation de données d'état qui comprennent l'information rapportée à la sécurité selon des données d'indication graphiques à l'intérieur du composant d'indication d'état de sécurité (SSC) qui présente le niveau de sécurité SIL > 0, lequel composant est fonctionnellement indépendant des composants d'indication d'intégrité de base (BIC) qui présentent le niveau de sécurité SILO du poste de travail d'opérateur (OW) ; et
la transmission des données d'indication graphiques à un affichage (D) via le canal de sécurité (C3).

10. Procédé selon la revendication 9, **caractérisé en ce que** le canal de sécurité est routé par l'intermédiaire du poste de travail d'opérateur (OW).

11. Procédé selon la revendication 9 ou 10, **caractérisé en ce que** les données d'indication sont des données de pixmap/données de table de pixels et dans lequel les données d'indication sont transmises à l'affichage (D) en utilisant un procédé pour vérifier que le transfert des données de pixmap/données de table de pixels est correct.

12. Procédé selon l'une quelconque des revendications 9 à 11, **caractérisé en ce que** les données d'indication sont affichées au sein d'un navigateur Web du poste de travail d'opérateur.

13. Procédé selon la revendication 12, **caractérisé en ce que** les données d'indication affichées sont soumises à une relecture.

14. Procédé selon la revendication 13, **caractérisé en ce que** :

le composant d'indication d'état de sécurité génère un premier total de contrôle des données d'indication ; **en ce que** :
le navigateur Web génère un second total de contrôle des données soumises à une relecture et transmet le second total de contrôle au composant d'indication d'état de sécurité via le canal de sécurité ; et **en ce que** :
le composant d'indication d'état de sécurité compare le premier total de contrôle et le second total de contrôle.

15. Procédé selon la revendication 13 ou 14, **caractérisé en ce que** :
le navigateur Web transmet les données soumises à une relecture au composant d'indication d'état de sécurité via le canal de sécurité ; et **en ce que** :
le composant d'indication d'état de sécurité compare les données soumises à une relecture avec les données d'indication.

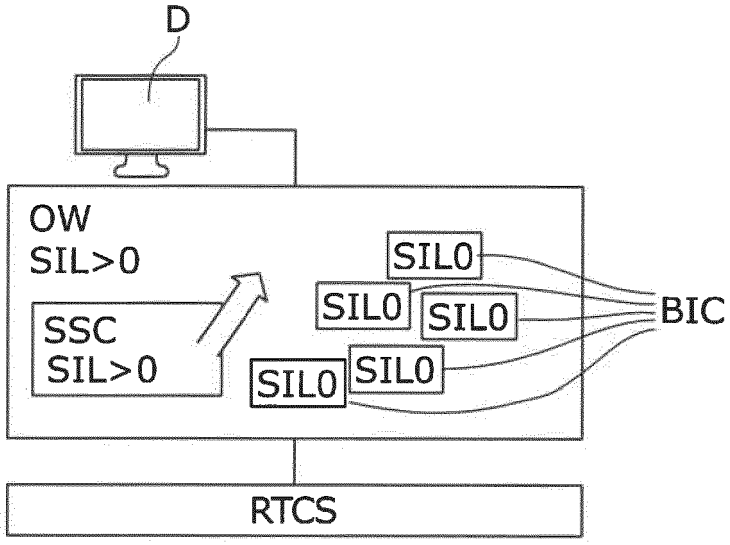
D
OW
SIL>0
SSC
SIL>0
SIL0
SIL0
SIL0
SIL0
SIL0
BIC
RTCS

Fig. 1

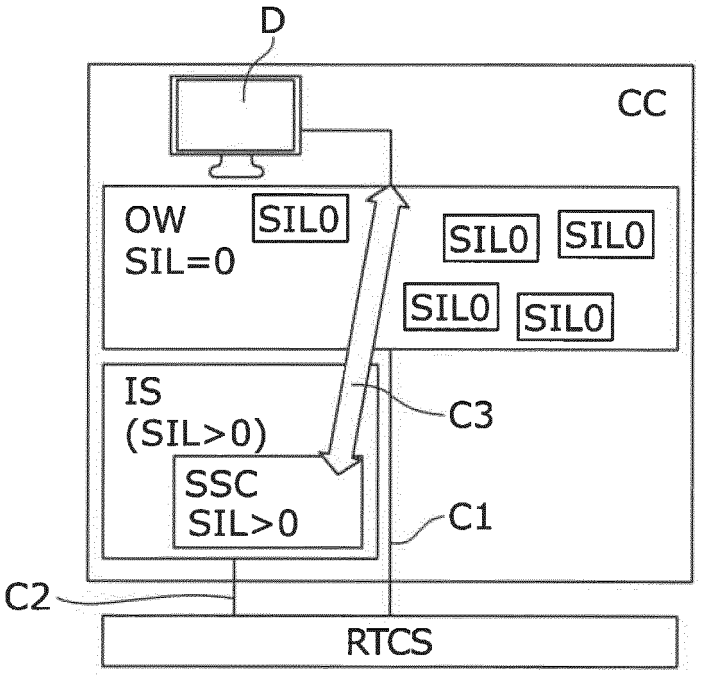
D
CC
OW
SIL=0
SIL0
SIL0
SIL0
SIL0
SIL0
IS
(SIL>0)
SSC
SIL>0
C3
C1
C2
RTCS

Fig. 2

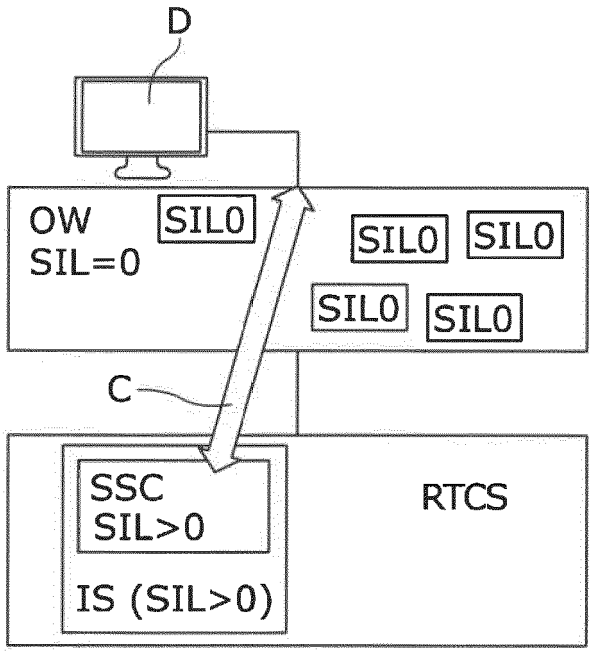
D
OW
SIL=0
SIL0
SIL0
SIL0
SIL0
SIL0
C
SSC
SIL>0
IS (SIL>0)
RTCS

Fig. 3

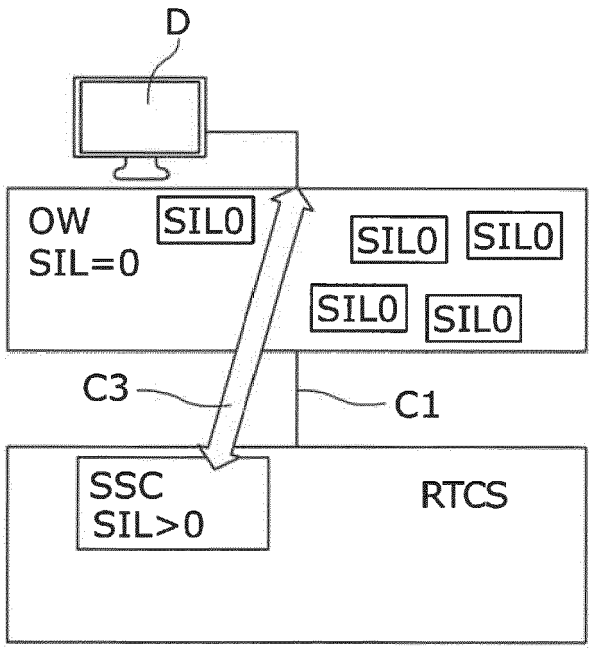
D
OW
SIL=0
SIL0
SIL0
SIL0
SIL0
SIL0
C3
C1
SSC
SIL>0
RTCS

Fig. 4

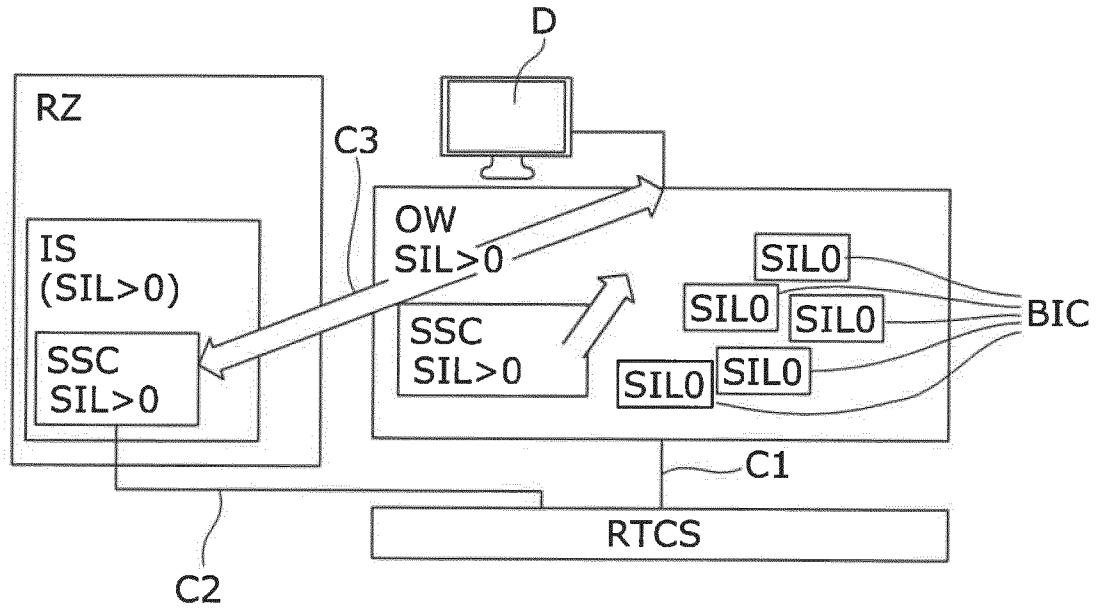
D
RZ
C3
IS
(SIL>0)
SSC
SIL>0
OW
SIL>0
SSC
SIL>0
SIL0
SIL0
SIL0
SIL0
SIL0
BIC
C1
RTCS
C2

Fig. 5

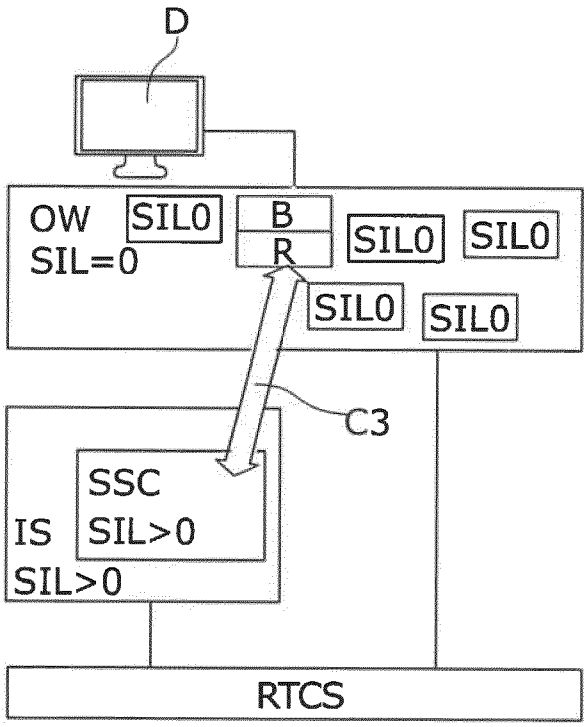
D
OW
SIL=0
SIL0
B
R
SIL0
SIL0
SIL0
SIL0
C3
SSC
SIL>0
IS
SIL>0
RTCS

Fig. 6

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 3040862 A1 **[0009]**
- EP 0443377 A2 **[0053]**
- EP 2683589 B1 **[0053]**
- EP 2244188 A1 **[0053]**

Non-patent literature cited in the description

- **ANTWEILER**. Bahn-Betriebsleitsystem ILTIS. *Signal & Draht*, 1995, vol. 87 (10), 337-340 **[0053]**
- Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme. *EN 50128*, March 2012 **[0053]**
- **MANTERE, TIMO**. Electronic Imaging & Signal Processing - Image comparison based on morphological transforms. *SPIE Newsroom.*, 29 November 2007 **[0053]**