



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
14.12.2022 Bulletin 2022/50

(51) International Patent Classification (IPC):
B61L 27/00 (2022.01) **B61L 27/02** (2006.01)

(21) Application number: **21305805.0**

(52) Cooperative Patent Classification (CPC):
B61L 27/02; B61L 27/30

(22) Date of filing: **11.06.2021**

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

(71) Applicant: **ALSTOM Transport Technologies**
93400 Saint-Ouen (FR)

(72) Inventor: **SCHETTINI, Gianluca**
70026 MODUGNO (BA) (IT)

(74) Representative: **Lavoix**
2, place d'Estienne d'Orves
75441 Paris Cedex 09 (FR)

(54) **SYSTEM FOR LOCALLY MANAGING RAILWAY TRAFFIC IN RAILWAY STATIONS**

(57) A system for locally managing railway traffic in a railway station, comprising at least:

- a field device installed in or operatively associated with the railway station;
- a human-machine interface configured for displaying to an operator fail-safe information indicative of the current operative status of the field device and for outputting an instruction signal indicative of fail-safe instructions, inputted by an operator, to be executed by the field device;
- a first control interface which is configured to acquire a first input signal indicative of the current operative status of the field device and to output towards the human-machine-interface a first output signal indicative of the current operative status of the field device to be displayed by the human-machine interface, the first control interface being further configured to output towards the field device, based on a fail-safe instruction inputted by said operator into the human-machine-interface, a command signal indicative of the inputted fail-safe instruction to be executed by the field device;
- a first control system configured to execute a predefined first control logic and generate a first check signal based on the first output signal outputted by the first control interface towards the human-machine-interface or a second check signal based on the instruction signal outputted by the human machine interface;
- a second control system configured to execute a predefined second control logic and generate a third check signal based on the first output signal outputted by the first control interface towards said human-machine-interface or a fourth check signal based on the instruction signal outputted by the human machine interface; and
- a communication interface configured to output towards the first control interface a first confirmation signal enabling the first control interface to output towards the field device the command signal indicative of the fail-safe in-

struction to be executed by the device only if the second and fourth check signals are consistent to each other, and to output towards the human machine interface a second confirmation signal enabling the display by the human-machine interface of the actual status of the field device only if the first and third check signals are consistent to each other.

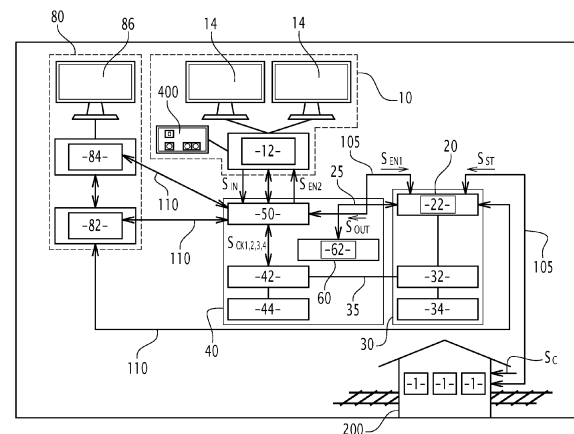


FIG.1

Description

[0001] The present invention concerns a system for locally managing railway traffic in railway stations, in particular in minor or local area railway stations.

[0002] As known, railways stations are equipped with different types of field devices, such as point machines, track circuits, level crossings, light signals, et cetera, which should be properly managed in order to guarantee the proper functioning of the station and of the railway line along which the station is installed.

[0003] In case of large stations, where the number of available tracks is considerably high, the number of field devices used is correspondingly high and their management requires the implementation of a rather complex and sophisticated control architecture in terms of software and hardware parts used and related interoperability.

[0004] In particular, nowadays field devices of large stations are managed using a central logic computer (CLC) which manages suitable interlocking rules to operate the equipment on the field according to the highest possible safety standards; to this end, known CLCs are configured to operate as a redundant reactive fail-safe machine, namely the components devised to manage the field devices are duplicated to form a normally operating machine and a second substantially identical back-up machine which is used only if there is any failure of the normally operating machine.

[0005] While this known control architecture allows an effective management of large stations, in case of small stations its implementation leads to a substantial oversizing of the overall control architecture.

[0006] Indeed, small stations, e.g. stations installed along secondary or local railways lines or locations, includes a reduced number of tracks, e.g. up to a very few units, and the number of field devices used is correspondingly very limited when compared with that of large or main stations which include several main and parallel tracks, e.g. up to some tens.

[0007] A solution alternative to that of replicating the control architecture used in large stations also locally in small ones, foresees to manage remotely the field devices installed in a small station by exploiting the control system installed remotely in a large station.

[0008] However, in this case if for whatever reason the operative connection between the small station and the associated large station is lost, then it will not be possible to properly operate the small station until the operative connection is re-established.

[0009] Hence, as evident from the above, there is still room and desire for further improvements about the way railway traffic is managed especially at small or local railway stations, and more in particular on how field devices therein installed are controlled to this end.

[0010] Therefore, it is a main aim of the present invention to fulfill at least partially such room and desire, and in particular to provide a solution for managing traffic in

railways stations, wherein field devices are locally managed according to a simplified control architecture particularly suitable for small or local stations.

[0011] This aim is achieved by a system for managing traffic at a railway station, characterized in that it comprises at least:

- at least one field device which is installed in or is operatively associated with the railway station;
- a human-machine interface which is configured for displaying to an operator at least fail-safe information indicative of the current operative status of the at least one field device and for outputting an instruction signal indicative of one or more fail-safe instructions, inputted by an operator, to be transmitted to and executed by the at least one field device;
- at least a first control interface which is configured at least to acquire a first input signal indicative of the current operative status of said at least one field device and to output towards said human-machine-interface a first output signal indicative of the current operative status of the at least one field device to be displayed by the human-machine interface, the first control interface being further configured to output towards said at least one field device, based on a fail-safe instruction inputted by said operator into the human-machine-interface, a command signal indicative of the inputted fail-safe instruction to be executed by the at least one field device;
- a first control system configured to execute a predefined first control logic and generate a first check signal based on said first output signal outputted by the first control interface towards said human-machine-interface or a second check signal based on said instruction signal outputted by the human machine interface;
- a second control system configured to execute a predefined second control logic and generate a third check signal based on said first output signal outputted by the first control interface towards said human-machine-interface or a fourth check signal based on said instruction signal outputted by the human machine interface; and
- a communication interface configured to output towards the first control interface a first confirmation signal enabling the first control interface to output towards said at least one field device said command signal indicative of the fail-safe instruction inputted to be executed by the at least one field device only if said second and fourth check signals are consistent to each other, and to output towards the human machine interface a second confirmation signal enabling the display by the human-machine interface of the actual status of the at least one field device only if said first and third check signals are consistent to each other.

[0012] According to some embodiments, the system

for managing traffic at a railway station according to the invention may comprise one or more of the following features, which may be combined in any technical feasible combination:

- the first control system comprises at least a first elaboration unit and a first software module which includes coded instructions that, when executed by said first elaboration unit, cause the first elaboration unit to execute said predefined first control logic;
- the second control system comprises at least a second elaboration unit and a second software module which includes coded instructions that, when executed by said second elaboration unit, cause the second elaboration unit to execute said predefined second control logic;
- the first control interface is configured to generate said first output signal and said command signal by executing one or more predetermined elaboration steps;
- the first control interface is embedded into said first control system;
- the first control interface is constituted by or comprises a software module which includes coded instructions executed by said first processing unit;
- the software module of the first control interface comprises a software Boolean engine configured to generate said first output signal and said command signal in the form of Boolean logic signals;
- the locally managing system comprises a second control interface which is adapted to verify if said first control interface executed correctly said one or more predetermined elaboration steps;
- the second control interface is embedded into said second control system;
- the communication interface is embedded into one of said first and second control system;
- the communication interface is further configured:
 - to output, to the human-machine-interface a signal adapted to display for a user an information representing the existence of an error condition related to the first input signal acquired by the first control interface if said first and third check signals are inconsistent to each other; and/or
 - to invalidate said command signal indicative of the fail-safe instruction inputted in the human-machine-interface by an operator, preventing the first control interface from outputting said command signal towards the at least one field device, if said second and fourth check signals are inconsistent to each other;
- the locally managing system further comprises a third control interface which is configured at least:
 - to acquire a further input signal indicative of the current operative status of the at least one field

device 1 and to output towards the human-machine-interface a further output signal indicative of the acquired operative status of the at least one field device to be displayed by the human-machine-interface for an operator; and,

- to output towards the at least one field device, based on a fail-safe instruction inputted by an operator into the human-machine-interface, a further command signal indicative of the inputted fail-safe instruction to be executed by the at least one field device 1.

- the third control interface is further configured to verify if said first control interface executed correctly one or more predetermined elaboration steps.

[0013] Further characteristics and advantages will become apparent from the description of some preferred but not exclusive exemplary embodiments of a local managing system according to the present disclosure, illustrated only by way of non-limitative examples with the accompanying drawings, wherein:

Figure 1 is a schematic block diagram showing a possible embodiment of a system for locally managing railway traffic in a railway station according to the invention;

Figure 2 is a schematic block diagram showing a further possible embodiment of a system for locally managing railway traffic in a railway station according to the invention.

[0014] It should be noted that in the detailed description that follows, identical or similar components, either from a structural and/or functional point of view, have the same reference numerals, regardless of whether they are shown in different embodiments of the present disclosure; it should also be noted that in order to clearly and concisely describe the present disclosure, the drawings may not necessarily be to scale and certain features of the disclosure may be shown in somewhat schematic form.

[0015] Further, when the term "adapted" or "arranged" or "configured" or "shaped", is used herein while referring to any component as a whole, or to any part of a component, or to a combination of components, it has to be understood that it means and encompasses correspondingly either the structure, and/or configuration and/or form and/or positioning of the related component or part thereof, or combinations, such term refers to.

[0016] In particular, for electronic and/or software means, each of the above listed terms means and encompasses electronic circuits or parts thereof, as well as stored, embedded or running software codes and/or routines, algorithms, or complete programs, suitably designed for achieving the technical result and/or the functional performances for which such means are devised.

[0017] Further, in the following description and claims,

the numeral ordinals first, second, third et cetera..., will be used only for the sake of clarity of description and in no way they should be understood as limiting for whatsoever reason; in particular, the indication for instance of the "third signal..." does not imply necessarily the presence or strict need of the preceding "first" or "second" signals, unless such presence is clearly evident for the correct functioning of the relevant embodiment(s) described, nor that the order should be the one exactly in the cardinal sequence described with reference to the illustrated exemplary embodiment(s).

[0018] Figures 1 and 2 schematically illustrate a system, indicated by the overall reference number 100, which is locally installed at and is suitable for managing railway traffic in an associated railway station, notably a local area or small railway station, schematically represented in figures 1 and 2 with the reference number 200.

[0019] As illustrated, the local managing system 100 according to the invention comprises at least one field device, schematically represented by the reference number 1, which is installed in or is operatively associated with the railway station 200 and is under the control of the local managing system 100 itself.

[0020] Clearly, even if the railway station 200 is a local or small one and therefore comprises a number of field devices substantially reduced with respect to main or bigger stations, it can comprise anyhow a certain number of field devices 1, such as point machines, track circuits, level crossings, light signals, et cetera; therefore, what described in the following about one field device 1 has to be understood as applicable in the same way to all field devices 1 installed in or operatively associated with the railway station 200 which are under the control of the local managing system 100.

[0021] The system 100 according to the invention further comprises a human-machine interface, indicated in figures 1 and 2 by the overall reference number 10, hereinafter referred to also as the "HMI" 10, which is configured for displaying to an operator at least fail-safe information indicative of the current operative status of the at least one field device 1 and for outputting an instruction signal S_{IN} indicative of one or more fail-safe instructions, inputted by an operator, to be transmitted to and executed by the at least one field device 1.

[0022] With the definition of fail-safe information or instructions, it has to be understood hereby a type of displayed information or inputted instruction that if erroneous or failing would cause unsafe or harmful conditions to people or equipment once accepted or executed; against this type of potential error or failure, and in the way that will result more in details in the following description, the system 100 or part thereof is designed to inherently prevent or mitigate unsafe consequences, for example by timely identifying such potential error or failure, and then properly warning an operator and/or maintaining the relevant operative status at least as safe as it was before accepting the potentially erroneous information or before executing a potentially erroneous in-

struction.

[0023] According to solutions well known in the art or readily available to those skilled in the art, and thus not described herein in details, the HMI 10 comprises for example an operator console and one or more video displays, schematically illustrated in the exemplary embodiments of figures 1 and 2 by the reference numbers 12 and 14, respectively.

[0024] Usefully, the system 100 according to the invention further comprises at least a first control interface 20 which is configured at least:

- to acquire a first input signal S_{st} indicative of the current operative status of the at least one field device 1 and to output towards the HMI 10 a first output signal S_{out} indicative of the current operative status of the at least one field device 1 to be displayed by the HMI 10 for the attention of an operator; and
- to output towards the at least one field device 1, based on a fail-safe instruction inputted by an operator into the HMI 10, e.g. via the console 12, a command signal S_c indicative of the inputted fail-safe instruction to be executed by the at least one field device 1.

[0025] Further, the system 100 comprises at least:

- a first control system, indicated by the overall reference number 30, which is configured to execute a predefined first control logic and generate a first check signal S_{CK1} based on the first output signal S_{out} outputted by the first control interface 20 towards the HMI 10, or a second check signal S_{CK2} based on said instruction signal S_{IN} outputted by the HMI 10; and
- a second control system, indicated by the overall reference 40, which is configured to execute a predefined second control logic and generate a third check signal S_{CK3} based on the first output signal S_{out} outputted by the first control interface 20 towards the HMI 10, or a fourth check signal S_{CK4} based on said instruction signal S_{IN} outputted by the HMI 10.

[0026] In particular, according to the exemplary embodiment illustrated in the figures, the first control system 30 comprises at least a first elaboration unit 32 and a first software module 34, wherein the first software module 34 includes coded instructions that, when executed by the first elaboration unit 32 cause the first elaboration unit 32 to execute said predefined first control logic and generate a first check signal S_{CK1} based on the first output signal S_{out} outputted by the first control interface 20 towards the HMI 10, or a second check signal S_{CK2} based on said instruction signal S_{IN} outputted by the HMI 10; In turn, the second control system 40 comprises at least a second elaboration unit 42 and a second software module 44, wherein the second software module 44 includes coded instructions that, when executed by the second

elaboration unit 42 cause the second elaboration unit 42 to execute said predefined second control logic and generate a third check signal S_{CK3} based on the first output signal S_{out} outputted by the first control interface 20 towards the HMI 10, or a fourth check signal S_{CK4} based on said instruction signal S_{IN} outputted by the HMI 10.

[0027] As illustrated in figures 1 and 2, the two control systems 30 and 40 are operatively linked to each other via a link 35, namely a link internal to the system 100.

[0028] In one possible example, the first control system 30 and the second control system 40 are for example constituted by or comprise each a corresponding server 30 and respectively 40, such servers being for example servers already installed in the railway station 200 and used for purposes other than those foreseen within the frame of the present invention.

[0029] Accordingly, the respective first and second elaboration units 32 and 42 are formed or comprise each a corresponding processor device of such servers, and the first and second software modules 34 and 44 can be stored in memory or equivalent storage units of the servers 30, 40 themselves.

[0030] As illustrated in figures 1 and 2, the system 100 comprises a communication interface 50 which is configured:

- to output towards the first control interface 20 a first confirmation signal S_{EN1} enabling the first control interface 20 to actually output towards the at least one field device 1 said command signal S_c indicative of the fail-safe instruction inputted in the HMI 10 and to be executed by the field device 1 itself, only if the second and fourth check signals S_{CK2} and S_{CK4} are consistent to each other; and/or
- to output towards the HMI 10 a second confirmation signal S_{EN2} enabling the display by the human-machine interface of the actual status of the at least one field device 1 only if said the first and third check signals S_{CK1} and S_{CK3} are consistent to each other.

[0031] With the definitions of "first and third check signals S_{CK1} and S_{CK3} consistent to each other" or correspondingly of "second and fourth check signals S_{CK2} and S_{CK4} consistent to each other", it is hereby meant that the information or informative content carried by such check signals should not be incoherent to each other, i.e. not substantially differing or even in contrast; in particular, such content should be in one possible embodiment identical to each other.

[0032] For example, following a first output signal S_{out} outputted by the first control interface 20 and received by both control systems 30 and 40, via the communication interface 50, a first check signal S_{CK1} generated by the first control system 30 indicating that a certain light signal S_1 is in a green status would be coherent with a third check signal S_{CK3} generated by the second control system 40 also indicating that the same light signal S_1 is in a green status.

[0033] On the contrary, if for example the third check signal S_{CK3} generated by the second control system 40 following the same first output signal S_{out} emitted by the first control interface 20 would indicate that the light signal S_1 is in a red status or that a different light signal S_2 is in a green status, then the first and third check signals S_{CK1} and S_{CK3} would be inconsistent.

[0034] Likewise, based on an instruction signal S_{IN} outputted via the HMI 10 indicating that a level crossing L1 should pass from "closed" to "opened", a second check signal S_{CK2} generated by the first control system 30 would be coherent with a fourth check signal S_{CK4} generated by the second control system 40 based on the same instruction signal S_{IN} received also by the second control system 40, if such fourth check signal S_{CK4} would also indicate that the level crossing L1 should pass from "closed" to "opened".

[0035] On the contrary, if for example the fourth check signal S_{CK4} generated by the second control system 40 based on the same received instruction signal S_{IN} would indicate that the level crossing L1 should remain "closed" or should pass from "opened" to "closed", then the second and fourth check signals S_{CK2} and S_{CK4} would be inconsistent to each other.

[0036] In particular, according to a possible embodiment, the communication interface 50 is further configured:

- to output, to the HMI 10 a signal adapted to display for a user, for example on one of the video displays 14, an information visually representing the existence of an error condition related to the signal S_{st} acquired by the first control interface 20 if said first and third check signals S_{CK1} and S_{CK3} are inconsistent to each other; and/or
- to invalidate the command signal S_c indicative of the fail-safe instruction inputted in the HMI 10 by an operator, thus preventing the first control interface 10 from outputting such command signal S_c towards the at least one field device 1, if said second and fourth check signals S_{CK2} and S_{CK4} are inconsistent to each other.

[0037] For example, if said first and third check signals S_{CK1} and S_{CK3} are inconsistent to each other, then the communication interface 50 can output a signal resulting in a corrupted image displayed on one of the monitors 14, thus visually and clearly highlighting to an operator the occurrence of such erroneous condition. For example, for a light signal such image can be constituted by a stain or patch of a color and/or form clearly unrelated to the usual or standard colors and/or forms used for displaying the current status of such light signal.

[0038] In turn, the control signal S_c can be invalidated by the communication interface 50, for example by sending to the first control interface 20 an inhibiting signal which remains valid until the erroneous condition is not solved after a certain number of iterations, or if such er-

roneous condition continues, until when this erroneous condition is otherwise solved by a maintenance intervention on the equipment of the system 100 causing it.

[0039] According to a possible embodiment, the communication interface 50 is further configured to submit to an operator, who has inputted into the HMI 10 an instruction to be confirmed and executed using a safe device for confirmation 400, thus causing the generation of the corresponding signal S_{IN} indicative of one or more fail-safe instructions to be transmitted to and executed by the at least one field device 1, a verification check requesting the operator to reconfirm if the inputted instruction, using the safe device for confirmation 400, reflects the true intention of the operator and should be effectively processed and in case executed.

[0040] Only after the operator has positively replied to the verification check, then the communication interface 50 can allow the instruction signal S_{IN} to be routed ahead and be properly processed first by the control systems 30 and 40 in the manner and for the scope previously described, and thereafter finally elaborated and outputted by the first control interface 20, in the elaborated form of the Boolean command signal S_c towards the relevant field device 1.

[0041] The verification check can be realized for instance via a simple question displayed on one of the video displays 14 to the attention of the operator.

[0042] In one possible embodiment, the first control interface 20 is configured to generate the first output signal S_{out} or the command signal S_c by executing one or more predetermined elaboration steps, following the reception in input from the communication interface 50 of the first confirmation signal S_{EN1} , or respectively following the acquisition in input of the first input signal S_{st} indicative of the current operative status of the at least one field device 1.

[0043] Communications between the first control interface 20 and the various field devices 1, as well as between the communication interface 50 and the first control interface 20 is realized by connections means 105 using for example a vital or fail-safe field bus.

[0044] According to a possible embodiment, the communication network realized by the connections means 105 is external to the components/parts of the system 100.

[0045] Conveniently, in one possible embodiment, the system 100 further comprises a second control interface 60, operatively linked with the first control interface 20, which is adapted to verify if the first control interface 20 executed correctly the one or more predetermined elaboration steps, i.e. it followed the exact and predetermined sequence of elaboration steps.

[0046] As illustrated in figures 1 and 2, the first and second control interfaces 20 and 60 are operatively linked to each other via a link 25, namely a link internal to the system 100 itself.

[0047] In this case, the first control interface 20 informs, via the link 25, the second control interface 60 that it has

completed the sequence of elaboration steps and thus the second control interface 60 is triggered to check if the first control interface 20 operated correctly and in particular followed exactly the predetermined sequence.

[0048] In one possible embodiment, the first control interface 20 is embedded into the first control system 30.

[0049] In particular, according to the embodiments illustrated in figures 1 and 2, the first control interface 20 is constituted by or comprises a software module 22 which is embedded for example into a memory or storage unit of the first control system 30, e.g. in its server, and contains coded instructions which are executed by the first processing unit 32.

[0050] According to a possible embodiment, the software module 22 of the first control interface 20 comprises a software Boolean engine 22 configured to generate the first output signal S_{out} and the command signal S_c in the form of Boolean logic signals.

[0051] In one possible embodiment, the second control interface 60 is embedded into the second control system 40.

[0052] In particular, according to the embodiments illustrated in figures 1 and 2, the second control interface 60 is constituted by or comprises a software module 62 which is embedded for example into a memory or storage unit of the second control system 40, e.g. in its server, and contains coded instructions which are executed by the second processing unit 42.

[0053] According to a possible embodiment, also the software module 62 of the second control interface 60 comprises a software Boolean engine 22 configured to generate signals in the form of Boolean logic signals.

[0054] In turn, according to a possible embodiment, the communication interface 50 is embedded into one of the first and second control system 30, 40.

[0055] In one possible embodiment, the communication interface 50 is constituted by or comprises a software module 52 which includes coded instructions executed by the first processing unit 32 or by the second processing unit 42.

[0056] In the exemplary embodiments illustrated in figures 1 and 2, the communication interface 50 is embedded into the second control system 40, e.g. it is stored in a storage or memory unit of the server 40, and the coded instructions of its software module 52 are executed by the second processing unit 42.

[0057] In practice, according to this embodiment, the communication interface 50 receives directly the signals to be transmitted from the HMI 10 or from the first control interface 20, which signals are shared, via the internal link 35, by the first and second control systems 30 and 40 which process them in order to generate the corresponding check signals.

[0058] Then, if the check signals are consistent to each other as above indicated, then the communication interface 50 outputs towards the first control interface 20 the first enabling signal S_{EN1} or towards the human machine interface 10 the second enabling signal $SEN2$.

[0059] In an exemplary embodiment illustrated in figure 2, the system 100 according to the invention comprises a third control interface 70, which is operatively linked to the first and second control interfaces 20, 60 and to the communication interface 50.

[0060] The control interface 70 is used in order to provide the system 100 with an adequate redundancy, for example to replace at least the first control interface 20 if it does not function properly.

[0061] In particular, the control interface 70 is configured, likewise the first control interface 20, at least:

- to acquire a further input signal S_{st} indicative of the current operative status of the at least one field device 1 and to output towards the HMI 10 a further output signal S_{out} indicative of the acquired operative status of the at least one field device 1 to be displayed by the HMI 10 for the attention of an operator; and
- to output towards the at least one field device 1, based on a fail-safe instruction inputted by an operator into the HMI 10, e.g. via the console 12 and confirmed using the safe device for confirmation 400, a further command signal S_c indicative of the inputted fail-safe instruction to be executed by the at least one field device 1.

[0062] According to this embodiment, the third control interface 70 is an entity separated from the first and second control interfaces 20 and 60 and comprises an own further processing unit 72 and at least a further software module 74 which includes coded instructions executed by said further processing unit 72.

[0063] In particular, the further software module 74 of the third control interface 70 comprises a software Boolean engine 74 configured to generate the further output signal S_{out} and said further command signal S_c in the form of Boolean logic signals.

[0064] Conveniently, in a possible embodiment, the third control interface 70 is further configured to verify, in the same manner as done by the second control interface 60, if the first control interface 20 executed correctly the one or more predetermined elaboration steps; to this end, the control interface 70 can be provided with the same software module 62 of the second control interface 60.

[0065] In this way, in normal operating conditions, i.e. when the first control interface 20 and the second control interface 60 are each properly working, the third control interface 70 is in a sleeping mode, while it can replace either the first control interface 20 or the second control interface 60 if any of them malfunctions.

[0066] The communications between the third control interface 70 with the first control interface 20, the communication interface 50, and the various field devices 1, is also realized by connections means 105 using for example a vital or fail-safe field bus, which are external to the components/parts of the system 100. Further, as illustrated in figure 2, the third control interface 70 is operatively linked with the first and second control interfac-

es 20 via a respective link 75, 76, namely two corresponding links internal to the system 100 itself.

[0067] According to a possible embodiment, and as illustrated in figure 1, the system 100 comprises an additional control system 80 which includes for example a server 82, a workstation 84 and a monitor 86. The control system 80 is configured to exchange with said communication interface 50, for example some basic or non fail-safe data related to the railway traffic in the station 200 to be displayed by the HMI 10. Such non-fail-safe data can include for instance information about the identification number and routes of trains going to transit from the station 200, et cetera. The control system 80 can be in operative communication with the first control interface 20, in order for example to send to it non fail-safe or non safety-related command or control signals.

[0068] To this end, the communication between the system 80 and the communication interface 50 and/or the first communication interface 20 is realized by connections 110 using for example a non-vital field bus.

[0069] In the system 100 according to the invention, also this type of basic information can be conveyed by the communication interface 50 to the first and second control system 30 and 40 in order for them to elaborate the information received and output each a corresponding further checking signal. Also in this case, the information received from the control system 80 can be displayed on the HMI 10 only if such two further checking signals are consistent to each other.

[0070] In an alternative embodiment illustrated in figure 2, the HMI 10 can be configured to integrate also the functionalities executed by the additional control system 80, thus allowing to input and visualize directly on one of its video display 14, also these basic or non-fail safe data or information, as well as any other non-fail safe related commands or controls.

[0071] Hence, it is evident from the foregoing description that the system 100 according to the present invention achieves the intended aim and objects since it allows to manage traffic, and in particular to control field devices, especially at small stations, according to a simplified architecture.

[0072] Indeed, with respect to known solutions, the system 100 allows sparing in particular hardware parts and also connections with a remote central logic computer, thus reducing at the same time the burden of the logic motor executed by the remote central logic computer itself; in particular, where available, the system 100 can additionally exploit hardware components/parts already installed in small stations for other purposes, such as the servers 30 and 40 which can be properly configured, via the use of the described software modules, to implement the functionalities foreseen within the frame of the present invention for the limited environment of a small station.

[0073] This solution is achieved satisfying at the same the highest standards of safety. Indeed, the two control systems 30, 40 realize a "composite fail-safe" two-out-

of-two (2oo2) protection architecture by verifying the consistency of the outputs provided by the HMI 10 and the first control interface 20. In addition, the second control interface 60 adds a further margin of safety by checking the correctness of the elaborations executed by the first control interface 20 and, when implemented, the third control interface 70 provides redundancy.

[0074] The system 100 thus conceived is susceptible of modifications and variations, all of which are within the scope of the inventive concept as defined in particular by the appended claims, and contemplates any possible combination of the embodiments or parts thereof hereinbefore described; for example, it is possible to use the third control interface 70 also in the embodiment of figure 1, and in such a case the additional control system 80 can be operatively connected also to it via a further connection 110 using for example a vital or fail-safe field bus. In relation to the specific application, some of the components or parts described, can be shaped or positioned differently from what described, or there could be a number of components different from that described; for example one or more of the first control interface 20, the second control interface 60 and the communication interface 50 can be realized as an entity separated from the respective first control system 30 and second control system 40 and can include an own processor for executing the coded instruction of the own software module 22, 52, 62. The described servers and/or elaboration or processing units can be constituted by, or comprise, any suitable server or processorbased device, e.g. a processor of a type commercially available, suitably programmed and provided to the extent necessary with circuitry, in order to perform the innovative functionalities devised for the system 100 according to the present invention, et cetera.

[0075] All the details may furthermore be replaced with technically equivalent elements.

Claims

1. A system (100) for locally managing railway traffic in a railway station (200), **characterized in that** it comprises at least:

- at least one field device (1) which is installed in or is operatively associated with the railway station (200);
- a human-machine interface (10) which is configured for displaying to an operator at least fail-safe information indicative of the current operative status of the at least one field device (1) and for outputting an instruction signal (S_{IN}) indicative of one or more fail-safe instructions, inputted by an operator, to be transmitted to and executed by the at least one field device (1);
- at least a first control interface (20) which is configured at least to acquire a first input signal

(S_{st}) indicative of the current operative status of said at least one field device (1) and to output towards said human-machine-interface (10) a first output signal (S_{out}) indicative of the current operative status of the at least one field device (1) to be displayed by the human-machine interface (10), the first control interface (20) being further configured to output towards said at least one field device (1), based on a fail-safe instruction inputted by said operator into the human-machine-interface (10), a command signal (S_c) indicative of the inputted fail-safe instruction to be executed by the at least one field device (1);

- a first control system (30) configured to execute a predefined first control logic and generate a first check signal (S_{CK1}) based on said first output signal (S_{out}) outputted by the first control interface (20) towards said human-machine-interface (10) or a second check signal (S_{CK2}) based on said instruction signal (S_{IN}) outputted by the human machine interface (10);
- a second control system (40) configured to execute a predefined second control logic and generate a third check signal (S_{CK3}) based on said first output signal (S_{out}) outputted by the first control interface (20) towards said human-machine-interface (10) or a fourth check signal (S_{CK4}) based on said instruction signal (S_{in}) outputted by the human machine interface (10); and
- a communication interface (50) configured to output towards the first control interface (20) a first confirmation signal (S_{EN1}) enabling the first control interface (20) to output towards said at least one field device (1) said command signal (S_c) indicative of the fail-safe instruction inputted to be executed by the at least one field device (1) only if said second and fourth check signals (S_{CK2} , S_{CK4}) are consistent to each other, and to output towards the human machine interface (10) a second confirmation signal (S_{EN2}) enabling the display by the human-machine interface (10) of the actual status of the at least one field device (1) only if said first and third check signals (S_{CK1} , S_{CK3}) are consistent to each other.

2. A system (100) according to claim 1, wherein said first control system (30) comprises at least a first elaboration unit (32) and a first software module (34) which includes coded instructions that, when executed by said first elaboration unit (34), cause the first elaboration unit (32) to execute said predefined first control logic.

3. A system (100) according to claim 1 or 2, wherein said second control system (40) comprises at least a second elaboration unit (42) and a second software module (44) which includes coded instructions that,

when executed by said second elaboration unit (42), cause the second elaboration unit (44) to execute said predefined second control logic.

4. A system (100) according to one or more of the previous claims, wherein said first control interface (20) is configured to generate said first output signal (S_{out}) and said command signal (S_c) by executing one or more predetermined elaboration steps. 10
5. A system (100) according to one or more of the previous claims, wherein said first control interface (20) is embedded into said first control system (30).
6. A system (100) according to one or more of the previous claims, wherein said first control interface (20) is constituted by or comprises a software module (22) which includes coded instructions executed by said first processing unit (32). 15
7. A system (100) according to claim 6, wherein said software module (22) of the first control interface (20) comprises a software Boolean engine (22) configured to generate said first output signal (S_{out}) and said command signal (S_c) in the form of Boolean logic signals. 20
8. A system (100) according to claim 4, wherein it further comprises a second control interface (60) which is adapted to verify if said first control interface (20) executed correctly said one or more predetermined elaboration steps. 30
9. A system (100) according to claim 6, wherein said second control interface (60) is embedded into said second control system (40). 35
10. A system (100) according to one or more of the previous claims, wherein said communication interface (50) is embedded into one of said first and second control system (30, 40). 40
11. A system (100) according to one or more of the previous claims, wherein said communication interface (50) is further configured: 45
 - to output, to the human-machine-interface (10) a signal adapted to display for a user an information representing the existence of an error condition related to the first input signal (S_{st}) acquired by the first control interface (20) if said first and third check signals (S_{CK1} , S_{CK3}) are inconsistent to each other; and/or 50
 - to invalidate said command signal (S_c) indicative of the fail-safe instruction inputted in the human-machine-interface (10) by an operator, preventing the first control interface (10) from outputting said command signal (S_c) towards 55

the at least one field device (1), if said second and fourth check signals (S_{CK2} , S_{CK4}) are inconsistent to each other.

12. A system (100) according to one or more of the previous claims, wherein it further comprises a third control interface (70) which is configured at least:
 - to acquire a further input signal (S_{st}) indicative of the current operative status of the at least one field device 1 and to output towards the human-machine-interface (10) a further output signal (S_{out}) indicative of the acquired operative status of the at least one field device (1) to be displayed by the human-machine-interface (10) for an operator; and,
 - to output towards the at least one field device (1), based on a fail-safe instruction inputted by an operator into the human-machine-interface (10) and confirmed by a safe device for confirmation (400), a further command signal (S_c) indicative of the inputted fail-safe instruction to be executed by the at least one field device 1.
13. A system (100) according to claim 12, wherein said third control interface (70) is further configured to verify if said first control interface (20) executed correctly one or more predetermined elaboration steps.

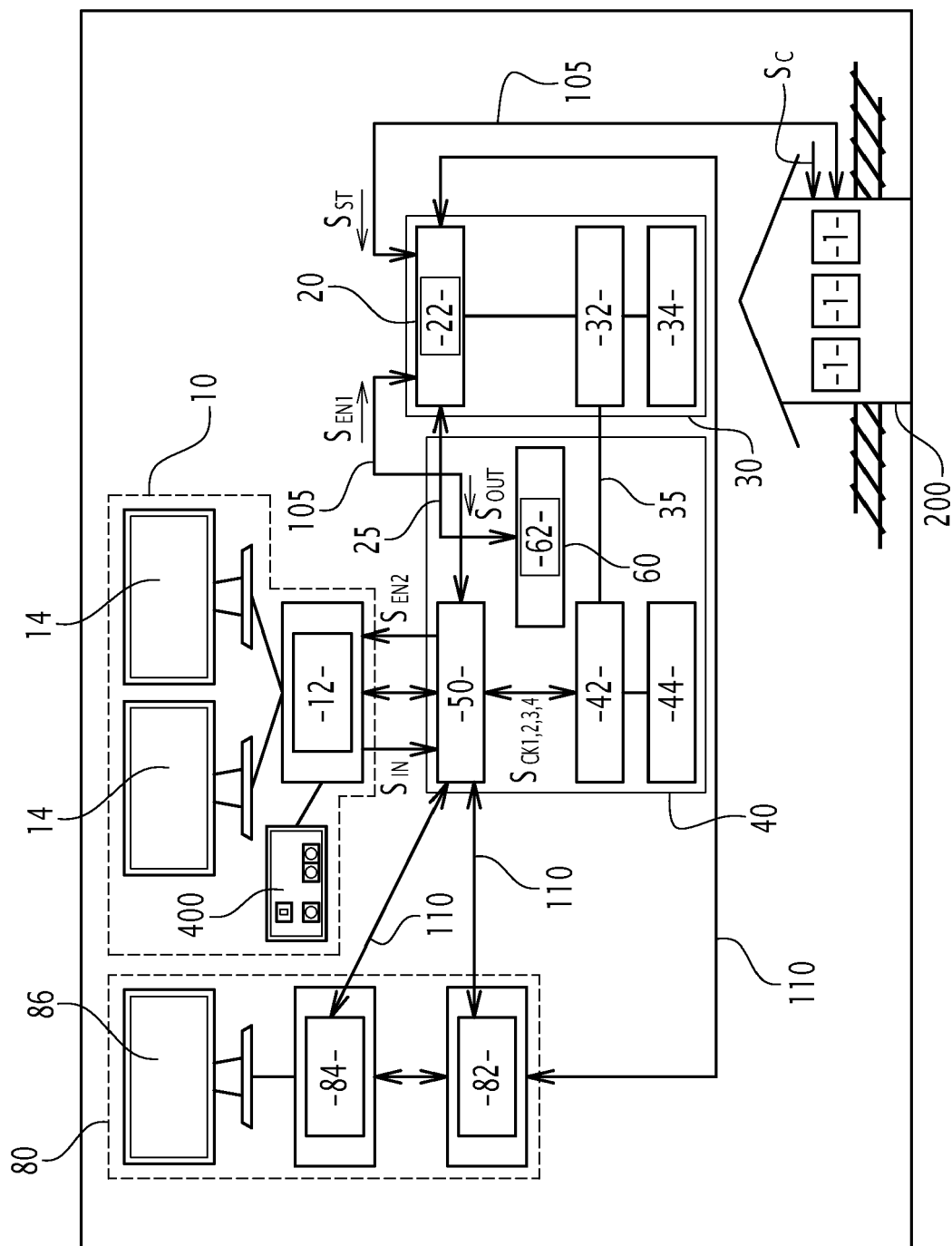


FIG.1

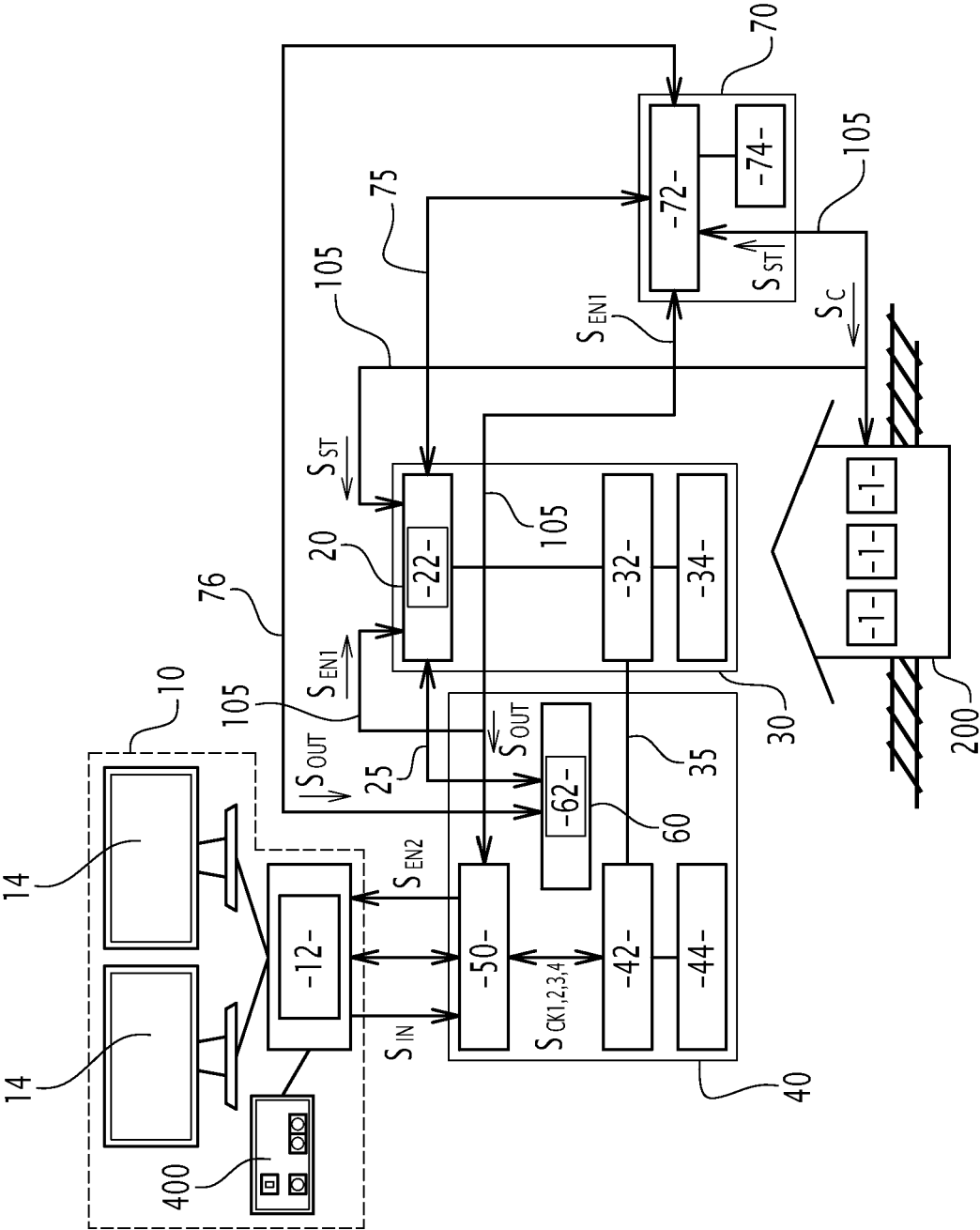


FIG. 2



EUROPEAN SEARCH REPORT

Application Number
EP 21 30 5805

5

10

15

20

25

30

35

40

45

50

55

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	ANDREAS LINHARDT: "Ein Konzept, viele Anwendungen & Der Doppelrechner A212 als sicheres Modul / One concept, multiple applications & the A212 double controller as a safe module", SIGNAL UND DRAHT: SIGNALLING & DATA COMMUNICATION, vol. 108, no. 1+2, 9 February 2016 (2016-02-09), pages 36-43, XP055249254, DE ISSN: 0037-4997 * page 36 - page 43; figures 1-4 *	1-13	INV. B61L27/00 B61L27/02
Y	US 2014/229040 A1 (WEBER CLAUS [US] ET AL) 14 August 2014 (2014-08-14) * paragraph [0005] - paragraph [0043]; figures 1-6 *	1-13	
Y	EP 3 608 200 A1 (CRSC RESEARCH & DESIGN INSTITUTE GROUP CO LTD [CN]) 12 February 2020 (2020-02-12) * paragraph [0007] - paragraph [0069]; figures 1-5 *	1-13	TECHNICAL FIELDS SEARCHED (IPC) B61L
The present search report has been drawn up for all claims			
Place of search Munich		Date of completion of the search 30 November 2021	Examiner Kassner, Holger
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	

 1
EPO FORM 1503 03.82 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 21 30 5805

5

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.

30-11-2021

10

15

20

25

30

35

40

45

50

55

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014229040 A1	14-08-2014	US 2014229040 A1	14-08-2014
		US 2016082994 A1	24-03-2016
		US 2017129515 A1	11-05-2017
		US 2018111634 A1	26-04-2018
		US 2019202486 A1	04-07-2019

EP 3608200 A1	12-02-2020	CN 108032876 A	15-05-2018
		EP 3608200 A1	12-02-2020
		WO 2019091063 A1	16-05-2019
