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

(11) **EP 4 234 359 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
30.08.2023 Bulletin 2023/35

(21) Application number: **23158266.9**

(22) Date of filing: **23.02.2023**

(51) International Patent Classification (IPC):
B61L 25/08 *(2006.01)* ***B61L 27/30*** *(2022.01)*

(52) Cooperative Patent Classification (CPC):
B61L 25/08; B61L 27/30

(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 ME MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA
Designated Validation States:
KH MA MD TN

(30) Priority: **24.02.2022 IT 202200003482**

(71) Applicant: **RFI S.p.A.**
00161 Roma RM (IT)

(72) Inventors:
- **BARBARESCHI, MARIO**
  NAPOLI (IT)
- **DE SIMONE, SALVATORE**
  80030 TUFINO - NAPOLI (IT)
- **MUNGIELLO, INNOCENZO**
  80030 ROCCARAINOLA - NAPOLI (IT)
- **ZOPPI, TOMMASO**
  FIRENZE (IT)

(74) Representative: **Conti, Marco**
Bugnion S.p.A.
Via di Corticella, 87
40128 Bologna (IT)

(54) **SYSTEM AND METHOD FOR DISPLAYING THE STATUS OF A RAILWAY TRANSPORTATION PLANT**

(57) Described is a system in accordance with the requirements specified for the maximum levels of safety integrity and security for safety-critical applications, designed to: (a) safely display the status of a railway transportation plant on an operator interface terminal, consisting of a commercial off-the-shelf (COTS) device (3), of fixed or mobile type (such as, for example, tablet and smartphone devices), connected through an open network (including the 3G/4G/LTE/5G mobile networks) to a calculation terminal (2), which receives the status of the railway transportation plant from a command and control platform (10); (b) sending commands towards the command and control platform (10) from the COTS operator terminal (3). Protection of the transmission of data over an open network (security) is guaranteed by a "transfer server" (4), which provides a protected workspace, for example, in accordance with NIS-2016/1148, for controlling access and directing the railway transportation plant to the command and control platform (10), for decrypting and decompressing images and for any other type of communication from and to the COTS operator terminal. The maximum Safety Integrity Level (SIL) is guaranteed by the architecture of the calculation terminal (2), in accordance with the requirements defined by CENELEC EN 50126 EN 50128 and EN 50129 standards, and by decrypting on the transfer server (4) the image previously encrypted by the calculation terminal (2) before transmission. This system may also be used in all industrial applications different from railway applications, in which it is necessary to safely control remotely a generic operator interface terminal.

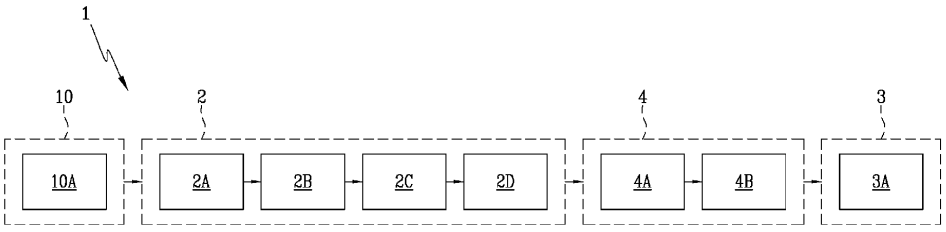

Fig.2

EP 4 234 359 A1

Description

[0001] This invention relates to a system and a method for displaying a status of a railway transportation plant on a terminal of a commercial type connected on an open network.

[0002] The term "*open network*" means, as defined in CENELEC EN 50159, an "open transmission system - a transmission system with an unknown number of participants, with unknown, variable and unreliable properties, used for unknown telecommunications services and with potential for unauthorised access".

[0003] The invention relates to the sector of safely displaying the status of a railway transportation plant or parts of it, that is to say, railway bodies such as, for example, signals, switches, track circuits, level crossings and others; The invention also relates to the sector of safely forwarding commands for managing the status of a railway transportation plant or parts of it, by an operator through an operator terminal of a commercial type connected on an open network.

[0004] In particular, in this sector, user interfaces, that is, display and control systems, are used, as in the case of the so-called *luminous panel* and *operator terminal*, which allow an operator to understand the status of the railway transportation plant and to impart commands for managing the plant. In addition to or instead of the luminous panel and the operator terminal, which are fixed types of user interfaces, there may be mobile user interfaces, such as, for example, tablet devices, comprising a display screen and a system for imparting commands. In this technical sector, the safety of the railway signalling is managed by a command and control platform, also called the safety nucleus or central apparatus, which is, for an example of the railway sector, designed to safely execute the routing logics or the spacing of the trains, control the compatibility between the commands sent by an operator and the status of the railway transportation plant, in such a way that it is not possible to perform movements which are in conflict with each other; therefore, in order to guarantee the correct operation of the system, the command and control platform must meet certain safety requirements; in particular, in the rail sector, these systems are developed in accordance with the European safety standard CENELEC, and must meet the requirements of the SIL4 level (*Safety Integrity Level 4)* defined in EN 50126, EN 50128 and EN 50129. Similarly, it is important that the display and control systems for the management of the plant, that is to say, the user interfaces, comply with a sufficiently high safety standard, so that the actions of the operator are performed in a safe manner and in a manner consistent with the status of the railway transportation plant.

[0005] While there are different methods to achieve this objective with systems designed for the purpose and connected on closed networks, achieving the same objective is particularly complex when operator interfaces using commercial devices must be used (COTS: *commercial off-the-shelf*) and connected via an open network.

[0006] For this purpose, display systems are known which use procedures for checking the correctness and integrity of information and images regarding the status of the plant to be displayed.

[0007] An example of such systems is contained in patent document EP3438828B1, which describes a system where the correct display of the image is checked by means of a feedback control between an image to be displayed, generated by a COTS device, and the data, acquired from a safety nucleus, that is to say, a control and drive platform, and starting from which the image was generated. Since the image is generated inside a COTS device, the measures adopted to achieve a sufficiently high safety standard - and which include the adoption of feedback mechanisms - in this case make the system complex and its performance levels potentially critical.

[0008] A further example is contained in patent document ITGE2011000034, which describes a system in which a first processor generates an image and sends it to a screen, from which a *frame grabber* device captures the image and sending it to a second processor; the second processor generates a second image and compares the image captured by the *frame grabber*; thus, in this case, too, the control is performed by feedback. However, the presence of the *frame grabber* device and feedback control make the system complex. Moreover, this system is difficult to make on portable devices, that is, mobile devices, connected on an open network and cannot use terminals of the commercial type.

[0009] Patent document IL72348A describes two processors which generate each of the graphical information (that is, symbols) in parallel and transfer, to two display controllers, which transform the information into images. These images are sent, as well as to a display (denoted in the drawings by BS), to the two processors by means of a feedback channel which uses a shift register. The two processors compare the information received byte-to-byte and if the comparison fails, then the transmission is interrupted. The method described by patent document IL72348A can be used efficiently because the images they generate have a low resolution (approximately 500x500 pixels). Moreover, the display on which the image is displayed is a display which may be controlled completely by the operator, and therefore not COTS; therefore, this system is not very suitable for processing high resolution images and also when you want to display them on COTS type displays.

[0010] Other examples of systems for displaying a status of a railway transportation plant are described by patent documents EP0970869B1 and DE4432419A1; however, not even these documents provide a solution which is able to satisfy the needs of the market.

[0011] The aim of the invention is to provide a system and a method for displaying the status of a railway transportation plant by means of a COTS operator terminal

connected on an open network which overcome the drawbacks of the above-mentioned prior art techniques and which is simple to construct.

[0012] Said aim is fully achieved by the system and method according to the invention as characterised in the appended claims.

[0013] The system comprises a command and control platform, configured to provide a flow of input data. The flow of input data represents the status of the railway transportation plant or parts of the railway transportation plant, that is to say, railway bodies such as, for example, signals, points, track circuits, level crossings and others.

[0014] The system comprises a calculation terminal, configured for receiving a flow of input data. According to an example, the computer terminal is in compliance with the requirements for the maximum levels of safety integrity as specified for safety-critical applications and defined by CENELEC EN 50128 and EN 50129. Preferably, the calculation terminal is configured for receiving the flow of input data from the command and control platform. The calculation terminal is configured for generating a flow of first images and a flow of second images starting from the flow of input data. Preferably, the images of the flow of first images and of the flow of second images are in a raw format and the calculation terminal is configured for converting the images of the flow of first images and of the flow of second images from the raw format to a standard format. The expression "raw" referred to the image format may be used as a synonym for "not processed" or "unrefined". In expression "raw format" means that the image generated is stored by saving, for each pixel of the image, the R, G and B components (preferably without other additional information and/or without processing said R, G and B components). Therefore, the images of the flow of first images may be in a raw format, that is to say, the images of the flow of first images may be generated by saving, for each pixel of said images, the R, G and B components. The images of the flow of second images may be in a raw format, that is to say, the images of the flow of second images may be generated by saving, for each pixel of the images, the R, G and B components.

[0015] In particular, the flow of input data includes a plurality of data series, each data series of the plurality of data series representing the status of the railway transportation plant or parts of the railway transportation plant at a same instant. Each image of the flow of first images is generated starting from a respective data series of the plurality of data series.

[0016] Similarly, each image of the flow of second images is generated starting from a respective data series of the plurality of data series.

[0017] According to a preferred example, the calculation terminal includes a first processor. The first processor is programmed to generate a flow of first images. Preferably, the first processor is programmed to generate, starting from the flow of input data, a flow of first images. Preferably, the calculation terminal includes a second processor. The second processor is programmed to generate a flow of second images. Preferably, the second processor is programmed to generate, starting from the flow of input data, a flow of second images.

[0018] Preferably, the first processor and the second processor receive as input the same flow of input data for generating, in a parallel fashion, the flow of first images and the flow of second images, respectively.

[0019] Therefore, starting from each data series of the plurality of data series, the first processor is programmed for generating an image, in this way forming a corresponding flow of first images. Similarly, starting from each data series of the plurality of data series, the second processor is programmed for generating an image, in this way forming a corresponding flow of second images.

[0020] The first processor is programmed to generate images of the flow of first images in raw format. The first processor is also programmed for converting each image from the raw format to a predetermined standard format, for example, to the jpeg, gif, png or bitmap formats. The second processor is programmed to generate images of the flow of second images in raw format. The second processor is also programmed for converting each image from the raw format to a predetermined standard format, for example, to the jpeg, gif, png or bitmap formats.

[0021] Preferably, the first processor and the second processor are programmed for generating the respective images (that is, the first images of the flow of first images and the second images of the flow of second images, respectively) in a raw format and to convert each image from the raw format to a predetermined standard format, for example, to the jpeg, gif, png or bitmap formats.

[0022] Preferably, a first image of the flow of first images, generated starting from a data series of the plurality of input data series and a corresponding second image of the flow of second images, generated starting from the same data series of the plurality of data series, forms a pair of images. In particular, each image of the flow of first images and of the flow of second images, generated starting from the same data series of the plurality of data series, forms a pair of images. In this way, starting from the flow of first images and the flow of second images, the calculation terminal generates a flow of pairs of images.

[0023] The first processor and the second processor can be programmed to generate the respective images in a raw format, by executing applications (that is to say, software) in accordance with the requirements specified for the maximum levels of safety integrity for safety-critical applications (for example, applications that comply with SIL4 requirements according to CENELEC EN 50128) without the need to use commercial graphics libraries. The term "commercial", referring to graphics libraries, means that the graphics library may not comply with the requirements of CENELEC 50128 (to obtain certification for a certain level of SIL safety). A commercial graphics library can be provided free of charge or upon

payment of a license. Thus, the term "non-commercial graphics library" means a graphics library which has a certification (for example, a certification for a certain SIL safety level) and/or whose source code is possessed and the term "commercial graphics library" means a graphics library which does not have safety certifications and/or the source code is unavailable.

[0024] The calculation terminal is configured for generating a flow of output images, for example, starting from the flow of first or second images. The flow of output images may be intended to be displayed, for example by an operator terminal. The operator terminal may be formed by a COTS device. The COTS device may be connected to the calculation terminal via an open network. According to an example, the open network may comprise one of the 3G, 4G, LTE or 5G mobile networks.

[0025] According to an example, the calculation terminal is configured for checking that, for each pair of images formed by a first image of the flow of first images and a corresponding second image of the flow of second images, the first and the second images are consistent with each other. The computer terminal may be configured, in response to a positive outcome of said check, for enabling an output transmission of the stream of output images. In other words, the calculation terminal checks that, for each pair of images formed by a first image of the flow of first images and a second image of the flow of second images, the first image is consistent with the second image and vice versa, that is, it checks that the first image coincides with the second image and vice versa. The calculation terminal may be configured to check that the first and the second image of the pair of images are consistent with each other, wherein the first and the second image are in raw format or in a standard format.

[0026] The software that is run on the first processor and on the second processor, including the image generating software, complies with the requirements specified for the maximum levels of safety integrity for safety-critical applications (for example, SIL4 according to the railway standard CENELEC EN 50128), and thus does not use commercial off-the-shelf (COTS) libraries, and in particular does not use COTS graphics libraries.

[0027] For this reason and for checking consistency between the first and second images described above, the system is protected against errors in the process for generating the image by one between the first processor and the second processor.

[0028] In this regard, it should be noted that the pair of images is not controlled according to a feedback logic; in fact, the flow of output images intended to be displayed is only generated after receiving a response to checking the consistency between the images of a pair. This fact contributes to rendering the display on the COTS operator terminal secure.

[0029] The applications performed to generate the images and to convert them from raw format to standard format comply with the requirements for maximum safety levels (that is, SIL4). Therefore, the first processor and the second processor are programmed to generate, respectively, a flow of first images and a flow of second images starting from the flow of input data, by applications which comply with the requirements specified for maximum safety levels.

[0030] An output image of the flow of output images preferably shows to the operator, through a screen, a graphical view which shows the status of a railway transportation plant or the status of parts of the railway transportation plant, such as, for example, the position of a points device, the aspect of a high signal, and others.

[0031] According to an example, the system comprises a memory, in which a graphical data structure is loaded. The graphical data structure includes a plurality of graphical data records wherein the graphical data records represent the symbols included in a reference image of the railway transportation plant and represent the position of the symbols inside the reference image. Preferably, the graphical data structure conforms to a predetermined level of safety integrity. The memory comprises instructions for managing the output image. Preferably, the management instructions comply with predetermined safety integrity requirements;

[0032] The calculation terminal may be programmed to perform the management instructions of the image representing the status of a railway transportation plant and generate the output image.

[0033] According to an example embodiment, the computer terminal includes a bi-directional communication channel. Preferably, the bi-directional channel connects together the first processor and the second processor. For example, the bi-directional channel may be configured for sharing information between the first processor and the second processor. In particular, the first and the second processors are programmed to check the correspondence of a respective pair of images, formed by a first image of the flow of first images and a corresponding second image of the flow of second images.

[0034] For example, the first processor and the second processor exchange, that is to say, share information, which may include, for example, a first and a second image. For this reason, the checking of the consistency between images is performed in a redundant fashion, that is to say, the checking of the consistency between images is performed both by the first processor and by the second processor. This feature therefore constitutes an element for protecting the safety of the system.

[0035] For example, from said checking, the first processor is programmed to generate a first check signal, representing the consistency of the respective pair of images. For example, from said check, the second processor is programmed to generate a second check signal, representing the consistency of the respective pair of images. Preferably, each processor of the pair consisting of the first and second processors is programmed to check a respective pair of images, to generate a first check signal and a second check signal, respectively, each first and second check signal representing the con-

sistency of the respective pair of images. In particular, each processor of the pair consisting of the first and second processor is programmed to check each pair of the flow of pairs of images. Consequently, the first processor and the second processor, generate, respectively, a flow of first check signals and a flow of second check signals.

[0036] According to an example embodiment, the first processor is programmed to derive, starting from the first image, a first signature and the information shared between the first and the second processor includes the first signature. In this way, the first processor derives a flow of first signatures, starting from the corresponding flow of first images. According to an example, the second processor is programmed to derive, starting from the second image, a second signature and the information shared between the first and the second processor includes the second signature. In this way, the second processor derives a flow of second signatures, starting from the corresponding flow of second images. Preferably, the first and the second processor are programmed to derive, starting from the first image and from the second image, respectively, a corresponding first and second signature, and the information shared between the first and the second processor includes the first and the second signature, for each pair of images.

[0037] Since the first processor and the second processor exchange their respective signatures between each other, this means that the checking of the consistency between the images does not occur by checking the images, but by checking the consistency of the signatures derived from the images, making the checking faster. For example, the signature of an image may be derived by applying to the image a function which uniquely identifies the image. For example, the function may be a HASH function. According to an example embodiment, the calculation terminal is equipped with an operating system. Preferably, the operating system is a real-time operating system. The real-time operating system ensures the determinism of operations carried out under its supervision. The real-time operating system can comply with the requirements specified for the maximum levels of safety integrity as required for safety-critical applications by CENELEC EN 50128 and EN 50129 (that is, SIL4).

[0038] The calculation terminal may be configured to perform, under the supervision of the real-time operating system, some operations for which the first processor and the second processor, that is, the calculation terminal, are programmed. These functions can include, for example:

- generating the flow of first images and the flow of second images in the raw format,
- the conversion of each first image and second image from the raw format to the predetermined standard format,
- checking the consistency of the pair of images and
- the transmission of the flow of output images, that is to say, of the output images.

[0039] According to an example embodiment, the system comprises an operator terminal, that is to say, an operator terminal which can be used, for example, by a railway operator. The operator terminal may include a fixed terminal, such as, for example, a COTS computer, or a COTS mobile terminal, such as a tablet or smartphone. Preferably, the operator terminal includes a screen for displaying a flow of output images.

[0040] According to an example embodiment, the system comprises a transfer server. The aim of the transfer server is to transfer data, for example the flow of output images, to an operator terminal, preferably a COTS operator terminal. In particular, the aim of the transfer server is to provide a protected workspace, that is to say, a working environment in which communications to the operator terminal and starting from the operator terminal are carried out in a secure manner and protected from intrusion, especially if the operator terminal is a COTS device. According to an example, the transfer server complies with the applicable security requirements as specified by NIS-2016/1148.

[0041] According to an example, the calculation terminal may be configured for encrypting or, in addition, for compressing each image of the flow of output images. The calculation terminal may also be configured for transmitting each image of the flow of output images encrypted, or in addition, compressed, to the transfer server. The transfer server may be configured to decrypt, or in addition decompress, each image of the flow of output images. The transfer server may be configured to make the flow of output images available to a COTS operator terminal. For example, the transfer server may be configured to provide a flow of output images to a COTS operator terminal, operatively connected to the transfer server, through a communication connection, for example available at least temporarily, that is, available at least for the time necessary for completion of a work session. For this purpose, for example, the COTS operator terminal may be configured to connect to the transfer server by means of a network authentication procedure, by which an operator enters its own access credentials, that is to say, a user name and a password.

[0042] According to an example, the system may include a management server, configured to receive the access credentials from the operator terminal and manage the network authentication procedure, enabling the communication connection between the operator terminal and the transfer server for the time necessary for the completion of a work session. According to an example embodiment, the transfer server is a network server. For example, the network server is designed to transfer the flow of output images to the COTS operator terminal, through a web page. More specifically, the network server may be configured to receive the flow of output images from the calculation terminal, to decipher and decompress each image of the flow of output images and to

create a web page containing an image of the flow of output images corresponding to the updated status of the plant. The network server may be configured to transmit the web page to the COTS operator terminal, for example by means of a connection on an open network.

[0043] The transfer server is designed to transfer a flow of output images to a COTS device, so as to increase the security and protection of the flow of output images.

[0044] According to an alternative example, the transfer server transmits each image of the flow of output images to the COTS operator terminal, the COTS operator terminal being configured to decompress and decrypt each image of the flow of output images.

[0045] The operator terminal may include a control system, configured for controlling the railway transportation plant or parts of the railway transportation plant. For example, the control system may include a touch screen monitor, and in addition or alternatively include a mouse, and in addition or alternatively, a keyboard, which allow the operator to interact with the operator terminal to impart commands. The operator terminal may be connected to the calculation terminal and may comprise a control system, for sending a control signal to the calculation terminal, for controlling the railway transportation plant or parts of the railway transportation plant.

[0046] The system may comprise an authorisation system, in order to check and authorise the control signals generated by the operator terminal. For that purpose, the calculation terminal may be configured for receiving a control signal from the operator terminal and generating, in response to the control signal, a one-time password. The calculation terminal may also be configured to generate a request signal for the operator terminal, that is to say, a signal requesting an insertion of the one-time password by the operator. The operator terminal may be configured to receive the one-time password from the calculation terminal. The operator terminal may be configured to receive from the calculation terminal the signal requesting insertion of the one-time password.

[0047] In response to the signal for requesting the insertion of the one-time password by means of the calculation terminal, the operator terminal may be configured to return the one-time password to the calculation terminal. Preferably, the transmission of the one-time password from the calculation terminal to the operator terminal takes place using a communication channel different from the communication channel used for returning the one-time password from the operator terminal to the calculation terminal. According to an example, the transmission of the one-time-password from the calculation terminal to the operator terminal is performed using SMS technology, whilst the return of the one-time-password to the calculation terminal from the operator terminal is performed using a data connection. According to another example, the transmission and the return of the one-time-password occur on two different channels which use the same technology, for example which use a data connection, but on different connections.

[0048] Preferably, the transmission of the one-time password from the computer terminal to the operator terminal occurs using a communication channel different from the communication channel in which there is the transmission of the stream of output images from the computer terminal to the operator terminal. According to a further example, the system may comprise a personal mobile device, for example a smartphone supplied to the operator, connected to the calculation terminal for the transmission, using a communication channel, of the one-time password, whilst the return of the one-time password occurs through a communication channel between the operator terminal, for example a tablet or an computer, and the calculation terminal.

[0049] According to an example, the transmission of the one-time password from the calculation terminal to the operator terminal and from the operator terminal to the calculation terminal is performed inside a protected workspace wherein all the data is transmitted to and from the operator terminal, including images, commands, user authentication data, encryption data.

[0050] According to an example, the terminal is configured to check that the one-time password generated by the calculation terminal, that is to say the one-time password transmitted from the calculation terminal to the operator terminal and the one-time password returned from the operator terminal to the calculation terminal are consistent with each other. If the control has a positive outcome, the calculation terminal is configured for transmitting the control signal to the command and control platform in response to said control, in such a way that only the commands positively checked are sent to the command and control platform.

[0051] According to an example, the COTS operator terminal is programmed for generating and transmitting to the calculation terminal, in addition to the control signal, a signal confirming the command by the operator. The calculation terminal may be programmed for receiving the command confirmation signal from the operator and for transmitting the command signal to the command and control platform, upon receiving the command confirmation signal.

[0052] According to an example embodiment, the calculation terminal includes a watchdog circuit. The watchdog circuit is connected to the first processor and to the second processor. The watchdog circuit can comply with the requirements specified for the maximum levels of safety integrity as required for safety-critical applications by CENELEC EN 50128 and EN 50129 (that is, SIL4). The watchdog circuit is configured to disable the transmission of the flow of output images, in response to a negative outcome of the consistency check of each pair of images of the flow of pairs of images generated by the first and by the second processor. For example, the watchdog circuit may be connected to the first processor to receive the first check signal from the first processor and disable the transmission of the output image , in response to a negative outcome of the check of the pair of

images. The watchdog circuit may also be connected to the second processor to receive the second check signal from the second processor and disable the transmission of the output image. According to a preferred embodiment, the watchdog circuit is connected to the first processor and to the second processor to receive, respectively, the first check signal and the second check signal and to disable the transmission of the output image from the calculation terminal upon a negative outcome of the check of the pair of images, that is to say, in response to the first check signal and to the second check signal, wherein at least one of the check signals represents a negative outcome of the check of the pair of images. In this way, the transmission of the output image is guaranteed only when both the first and the second processor are in accordance on the checking of the congruence of the pair of images. If at least one between the first processor and the second processor disagrees on the check of the consistency of the pair of images, or detects any other type of anomaly with potential impact on the safety of the system, the watchdog circuit is programmed to disable the transmission of the output image and prevent potentially dangerous decisions from being taken by the operator, as a result of a display which is inconsistent with the status of the system.

[0053] The invention also provides a method for displaying a status of a railway transportation plant.

[0054] The method comprises a step of preparing, by a command and control platform, a flow of input data representing the status of the railway transportation plant. The method comprises a step of receiving, at a calculation terminal, a flow of input data. According to an example, the computer terminal is in compliance with the requirements for the maximum levels of safety integrity as specified for safety-critical applications and defined by CENELEC EN 50128 and EN 50129 (that is, SIL4). The method comprises a step of generating, by the calculating terminal starting from a flow of input data, a flow of first images. The images of the flow of first images are, for example, in raw format. The method comprises a step of generating, by the calculating terminal, starting from a flow of input data, a flow of second images. The images of the flow of second images are, for example, in raw format. According to an example, the method comprises a step of converting, by the calculation terminal, the images of the flow of first images from the raw format to a standard format, the method may comprise a step of converting, by the calculation terminal, a flow of second images from the raw format to a standard format. The method comprises a step of checking, by the calculation terminal, for each pair of images formed by a first image of a flow of first images and by a corresponding second image of the flow of second images, that the first and the second images are consistent with each other. As a consequence of a check step, the method comprises a step of transmitting, by the computer terminal, that is to say, enabling the computer terminal for the transmission, the stream of output images, for example obtained starting from the stream of first or second images.

[0055] According to a preferred example, the calculation terminal includes a first processor and a second processor. The method comprises a step of receiving, at the calculation terminal, the flow of input data. The method comprises a step of generating, by the first processor, starting from the flow of input data, a flow of first images. Preferably, the images of the flow of first images are in a raw format. Preferably, the method comprises a further step of generating, by the second processor, starting from the flow of input data, a flow of second images. Preferably, the images of the flow of second images are in a raw format. The method comprises a step of converting, by the first processor and the second processor, the respective images from the raw format to a standard format. The method may comprise a step of checking, by the first processor and the second processor, for each pair of images formed by a first image of the flow of first images and by a corresponding second image of the flow of second images, that the first and the second images are consistent with each other. As a result of a check step, the method may comprise a step of enabling the transmission of a flow of output images, by the calculation terminal, obtained starting from the flow of first or second images.

[0056] The step of checking the first and second images of each pair of images may be performed on the images in raw format or in standard format.

[0057] According to an example, the first and second processors execute applications which comply with the requirements specified for the maximum levels of safety integrity for safety-critical applications and defined by CENELEC EN 50128 (that is, SIL4) without the need to use commercial graphics libraries for generation of the images.

[0058] Therefore, the first processor and the second processor generate (that is, the method comprises a step of generating, by the first processor and the second processor), respectively, a flow of first images and a flow of second images starting from the flow of input data, by applications which comply with the requirements specified for maximum safety levels (that is, SIL4).

[0059] According to an embodiment, the computer terminal includes a bi-directional communication channel between the first processor and the second processor, and the method may comprise a step of sharing information between the first processor and the second processor, through the bi-directional channel. The method may comprise a step of checking, by the first and the second processors, a respective pair of images. The method may also comprise a step of generating, by the first and the second processor, a first check signal and a second check signal, respectively, each check signal representing a consistency of the respective pair of images.

[0060] According to an example, the method comprises a step of preparing management instructions, the step of preparing instructions including a step of preparing a graphical data structure. The step of preparing the graph-

ical data structure may comprise a step of providing a reference image for the railway transportation plant. In particular, the reference image includes symbols positioned according to a configuration of the railway transportation plant, the symbols belonging to a plurality of predetermined symbols. The step of preparing the graphical data structure may comprise a step of scanning a reference image to identify the symbols included. The step of preparing the graphical data structure may comprise a step of generating the graphical data structure including a plurality of graphical data records, as a function of the symbols identified by the scanning and of an arrangement of the symbols identified in the reference image.

[0061] The method may comprise a step of checking the correctness of the structure of the graphical data to guarantee a predetermined level of security integrity. The method may include a step of loading management instructions and the graphical data structure in a calculation terminal, the calculation terminal being a component compliant with predetermined safety integrity requirements.

[0062] According to an embodiment, the method comprises a step of deriving, by the first and the second processor, starting from the first image and from the second image, respectively, a corresponding first signature and second signature. Preferably, the method comprises a step of sharing information between the first and the second processor, the step including the sharing of the first and the second signature, for each pair of images. According to an example embodiment, the method comprises a step of interrupting, by a watchdog circuit, for example in accordance with the requirements specified for the maximum levels of safety integrity as required for safety-critical applications by CENELEC EN 50128 and EN 50129 (that is, SIL4), the transmission of the flow of output images. Preferably, the method comprises a step of interrupting, by a watchdog circuit, the transmission of the flow of output images in response to a negative outcome of the check. For example, the method may comprise a step for receiving, at the watchdog circuit, a first check signal and a second check signal and a step of interrupting the transmission of the flow of output images in response to a negative outcome of the check of the pair of images, that is, in response to at least one between the first check signal and the second check signal being negative, that is to say, displaying a negative outcome of the check of the pair of images by the first processor or by the second processor.

[0063] According to an embodiment, the method comprises preparing a transfer server, the transfer server providing a protected workspace, preferably, if the operator terminal includes a COTS device, that is to say, an environment in which communications to the operator terminal and starting from the operator terminal are carried out in a secure manner and protected from intrusions. According to an example, the transfer server is made in accordance with the security requirements that ensure the security characteristics required by the NIS-2016/1148 regulations, for example by the NIS-2016/1148 regulations. For this purpose, the method may comprise a step of encrypting, or in addition, compressing, for example by the calculation terminal, each image of the flow of output images. The method may comprise a step of transferring, by the calculation terminal, the flow of output images, for example to the transfer server. The method may comprise a step of decrypting, or in addition of decompressing, by the transfer server, each image of the flow of output images. The method may comprise preparing a COTS operator terminal, for example operatively connected to the transfer server, through a communication connection, available at least temporarily, that is, available at least for a time necessary for completion of a working session. For example, the COTS operator terminal may be configured to connect to the transfer server by means of a network authentication procedure, by which an operator enters access credentials, that is to say, a user name and a password. According to an example, the method may comprise a step of network authentication, by a management server. The network authentication may comprise a step of receiving access credentials coming from the operator terminal and a step of checking the credentials for enabling the communication connection between the operator terminal and the transfer server at least for the time necessary for completion of a work session.

[0064] The method may comprise a step of feeding the flow of output images to the COTS operator terminal, by the transfer server. The method may comprise a step of displaying, by the COTS operator terminal, each image of the flow of output images.

[0065] According to an embodiment, the method comprises a step, executed by an operator terminal, for controlling the plant or parts of the railway transportation plant. For this purpose, the method may comprise a step of sending a control signal by the operator terminal. The operator terminal may be a COTS operator terminal, for example a tablet or a computer. The method may comprise a step of receiving, by the calculation terminal, a control signal from a COTS operator terminal. The method may include a step of generating a one-time password by the calculation terminal, in response to the control signal. The method may comprise a further step of generating a request signal for the COTS operator terminal, by the calculation terminal, that is to say, a signal requesting an insertion of the one-time password by an operator. The method may comprise a step of receiving the one-time password by the COTS operator terminal. Moreover, the method may include a step of returning the one-time password to the calculation terminal in response to the request signal for insertion of the one-time password by the calculation terminal. Preferably, the method may comprise a further step, by the calculation terminal, of checking that the one-time password generated by the terminal, that is to say the one-time password transmitted from the calculation terminal to the COTS

operator terminal and the one-time password returned by the COTS operator terminal are consistent with each other. The method may also comprise a step, executed by the calculation terminal, of transmitting the control signal to the command and control platform, in the case of a positive outcome of said control.

[0066] According to an example, the method comprises a step, by means of the calculation terminal, for receiving a control signal from the COTS operator terminal. The method may comprise steps, by means of the COTS operator terminal, for generating and transmitting the control signal to the calculation terminal, for generating and transmitting, to the calculation terminal, a signal for confirming the command by an operator, and, by means of the calculation terminal, the steps of receiving the signal for confirming the command by the operator and transmitting the control signal to the command and control platform, upon receiving said confirmation signal. According to an example, the transmission of the signal confirming the control signal occurs by means of the transfer server, based on the security functions of offered by the protected workspace. The system according to the invention complies with the most stringent safety requirements for safety-critical and security applications, and allows the following aims to be achieved:

- safely displaying the status of a railway transportation plant on an operator interface terminal, possibly also of a commercial type (including tablet devices), connected through an open network (including the 3G/4G/LTE/5G mobile networks) to a processing system, which receives the status of the railway transportation plant from a command and control platform;
- sending commands from the operator terminal towards the command and control platform.

[0067] Protection of the transmission of data over an open network (security) is guaranteed by a secure platform (transfer server), which preferably complies with NIS-2016/1148, for controlling access and directing towards the control platform of the railway transportation plant, for decoding (decrypting) and decompressing images and for any other type of communication from and to the terminal.

[0068] The Safety Integrity Level (SIL) is particularly high, thanks also to the architecture of the calculation terminal, which preferably conforms to the requirements specified by the CENELEC EN 50128 and EN 50129 standards; another aspect which contributes to maintaining a high Level of Safety Integrity is represented by the decoding (decrypting) on the operator terminal of the coded image (encrypted) from the calculation terminal before the transmission.

[0069] It should be noted that the system according to the invention may also be used in all the industrial applications different from railway applications, in which it is necessary to safely control remotely a generic operator interface terminal.

[0070] These and other features will become more apparent from the following description of a preferred embodiment, illustrated by way of non-limiting example in the accompanying drawings, in which:

- Figure 1 illustrates a system for displaying a status of a railway transportation plant, according to one or more of the aspects of the invention;
- Figure 2 illustrates a system for displaying a status of a railway transportation plant on a COTS operator terminal, according to one or more aspects of this disclosure;
- Figure 3 and Figure 4 illustrate a detail of the system, according to one or more of the aspects of the invention;
- Figures 5, 6 and 7 illustrate steps of the system for displaying a status of a railway transportation plant, according to one or more of the aspects of the invention.

[0071] The numeral 1 in the accompanying drawings denotes a system for displaying a status of a railway transportation plant.

[0072] The system 1 comprises a command and control platform 10 and a calculation terminal 2. The computer terminal 2 complies with the requirements specified for the maximum levels of safety integrity as required for safety-critical applications, according to CENELEC EN 50128 and EN 50129 regulations. The command and control platform 10 is configured to provide a flow of input data 100 to the calculation terminal 2. For this purpose, the command and control platform 10 is connected to the calculation terminal 2 for example by a closed network, for example a LAN network. The flow of input data 100 represents the status of the railway transportation plant or parts of the railway transportation plant, that is to say, railway bodies such as, for example, signals, points, track circuits, level crossings and others. In particular, the flow of input data 100 includes a plurality of data series. Each data series of the plurality of data series represents the status of the railway transportation plant or parts of it at the same instant.

[0073] The calculation terminal 2 is configured for receiving the flow of input data 100 from the command and control platform 10.

[0074] The calculation terminal 2 is configured for generating, starting from the flow of input data 100, a flow of first images 201A. In particular, each first image 201A of the flow of first images 201A is generated starting from a respective data series of the plurality of data series.

[0075] The calculation terminal 2 is also configured for generating, starting from the flow of input data 100, a flow of second images 201B. In particular, each second image 201B of the flow of second images 201B is generated starting from a respective data series of the plurality of data series. Therefore, starting from each data series of the plurality of data series, the calculation terminal 2 is

programmed for generating a first image 201A, forming, in this way, a corresponding flow of first images 201A. Similarly, starting from each data series of the plurality of data series, the calculation terminal 2 is programmed for generating a second image 201B, forming, in this way, a corresponding flow of second images 201B.

[0076] According to a preferred example, the calculation terminal 2 includes a first processor 200A and a second processor 200B. The first processor 200A is programmed for generating, starting from the flow of input data 100 to the calculation terminal 2, a flow of first images 201A. The second processor 200B is programmed for generating, starting from the flow of input data 100 to the calculation terminal 2, a flow of second images 201B. For this reason, the first processor 200A and the second processor 200B are programmed for generating, in parallel, the flow of first images 201A and the flow of second images 201B, respectively. In particular, the first processor 200A is programmed for generating an image starting from a data series of the plurality of the data series of the flow of input data 100, forming, in this way, the corresponding flow of first images 201A. Similarly, the second processor 201B is programmed for generating an image starting from a data series of the plurality of data series of the flow of input data 100, forming, in this way, the corresponding flow of second images 201B.

[0077] According to an example, the first processor 200A and the second processor 200B are programmed to execute applications which comply with the requirements specified for the maximum levels of safety integrity for safety-critical applications, according to CENELEC EN 50128 without the need to use commercial graphics libraries. and, preferably, under the supervision of a real time operating system. The real-time operating system may comply with the requirements specified for the maximum levels of safety integrity for safety-critical applications according to CENELEC EN 50128 regulations.

[0078] Preferably, the first processor 200A and the second processor 200B are programmed for generating the respective images (that is, the first images 201A of the flow of first images 201A and the second images 201B of the flow of second images 201B, respectively) in a raw format and to convert each image from the raw format to a predetermined standard format, for example, to the jpeg, gif, png or bitmap formats.

[0079] Each image of the flow of first images 201A and of the flow of second images 201B, generated starting from the same data series of the plurality of data series of the flow of input data 100, forms a pair of images; in this way, starting from the flow of first images 201A and from the flow of second images 201B, the calculation terminal 2 generates a flow of pairs of images.

[0080] According to an embodiment, the first processor 200A is programmed to derive, starting from each image of the flow of first images 201A, a corresponding flow of first signatures 202A. The second processor 200B is programmed for deriving, starting from each image of the flow of second images 201B, a corresponding flow of second signatures 202B. For example, each signature of the flow of first signatures 202A and of the flow of second signatures 202B is derived by applying, to each image of the flow of first images 201A and of the flow of second images 201B, a same function, for example a HASH function.

[0081] Preferably, the computer terminal 2 includes a bi-directional channel 203, which connects together the first processor 200A and the second processor 200B. In particular, the bi-directional channel 203 forms an inter-process communication: (IPC) to allow the sharing of information between the first processor 200A and the second processor 200B.

[0082] In particular, through the bi-directional channel 203, the first processor 200A and the second processor 200B exchange, that is, share with each other, respectively, the stream of first signatures 202A and the stream of second signatures 202B. Each processor of the pair consisting of the first processor 200A and the second processor 200B is programmed to check the consistency of each pair of images, comparing each first signature 202A of the flow of first signatures 202A with a corresponding second signature 202B of the flow of second signatures 202B. The first processor 200A is programmed to generate a first check signal 204A, representing the consistency of a first signature 202A with a corresponding second signature 202B, that is to say, a first signature 202A derived starting from a first image 201A of the flow of first images 201A and a corresponding second signature 202B derived starting from a second image 201B of the flow of second images 201B. The first processor 200A is programmed for generating a first check signal 204A for each pair of images of the flow of pairs of images, in such a way as to generate a corresponding flow of first check signals 204A.

[0083] Similarly, the second processor 200B is programmed to generate a second check signal 204B, representing the consistency of a first signature 202A with a corresponding second signature 202B, that is to say, a first signature 202A derived starting from a first image 201A of the flow of first images 201A and a corresponding second signature 202B derived starting from a second image 201B of the flow of second images 201B. The second processor 200B is programmed to generate a second check signal 204B for each pair of images of the flow of pairs of images, in such a way as to generate a corresponding flow of second check signals 204B.

[0084] According to an example embodiment, the calculation terminal 2 includes a watchdog circuit 205. The watchdog circuit 205 is preferably made according to the requirements specified for the maximum levels of safety integrity, as required for safety-critical applications according to CENELEC EN 50128 and EN 50129 regulations. The watchdog circuit 205 is connected to the first processor 200A and to the second processor 200B for receiving each first check signal 204A of the flow of first check signals 204A from the first processor 200A and the second check signal 204B of the flow of second check

signals 204B from the second processor 200B. In particular, each check signal of the first check signal 204A and of the second check signal 204B may have a positive outcome, in response to a positive outcome of the consistency of a pair of images, that is, in response to a positive outcome of the consistency of a pair of signatures, the pair of signatures being formed by a first signature 202A and a corresponding second signature 202B. Alternatively, each check signal of the first check signal 204A and of the second check signal 204B may have a negative outcome, in response to a negative outcome of the coherence of the pair of images.

[0085] In the case of a positive outcome of the first check signal 204A and the second check signal 204B, the calculation terminal 2 is configured for transmitting, starting from the flow of first images 201A or from the flow of second images 201B, a flow of output images 206. If at least one check signal between the first check signal 204A generated by the first processor 200A and the second check signal 204B generated by the second processor 200B has a negative outcome, the watchdog circuit 205 is programmed to interrupt the transmission of the flow of output images 206 by the calculation terminal 2.

[0086] According to an example embodiment, the system 1 comprises an operator terminal 3. For example, the operator terminal 3 may be a fixed terminal, such as, for example, a computer, or a mobile terminal, that is to say a mobile device, such as, for example, a tablet. The operator terminal includes a screen 300, for transmitting the flow of output images 206.

[0087] The operator terminal 3 may be a COTS operator terminal. According to an example embodiment wherein the operator terminal 3 is a COTS operator terminal, the system 1 comprises a transfer server 4. The transfer server 4 is connected to the calculation terminal 2 and to the COTS operator terminal 3. The transfer server 4 is designed to provide a protected workspace, that is to say, an environment in which the communications between the calculation terminal 2 and the COTS operator terminal 3 are carried out in a secure manner and protected from intrusion. The protected workspace, that is to say, the reference server, according to an example complies with the security requirements specified by NIS-2016/1148. According to an embodiment, the transfer server 4 is a network server. The calculation terminal 2 is configured for encrypting and for compressing each image of the flow of output images 206; the calculation terminal 2 is configured for transmitting the flow of encrypted and compressed output images 206 to the transfer server 4. The transfer server 4 is configured for decrypting and decompressing the flow of output images 206 received from the computer terminal 2. The transfer server 4 is configured to make the flow of output images 206 available to the COTS operator terminal 3. According to an example, the transfer server 4 is a network server. The network server is configured for decrypting and decompressing the stream of output images 206 and generating a web page containing each image of the output images 206. The network server is also configured for transmitting the web page to the COTS operator terminal 3 to be displayed on the screen 300 of the COTS operator terminal 3.

[0088] According to an example embodiment, the operator terminal 3 includes a control system 301, configured for controlling the railway transportation plant or parts of the railway transportation plant. According to an example, the operator terminal 3 is a mobile operator terminal, for example a tablet, and the control system 301 can include a keyboard 302, through which the operator can interact to generate a control signal. According to an example, the operator terminal 3 may be a fixed operator terminal, for example a computer, and the control system 301 can include a keyboard 302 and a mouse 303, through which the operator can interact to communicate with the operator terminal 3. According to an example, the operator terminal 3 is connected to the calculation terminal 2 and comprises a control system 301 for sending a control signal 304 to the calculation terminal 2.

[0089] According to an embodiment, the terminal 2 may be configured for receiving the control signal 304 from the operator terminal 3 and generating, in response to the control signal 304, a one-time password 306. The calculation terminal 2 may also be configured to generate a signal 307 requesting an insertion of the one-time password 306 for the operator terminal 3, that is to say, a signal requesting an insertion of the one-time password 306 by an operator to the operator terminal 3. The operator terminal 3 is configured to receive from the calculation terminal 2 the one-time password 306 is the signal 307 requesting the insertion of the one-time password 306. The operator terminal 3 is configured to return the one-time password to the calculation terminal 2, in response to the request signal 307 for inserting the one-time password 306 by the calculation terminal 2. Preferably, the transmission of the one-time password 306 from the calculation terminal 2 to the operator terminal 3 occurs using a communication channel different from the communication channel in which there is the transmission of the flow of output images 206 from the calculation terminal 2 to the operator terminal 3. In particular, the system 1 may comprise a personal mobile device 308, for example a smartphone supplied to the operator. The personal mobile device 308 is connected to the calculation terminal 2 for transmitting the one-time password 306. The return of the one-time password 306 from the operator terminal 3 to the calculation terminal 2 occurs by means of a communication channel between the operator terminal 3 and the calculation terminal 2. Preferably, the calculation terminal 2 is configured to control that the one-time password 306 generated by the calculation terminal 2, that is to say, the one-time password 306 transmitted by the calculation terminal 2 to the personal mobile device 308, on which the operator reads the one-time password, and one-time password 306 entered by the operator and then returned by the operator

terminal 3 to the calculation terminal 2 are consistent with each other. If the control has a positive outcome, or the password transmitted and the password returned are consistent with each other, the calculation terminal 2 is configured for transmitting, that is to say, forwarding, the control signal 304 to the control and drive platform 10 in response to said control.

[0090] According to an example, the COTS operator terminal 3 is programmed for generating and transmitting to the calculation terminal 2, in addition to the control signal 304, a signal for confirmation of the command by the operator and the calculation terminal 2 is further programmed for receiving the control confirmation signal from the operator and for transmitting the control signal 304 to the command and control platform 10, upon receiving the control confirmation signal.

[0091] With reference to Figures 1 and 2, the command and control platform 10 comprises a stage of:

- feeding, that is, transmitting, the flow of input data 100, representing the status of the railway transportation plant (stage 10.A).

[0092] The calculation terminal 2 comprises the following stages:

- generating the images starting from the flow of input data 100 (stage 2.A);
- consolidating the images (stage 2.B);
- generating a flow of output images 206 starting from consolidated images (stage 2.C)
- transmitting the flow of output images 206.

[0093] The operator terminal 3 comprises the following stages:

- receiving the flow of output images 206 and displaying each image of the flow of output images 206 (stage 3.A).

[0094] According to an embodiment wherein the operator terminal 3 is a COTS operator terminal, the system 1 comprises a transfer server 4, the calculation terminal 2 comprises a further stage of:

- encrypting and compressing the flow of output images 206 and transmission to the transfer server 4 (stage 2.D),

and the transfer server 4 comprises the following stages:

- decrypting and decompressing the flow of output images 206 (stage 4.A);
- preparing and updating a web page containing each image of the flow of output images and sending the web page to the COTS operator terminal 3 for displaying (stage 4.B).

[0095] The invention also provides a method for displaying a status of a railway transportation plant. This method is preferably implemented in a system 1 to represent the status of a railway transportation plant, according to one or more features described above.

[0096] Preferably, the method for displaying the status of a railway transportation plant comprises the following steps, which can be performed in sequence (illustrated by way of example in Figures 5-7).

[0097] A0. Preparing a command and control platform 10 and a computer terminal 2 in accordance with the requirements for the maximum levels of safety integrity for safety-critical applications and defined by CENELEC EN 50128 and EN 50129, the computer terminal 2 including a first processor 200A and a second processor 200B. Preparing, by the command and control platform 10, a flow of input data 100, representing the status of the railway transportation plant and transmission, preferably through a closed network, for example a LAN network, of the flow of input data 100, by the command and control platform 10.

[0098] A1. Receiving, by the calculation terminal 2, the flow of input data 100 and receiving, by each first processor 200A and second processor 200B the flow of input data 100. Generating, in parallel, by the first processor 200A and the second processor 200B, starting from the flow of input data 100, a flow of first images 201A and a flow of second images 201B, respectively, in raw format. Conversion, by the processor 200A and the second processor 200B of the respective images from the raw format to a standard format, such as jpeg, gif, png or bitmap. Each image of the flow of first images 201A and of the flow of second images 201B, generated starting from the same data series of the plurality of data series of the flow of input data 100, forms a pair of images in such a way as to form a flow of pairs of images.

[0099] A2. Deriving, by the first processor 200A and the second processor 200B, starting from each image of the flow of first images 201A and of the flow of second images 201B, respectively, a corresponding flow of first signatures 202A and a flow of second signatures 202B; the flow of first signatures 202A and the flow of second signatures 202B is derived by applying, to each image of the flow of first images 201A and of the flow of second images 201B, a same function, for example a HASH function.

[0100] A3. Exchanging, that is to say, sharing, between the first processor 200A and the second processor 200B, through a bi-directional communication channel 203, respectively, the stream of first signatures 202A and the stream of second signatures 202B.

[0101] A4. Checking the consistency, by the first processor 200A and the second processor 200B, of each pair of images by comparing each first signature 202A of the first flow of first signatures 202A with a corresponding second signature 202B of the flow of second signatures 202B. Generating, respectively, by the first processor 200A and the second processor 200B, a first check signal

204A and a second check signal 204B, respectively, for each pair of images of the flow of pairs of images, in such a way as to generate a corresponding flow of first check signals 204A and second check signals 204B. The first check signal 204A and the second check signal 204B each represent the consistency of a first signature 202A with a corresponding second signature 202B, that is to say, a first signature 202A derived from a first image 201A of the flow of first images 201A and a second signature 202B derived from a corresponding second image 201B of the flow of second images 201B.

[0102] A5. If a signal of the flow of first check signals 204A and second check signals 204B has a positive outcome, that is to say, if the check of the consistency of a pair has a positive outcome, enabling, by the watchdog circuit 205 complying with the requirements specified for the maximum levels of safety integrity for safety-critical applications according to CENELEC EN 50128 and EN 50129, at a transmission, by the calculation terminal 2, starting from the flow of first images 201A or from the flow of second images 201B, of a flow of output images 206 intended to be displayed.

[0103] A6. If at least one signal between the signals of the flow of first check signals 204A or of the flow of second check signals 204B has a negative outcome, interruption, by the watchdog circuit 205, of the transmission of the flow of output images 206 by the calculation terminal 2.

[0104] In an example embodiment, the method comprises the following further steps:

B0. Preparing a COTS operator terminal 3 and a transfer server 4, in particular a network server, the network server being connected to the calculation terminal 2 and to the COTS operator terminal 3, the network server providing a protected workspace, that is to say, an environment in which the communications between the processing terminal 2 and the COTS operator terminal 3 are carried out in a secure manner and protected from intrusion.

B1. Encryption and compression, by the calculation terminal 2, of each image of the flow of output images 206.

B2. Transmission, by the calculation terminal 2, of the flow of output images 206 encrypted and transmitted to the transfer server 4, that is to say, to the network server.

B3. Decrypting and decompressing, by the network server, of each image of the flow of output images 206 and updating of a web page containing each image of the flow of output images 206.

B4. Feeding, that is to say, transmission of each update of the web page containing each image of the flow of output images 206 to the COTS operator terminal 3

B5. Display of the updated web page on a screen 300 of the COTS operator terminal 3.

[0105] According to an example embodiment, the method comprises the following steps:

C1. Generating, by an operator terminal 3, a control signal 304, using a keyboard 302 and a mouse 303. Sending the control signal 304, by the operator terminal 3, to the calculation terminal 2.

C2. Receiving, from the calculation terminal 2, the control signal 304 and generating, in response to the control signal 304, a one-time password 306 and a signal 307 requesting an insertion of the one-time password 306 by an operator. Sending, by the calculation terminal 2, of the one-time password 306, to a personal mobile device 308, for example a smartphone, available to an operator, or directly to the operator terminal 3. Sending, by the calculation terminal 2, of the signal 307 requesting insertion of the one-time password 306, to the operator terminal 3.

C3. Return, by the operator terminal 3, of the one-time password 306, in response to the request signal 307.

C4. Checking, by the calculation terminal 2, that the one-time password 306 sent from the calculation terminal 2 to the personal mobile device 308 or to the operator terminal 3, and the one-time password returned, from the operator terminal 3 to the calculation terminal 2 are consistent with each other.

C5. If the consistency control has a positive outcome, forwarding, by the calculation terminal 2, of the control signal 304, to the command and control platform 10.

[0106] According to an example, the method includes a step of receiving, at the calculation terminal (2), the control signal (304) generated and transmitted by the COTS operator terminal (3); the method also comprises a step of generating and transmitting, to the calculation terminal (2), a signal confirming the command from an operator; the calculation terminal (2) receives the control confirmation signal and transmits the control signal (304), upon receiving the control confirmation signal.

Claims

1. A system (1) for displaying the status of a railway transportation plant, comprising:

- a command-and-control platform (10), configured for providing a stream of input data (100) representative of the status of the railway transportation plant;
- a computer terminal (2), set up to receive from the a command-and-control platform (10) the stream of input data (100), the computer terminal (2) including

a first processor (200A), programmed for

generating, from the stream of input data (100), a stream of first images (201A) and
a second processor (200B), programmed for generating, from the stream of input data (100), a stream of second images (201B),
wherein the first processor (200A) and the second processor (200B) are programmed for generating the respective images in a raw format and for converting each image from the raw format to a predetermined standard format, by executing applications compliant with the SIL4 level of safety integrity for safety-critical applications, without the use of commercial libraries, in particular without commercial graphic libraries,
wherein the computer terminal (2) is configured for
checking whether, for each image pair formed by a first image of the stream of first images (201A) and a corresponding second image of the stream of second images (201B), the first and the second image are consistent with each other, and
in dependence to said checking, generating, from the stream of first (201A) or second images (201B) a stream of output images (206) to be visualized from a *commercial off-the-shelf* (COTS) type operator terminal (3), stationary or mobile, connected via an open network to the computer terminal (2).

2. The system (1) according to claim 1, wherein the computer terminal (2) includes a bi-directional communication channel (203) between the first processor (200A) and the second processor (200B), configured for sharing information between the first processor (200A) and the second processor (200B), and wherein the first (200A) and the second processor (200B) are each programmed for checking a respective image pair, to generate a first check signal (204A) and a second check signal (204B), respectively, each of the first (204A) and second check signal (204B) being representative of a consistency of the image pair.

3. The system (1) according to claim 2, wherein the first (200A) and the second processor (200B) are programmed for deriving, from the first images (201A) and the second images (201B), respectively, a corresponding first (202A) and second signature (202B), and wherein the information shared between the first processor (200A) and the second processor (200B) include the first (202A) and the second signature (202B), for each image pair.

4. The system (1) according to any of the previous claims, wherein the computer terminal (2) is provided with a real-time operating system compliant with prescribed maximum level of safety integrity for safety-critical applications, and is programmed for carrying out, under the supervision of the real-time operating system, the generation of the stream of first images (201A) and the stream of second images (201B) in the raw format, and the stream of second images (201B), the conversion of each images from the raw format to the predetermined standard format, the checking of the consistency of the image pairs and the generation of the stream of output images (206).

5. The system (1) according to any of the previous claims, comprising a transfer server (4), in addition to the computer terminal (2), providing a protected workspace compliant with prescribed maximum level of security required by European norms and applicable to the technical field, wherein:

- the computer terminal (2) is configured for

  encrypting and compressing each image of the stream of output images (206) and
  sending the stream of output images (206) to the transfer server (4),

- the transfer server (4) is configured for

  decrypting and decompressing the stream of output images (206) and
  rendering the stream of output images (206) available to the user terminal (3) COTS operatively connected to the transfer server (4) through a communication channel available at least for the time necessary to complete the work session.

6. The system (1) according to any of the claims from 1 to 4 , comprising a transfer server (4), in addition to the computer terminal (2), providing a protected workspace, wherein:

- the computer terminal (2) is configured for

  encrypting and compressing each image of the stream of output images (206) and
  sending the stream of output images (206) to the transfer server (4),

- the transfer server (4) is configured for
  rendering the stream of output images (206) available to the user terminal (3) COTS,
- the user terminal (3) COTS is configured for
  decrypting and decompressing the stream of output images (206), the user terminal COTS (3) being operatively connected to the transfer server (4) through a communication channel available at least for the time necessary to complete the work session.

7. The system (1) according to any of the previous claims, wherein:

- the computer terminal (2) is programmed for

receiving a command signal (304) from the user terminal (3) COTS,
generating a one-time password (306) in response to the command signal (304) and a request signal (307) to enter the one-time password (306) by an operator, for the user terminal (3) COTS;

- the user terminal (3) COTS, is configured for

generating and sending the command signal (304) to the computer terminal (2),
receiving the one-time password (306) and sending the one-time password (306) back to the computer terminal (2), in response to the request signal (307), from the computer terminal (2), to enter the one-time password;

the computer terminal (2) being further programmed for

checking whether the one-time password (306) generated by the computer terminal (2) and the one-time password (306) sent back by the user terminal (3) COTS are consistent with each other and
sending the command signal (304) to the command-and-control platform (10) in response to said checking.

8. The system according to claim 7, wherein at least one of the following conditions is verified:

- a transmission channel of a one-time password (306) to and from the user terminal (3) COTS is different from the transmission channel used for the transmission of data between the computer terminal (2) and the user terminal (3) COTS:
- a transmission of all data, i.e. of the one-time password (306) and of the data, is executed by a protected workspace provided by a transfer server (4).

9. The system (1) according to any of the previous claims, wherein the computer terminal (2) includes a *watch-dog* circuit (205) compliant with prescribed maximum level of safety integrity for safety-critical applications, connected to the first processor (200A) and to the second processor (200B) and configured for disabling the stream of output images (206), responsive to a negative outcome of the checking or to any other anomaly with a potential impact on the safety of the system.

10. A method for displaying the status of a railway transportation plant, comprising the following steps:

- providing, by a command-and-control platform (10), a stream of input data (100), the input data (100) being representative of the status of the railway transportation plant;
- receiving, at the computer terminal (2), the stream of input data (100);
- generating, by the computer terminal (2), from the stream of input data (100), a stream of first images (201A) in a raw format,
- generating, by the computer terminal (2), from the stream of input data (100), a corresponding stream of second images (201B) in a raw format,
- converting, by the computer terminal (2), the images of the stream of first images (201A) and of the stream of second images (201B) from the raw format to a standard format,
- checking, by the computer terminal (2), for each image pair formed by a first image of the stream of first images (201A) and a corresponding second image of the stream of second images (201B), whether the first and the second images are consistent with each other, and
- in dependence to said checking, generating, by the computer terminal (2), from the stream of first (201A) or second images (201B), a stream of output images (206) to be displayed on a COTS type user terminal (3) connected via an open network to the computer terminal (2).

11. The method according to claim 10, wherein the step of generating the stream of first images (201A) and converting the images of the stream of first images (201A) to the standard format is carried out by a fist processor (200A) and wherein the step of generating the stream of second images (201B) and converting the images of the stream of second images (201B) to the standard format is carried out by a second processor (200B), the first processor (200A) and the second processor (200B) being distinct processors of the computer terminal (2) and executing applications compliant with the SIL4 level of safety integrity for safety-critical applications, without the use of commercial libraries for generating the images.

12. The method according to claim 11, wherein the computer terminal (2) includes a bi-directional communication channel (203) between the first processor (200A) and the second processor (200B), the method comprising the following steps:

- sharing information between the first processor (200A) and the second processor (200B), through the bi-directional channel (203),

- checking, by each of the first processor (200A) and the second processor (200B) a respective image pair,
- generating, by each of the first (200A) and second processor (200B), a fist check signal (204A) and a second check signal (204B), respectively, each of the of the first (204A) and second check signal (204B) being representative of a consistency of the image pair.

13. The method according to claim 12, further comprising a step of deriving, by the first (200A) and the second processor (200B), from the first and second images, respectively, a corresponding first (202A) and a second signature (202B), and wherein the said sharing information between the first (200A) and the second processor (200B) includes the first (202A) and the second signature (202B), for each image pair and the said checking of the first image (201A) and the second image (201B) includes a step of checking of a consistency between the first signature (202A) and the second signature (202B).

14. The method according to any of the claims from 10 to 13, comprising a step of interrupting, by a watchdog circuit (205) compliant with prescribed maximum level of safety integrity for safety-critical applications, the stream of output images (206), in response to a negative outcome of the checking or to any other anomaly with a potential impact on the safety of the system.

15. The method according to any of the claims from 10 to 14, comprising the following steps:

- providing a transfer server (4), defining a protected workspace compliant with prescribed maximum level of security required by European norms and applicable to the technical field;
- encrypting and compressing, by the computer terminal (2), the images of the stream of output images (206), and sending, by the computer terminal (2), the stream of output images (206) to the transfer server (4),
- decrypting and decompressing, by the transfer server (4), stream of output images (206);
- providing a user terminal (3), the user terminal (3) COTS connected via an open network to the computer terminal (2), the user terminal (3) COTS being operatively connected to the transfer server (4) through a communication channel available at least for the time necessary to complete the work session;
- rendering available, by the transfer server (4), the stream of output images (206) to the user terminal (3) COTS,
- displaying, by the user terminal (3) COTS, the stream of output images (206).

16. The method according to any of the claims from 10 to 14, comprising the following steps:

- providing a transfer server (4), defining a protected workspace,
- encrypting and compressing, by the computer terminal (2), the images of the stream of output images (206), and sending, by the computer terminal (2), the stream of output images (206) to the transfer server (4),
- providing a user terminal (3) COTS connected via an open network to the computer terminal (2), the user terminal (3) COTS being operatively connected to the transfer server (4) through a communication channel available at least for the time necessary to complete the work session;
- rendering available, by the transfer server (4), the stream of output images (206) to the user terminal (3) COTS,
- decrypting and decompressing, by the user terminal (3) COTS, the output images of the stream of output images (206);
- displaying, by the user terminal (3) COTS, the stream of output images (206).

17. The method according to any of the claims from 10 to 16, comprising the following steps of:

- at the computer terminal (2),

  receiving a command signal (304) from the user terminal (3) COTS,
  generating a one-time password (306) in response to the command signal (304) and a request signal (307) to enter the one-time password for the user terminal (3) COTS;

- at the user terminal (3) COTS,

  generating and sending the command signal (304) to the computer terminal (2)
  receiving the one-time password (306) and sending the one-time password (306) back to the computer terminal (2), in response to the request signal (307) to enter the one-time password from the computer terminal (2),

the method further comprising the steps, by the computer terminal (2),

checking whether the one-time password (306) generated by the computer terminal (2) and the one-time password (306) sent back by the COTS user terminal (3) are consistent with each other and
sending the command signal (304) to the command-and-control platform (10) in response to

said checking.

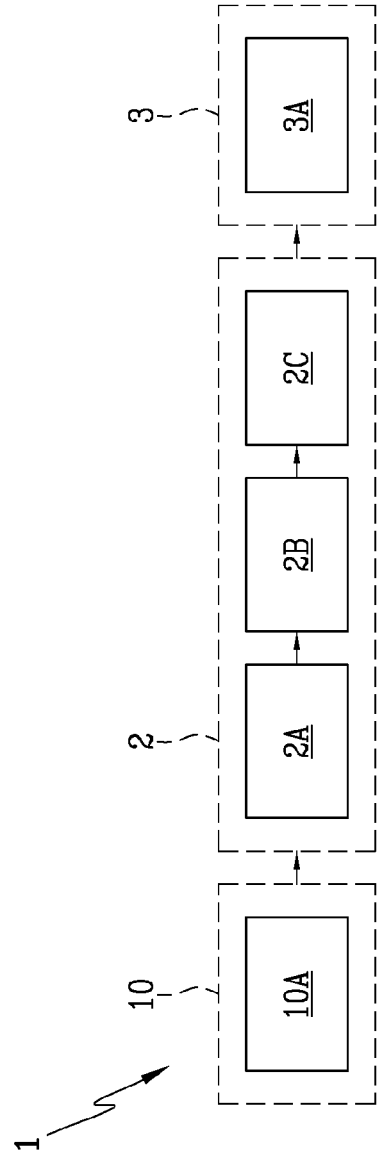

Fig.1

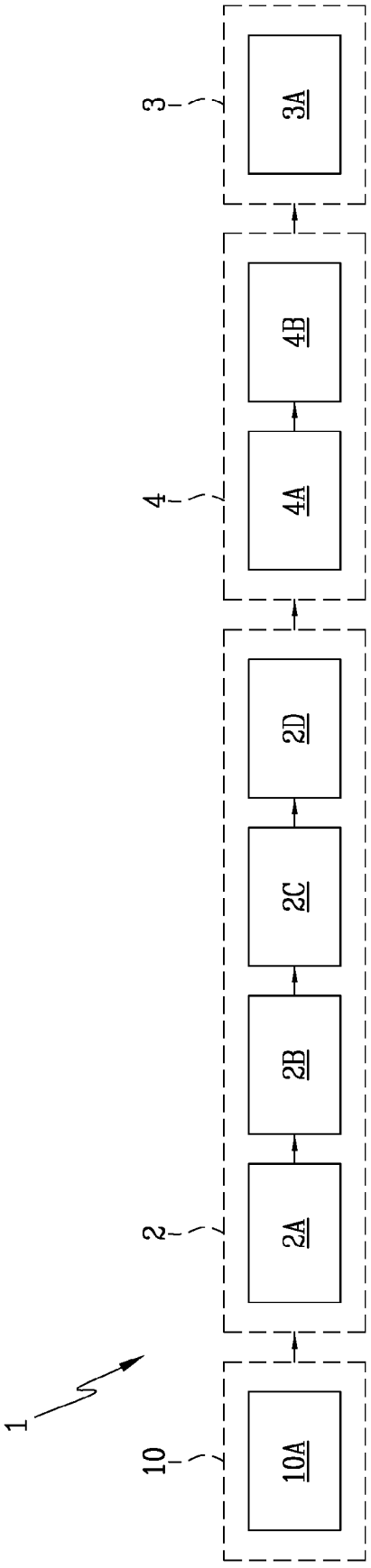

Fig.2

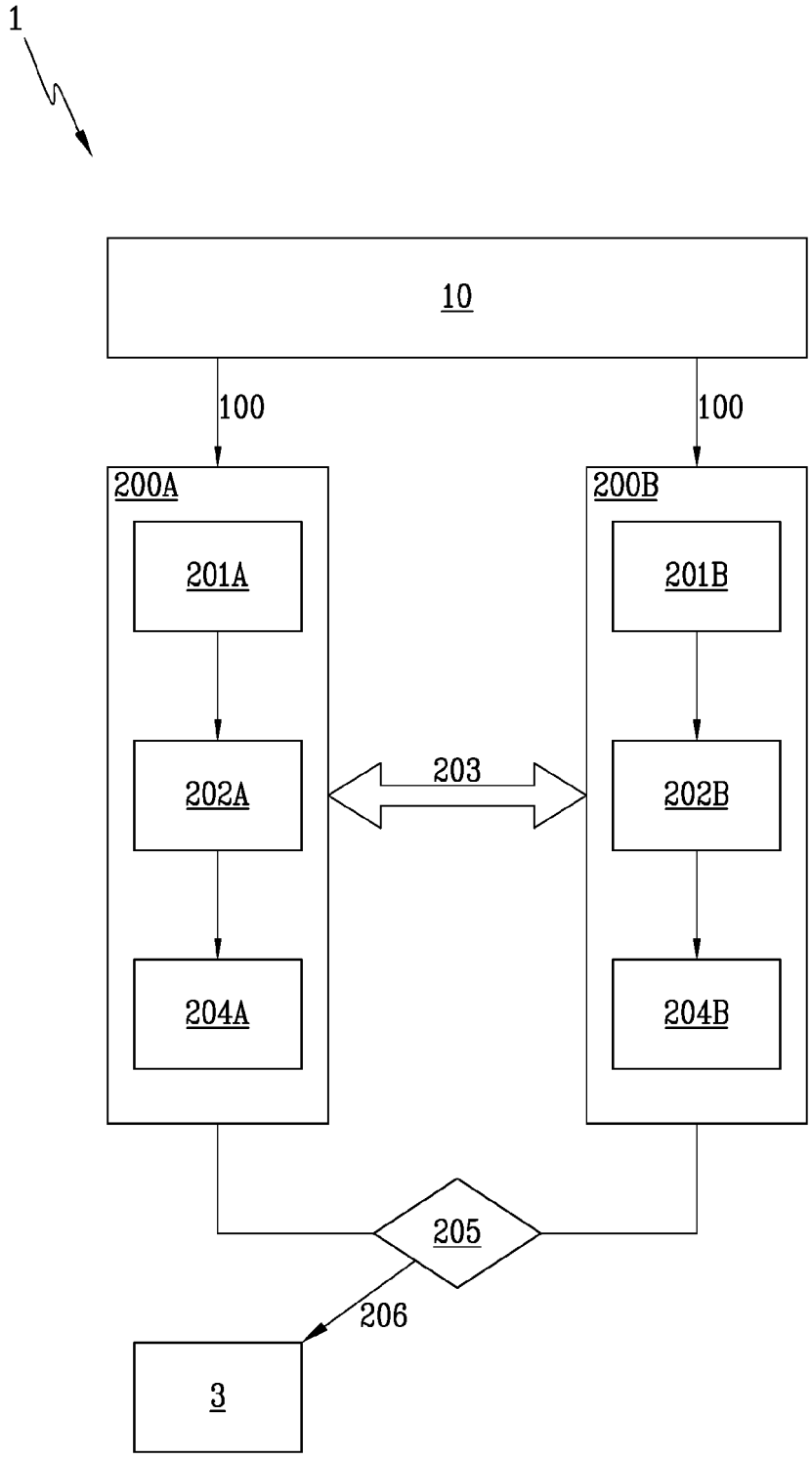
1
10
100
100
200A
200B
201A
201B
202A
203
202B
204A
204B
205
206
3

Fig.3

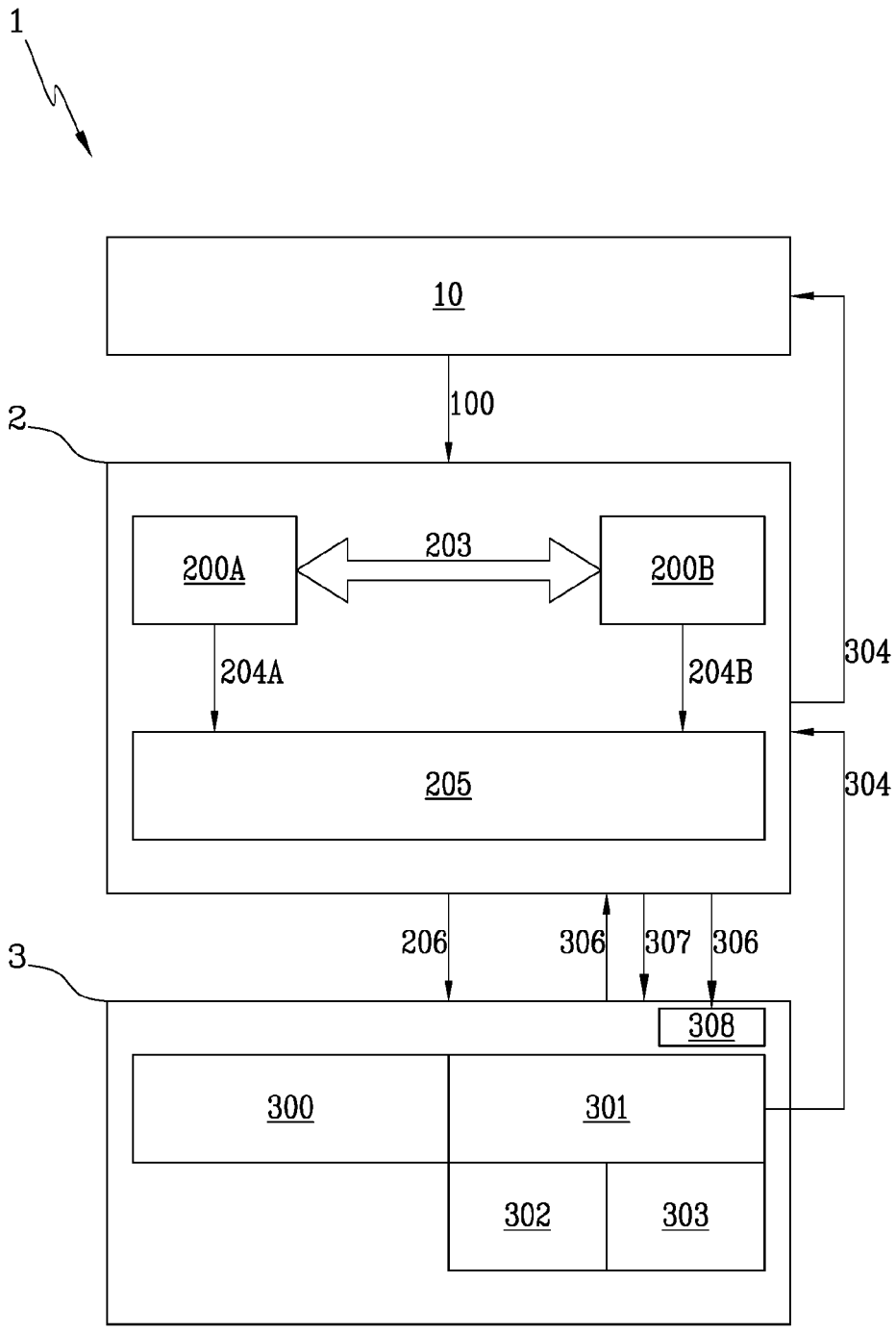
1
10
100
2
200A
203
200B
204A
204B
304
205
304
206
306
307
306
3
308
300
301
302
303

Fig.4

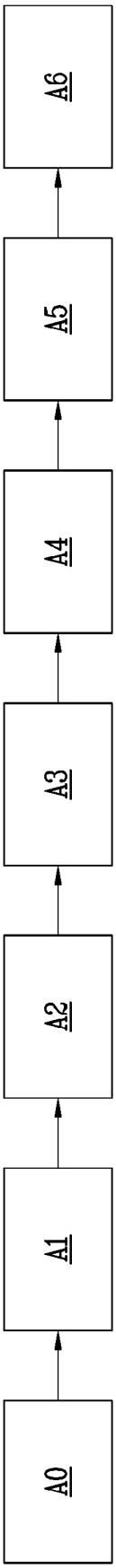

Fig.5

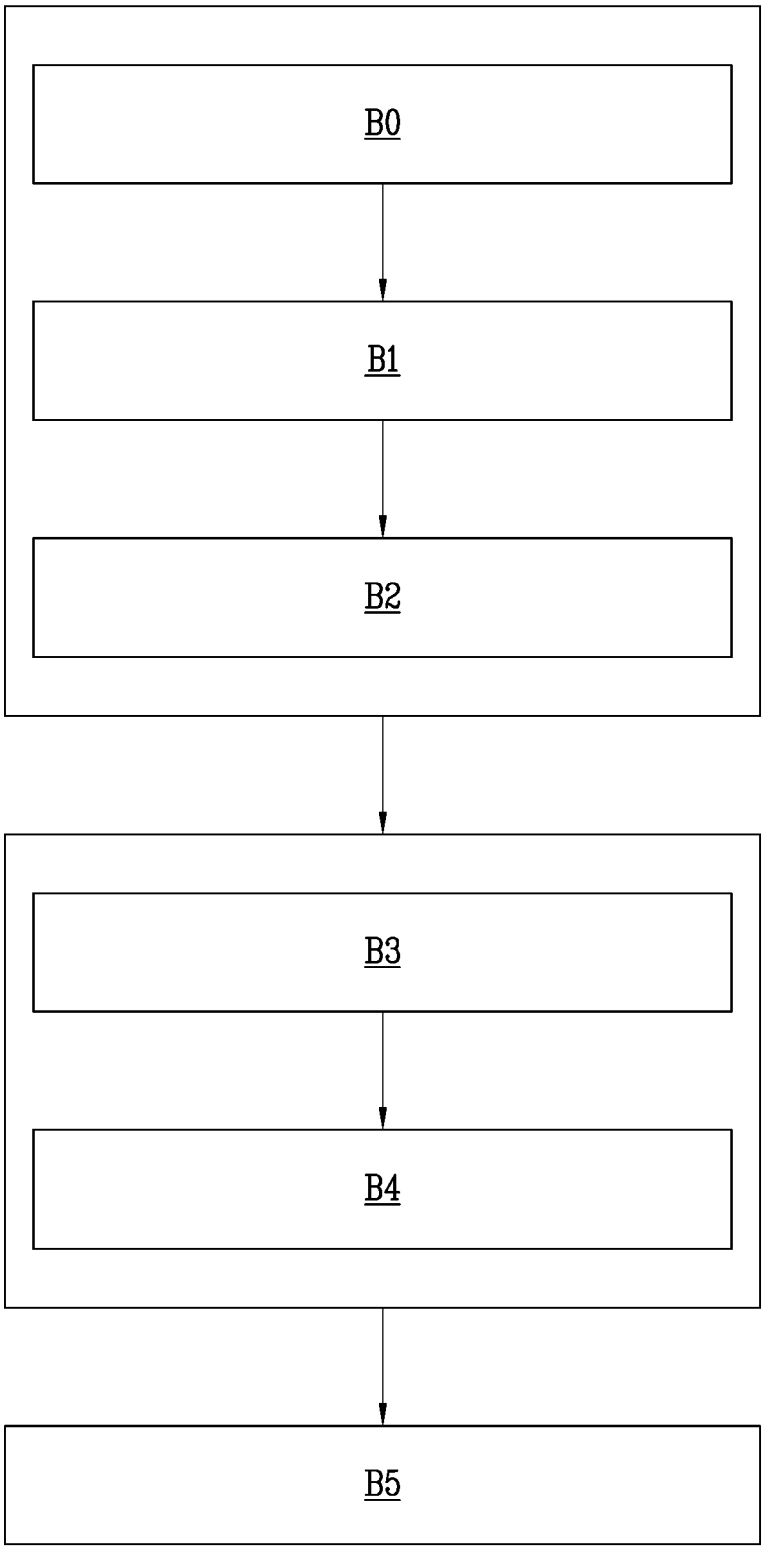

Fig.6

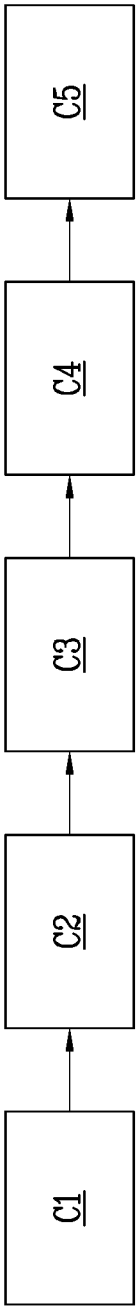

Fig.7

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 23 15 8266

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	IL 72 348 A (INT STANDARD ELECTRIC CORP [US]) 20 October 1987 (1987-10-20)	1-3,9-14	INV. B61L25/08
Y	* page 1, line 16- - page 2, line 4 * * page 2, line 14 - page 4, line 5 * * page 4, line 26 - page 6, line 17 * * page 8, line 10 - page 9, line 12 * * figure 1 * * page 7, lines 18-28 *	4-8, 15-17	B61L27/30
Y	"Railway applications - Communication, signalling and processing systems - Safety related communication in transmission systems", IEC 62280:2014, IEC, 3, RUE DE VAREMBÉ, PO BOX 131, CH-1211 GENEVA 20, SWITZERLAND, 6 February 2014 (2014-02-06), pages 1-132, XP082001126, * page 8 * * the whole document *	5,6,15, 16	
Y	EP 0 970 869 B1 (CIT ALCATEL [FR]) 22 March 2006 (2006-03-22) * figure 1 * * paragraph [0004] *	4	TECHNICAL FIELDS SEARCHED (IPC) B61L
Y	DE 44 32 419 A1 (SIEMENS AG [DE]) 7 March 1996 (1996-03-07) * claims 1, 5 * * abstract; figure * * column 2, line 9 - column 3, line 37 *	7,8,17	
A	WO 2012/025406 A1 (SIEMENS AG [DE]; THIEMANN JOERN [DE] ET AL.) 1 March 2012 (2012-03-01) * the whole document *	1-17	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	25 April 2023	Robinson, Victoria

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 23 15 8266

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

25-04-2023

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
IL 72348 A	20-10-1987	DE 3324313 A1	17-01-1985
		IL 72348 A	20-10-1987
		YU 111384 A	29-02-1988
		ZA 844956 B	27-02-1985
EP 0970869 B1	22-03-2006	AT 320954 T	15-04-2006
		DE 19830926 A1	13-01-2000
		EP 0970869 A2	12-01-2000
DE 4432419 A1	07-03-1996	DE 4432419 A1	07-03-1996
		NL 1001071 C2	20-04-1998
WO 2012025406 A1	01-03-2012	DE 102010036290 A1	01-03-2012
		WO 2012025406 A1	01-03-2012

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

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 3438828 B1 **[0007]**
- IT GE2011000034 **[0008]**
- IL 72348 A **[0009]**
- EP 0970869 B1 **[0010]**
- DE 4432419 A1 **[0010]**