

(19)



(11)

EP 2 050 648 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:

22.04.2009 Bulletin 2009/17

(51) Int Cl.:

B61L 23/04 ^(2006.01)

G08B 21/18 ^(2006.01)

(21) Application number: **08166815.4**

(22) Date of filing: **16.10.2008**

(84) Designated Contracting States:

**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT
RO SE SI SK TR**

Designated Extension States:

AL BA MK RS

(30) Priority: **19.10.2007 NL 2000947**

(71) Applicant: **Covalent IMS**

3831 EW Leusden (NL)

(72) Inventors:

- **Oerlemans, Diderick Christian**
1018 CH, Amsterdam (NL)
- **Rabenort, Arij Wim Martin**
3831 EW, Leusden (NL)

(74) Representative: **van Looijengoed, Ferry Antoin**

Theodorus et al

De Vries & Metman

Overschiestraat 180

1062 XK Amsterdam (NL)

(54) **Safety system, method and computer program for determining an operational safety**

(57) The invention is related to a safety system, method and computer program for determination of an operational security, which is in particular suitable for determining the security of an infrastructural object, for example a tunnel tube for train traffic. An output signal in-

cluding an indication of the operational security is generated after the calculation of a function status on the basis of, amongst other, the availability of the components in the partial systems.

EP 2 050 648 A2

DescriptionBackground of the invention

5 **[0001]** The present invention is related to a safety system, a method and a computer program for determining an operational security, which is in particular suitable for determining the operational security of an infrastructure object, for example a tunnel tube for train traffic.

Description of the Prior Art

10 **[0002]** A method and a computer program for monitoring of the integrity of a train have been described in US 7,222,003 B2. Virtual blocks along the track are able to detect the front and the back of the train, to determine whether the whole train has passed a virtual block. Thus can be determined if trains are on a safe distance of each other. Moreover, it can be detected if a train has been disconnected.

15 US 7,222,003 B2 makes it not possible to monitor the integrity of the surroundings of the train - for example of a train tunnel -, but has been aimed at the train itself.

20 **[0003]** A system and a method for the detection of a crack in a construction, such as a bridge or road, have been described in US 6,972,687 B1. When the construction breaks, a cable which has been attached to the construction will break as well. The crack in the cable will be detected, whereupon the traffic can be warned by means of for example a traffic light.

US 6,972,687 B1 makes it not possible to introduce nuances in the integrity of the construction. US 6,972,687 B1 only describes the existence of a crack or no crack. Moreover the detection is limited to the detection of a cable crack.

Summary of the invention

25 **[0004]** The aim of the present invention is to provide an improved safety system, a method and a computer program for determining an operational security.

30 **[0005]** In order to reach the aforesaid aim according to the invention, in a first aspect a safety system is provided for determining an operational security, wherein the safety system comprises a database, a partial system analyzer for determining an availability value for a part of the system, and a function analyzer for determining a function status. The database can comprise definitions for one or more partial systems, weighting factors of components, definitions for one or more functions and/or boundary values of the partial systems. Keeping these definitions and values in the database has the advantage that at any moment they can be adapted, removed or completed. An operational function is formed by one or more partial systems. A definition of an operational function determines the way a function is composed of one or more partial systems. The function analyzer can be linked with the partial system analyzer and/or with the database. This makes it possible for data to be exchanged between these elements. The partial system analyzer is provided with a means for receiving a definition of the partial system and one or more weighting factors from the database. The system analyzer is also provided with a means for the detection of a component status of one or more components which are included in the partial system and a means for calculating the availability value on the basis of weighting factors of the available components. This makes it possible to distinguish between available components and not available components, and moreover to express the availability of the components by a value. The value can be absolute or relative with respect to a maximum availability value, which can be reached if all components are available. Components can have different weighting factors, which can be dependent on the partial system in which they are incorporated. The function analyzer is provide with a means for receiving a definition of one or more operational functions and one or more boundary values from the database, and a means for the reception of one or more availability values of one or more partial systems from the partial system analyzer. The function analyzer also provides the means for the calculation of the function status based on the definition of the operational function, the one or more availability values of one or more partial systems and the one or more boundary values. This makes it possible for the function, and therefore a composition of partial systems, to calculate the current function status, whereby the boundary values for the availability of the partial systems are taken into account, among which a partial system which can be considered as being less reliable. The safety system also provides for a means of generating an output indicator, including an indication of the operational security on the basis of the calculated function status. This makes it possibly to use the indication of the operational security in systems within and/or outside the safety system. The output indicator can include for example the calculated function status.

45 **[0006]** In an embodiment the partial system analyzer provides a means for reducing the availability value based on one or more component rules. This offers the possibility to take the availability value of certain occurrences of the concerning components in the calculation of availability the value extra into account. An example of such an occurrence is the non-availability of two serial components which are present within the system.

55 **[0007]** In an embodiment the safety system also includes a safety status analyzer for determining the safety status of

a safety class. The safety status analyzer can be linked with the function analyzer and/or the database. This makes it possible to exchange data between these components. The database includes also one or more security class definitions. The security class definitions determine the way the safety status depends on the function values. The safety status analyzer is provided with a means for the reception of a security class definition from the database and a means for receiving one or more of the function statuses from the function analyzer. The safety status analyzer is also provided with a means for calculating the safety status, based on the security class definition and one or more function statuses. This makes it possible to calculate the current safety status for a certain safety class, whereby the status of functions such as these occur within the safety class are taken into account. The output indicator can include for example the calculated safety status.

[0008] In an embodiment the safety status can get one of the values: not damaged, damaged, seriously damaged, or broken down. This has as the advantage that the calculation of the safety status has only a limited number of possible outcomes, which simplifies the processing of it.

[0009] In an embodiment the safety status is calculated for at least one of the safety classes: prevention, mitigation, self-help, and/or assistance. This makes it possible to limit the number of safety statuses, which simplifies the processing of it. Moreover these safety classes cover the most important aspects concerning operational security.

[0010] In an embodiment the safety system has a means for the calculation of a safety status on the basis of the safety status of one or more safety classes. This makes it possible for the outcomes of the different safety classes to aggregate into a single value for the operational security. The output indicator for example can include the calculated safety status.

[0011] In an embodiment the safety status gets one of the values green, yellow or red, and is the safety system provided with a web interface for visualizing the output indicator on the web interface in the form of a traffic light. This makes it possible to visualize the operational security in a transparent manner.

[0012] In an embodiment the value of the safety status is liable to one or more of the following rules: if one safety status gets the value "damaged seriously" and the value of the safety status was "green", then the safety status will get the value "yellow"; if the value of the safety status gets the value "yellow", then there timer is started, which it is kept up by a clock included by the safety system; if the value of the safety status was yellow and the safety status gets no value green within a defined interval, then the safety status gets the value red; if more than one safety status gets the value "damaged seriously", then the safety status gets the value red; if the value of the safety status was red and at least three safety statuses get the value available, then the safety status gets the value yellow, where the timer continues as from the previous time that the safety status value got "yellow". This makes it possible to change the value of the safety status in a well controlled manner.

[0013] In an embodiment the safety system is provided with a log-database for storing the indications of the operational security on the basis of the calculated function statuses. This makes it possible to store the calculated function status for example the calculated security status and/or the calculated safety status for later uses.

[0014] In an embodiment the operational security concerns an operational security of an infrastructure object, for example tunnel tube for train traffic. This makes it possible to provide infrastructure objects such as tunnel tubes for train traffic for which the operational security is very important with a safety system.

[0015] In a second aspect of the invention a method is provided for determining an operational security conform the safety system as described above.

[0016] In a third aspect of the invention a computer program is provided for determining an operational security. The computer program includes computer code parts which, if these are carried out by a processor, are directed to the implementation of one or more steps of the method.

Brief description of the figures

[0017] The safety system, method and computer program according to the present invention, are further described under reference to the enclosed drawings in which:

Figure 1 is a schematic presentation of safety system of an exemplary embodiment of the present invention;

Figure 2 is a schematic presentation of safety system of an exemplary embodiment of the present invention;

Figure 3 is a schematic presentation of safety system of an exemplary embodiment of the present invention;

Figure 4 is a schematic presentation of a working method of an exemplary embodiment of the present invention;

Figure 5 is a schematic presentation of a manner in which an operational security can be determined;

Figure 6 is a schematic presentation of an application architecture in which a safety system has been incorporated;

Figure 7 is an example of a traffic light, such as can be presented in a web interface in conformity with an embodiment of the present invention.

Detailed description of the invention

[0018] Suitable embodiments of the present invention will be described below under reference to the figures.

The invention makes it possible to translate the status of the components to the operational security of tunnel tube.

[0019] Under reference to the figures 1 to 3, safety systems are shown for determining an operational security of tunnel tube.

[0020] Figure 1 shows a database 1, a system analyzer 2 and a function analyzer 3. The database 1 has been linked with the system analyzer 2. The database 1 and the system analyzer 2 have been linked with the function analyzer 3. The partial system analyzer 2 provides a means 21 for the detection of the component status 101 of one or more components. The component status 101 is for example offered as an input indicator. Partial system analyzer 2 has a means (24) for the reception of a definition of the partial system and one or more weighting factors from the database. Partial system analyzer 2 has been provided with a means 22 for calculating the availability value of a partial system on the basis of weighting factors of the available components. Partial system analyzer 2 provides a means 23 for reducing the availability value of the partial system on the basis of one or more component rules. The function analyzer 3 provides a means 32 for receiving a definition of an operational function and one or more boundary values from the database. Function generator 3 provides a means 31 for receiving one or more availability values of one or more partial systems from the partial system analyzer 2. Function generator 3 provides a means 34 for calculating the function status based on the definition of the operational function, the one or more availability values of one or more partial systems and one or more boundary values.

Function generator 3 provides a means 33 for generating an output signal 102. The output signal includes an indication of the operational security on the basis of the calculated function status. In this example the output signal includes the outcome of the calculated function status.

[0021] The component status can be originating from a computer system which keeps the component status. The component status can also be originating directly of the components. It is also possible that the component status is kept up manually and is subsequently introduced into the computer system, for example in the event that the status of a component is checked by an inspector during a visual inspection. A component has the status available (B) or not available (NB). A component belongs to a partial system. A component has a weighting factor, which reflects the relative importance for the system to which it belongs. A component may have a location or position (in a given order) in the tunnel tube. The component status may be communicated by the computer system, but can if necessary also be entered manually, as a result of an inspection report. An example of a component is a section valve and a main valve. The main valve will have a higher weighting factor than a section valve, and comparable with two beside each other located section valves. The section valves have been numbered rising in the tunnel tube, thereby fixing the position.

[0022] A partial system is composed of one or more components. A partial system has a maximum availability value ($BW_{\max}$), which is determined by the summation of the weighting factors of all the underlying components (C): $BW_{\max} = \sum(C)$. A partial system has an availability value (BW) that can be determined by adding up the weighting factors of all components with status B (C_B): $BW = \sum(C_B)$. There can be special rules which need to be applied, as a result of which the system degrades further, then the added up individual components. In that case the availability value is reduced by an extra term (T). A system can be allocated to several operational functions. For each operational function a weighting factor will be fixed, to indicate the contribution of the specific partial system to each function. An example of such a partial system is sprinkler system. The sprinkler system is composed of 100 section valves with a weighting factor 1. There exists a special component rule which tells that there may be no 2 section valves connected next to each other with the status NB. Is that, however, the case, then an extra calculation of $T=5$ must be applied. In the calculation example mentioned below, 2 section valves positioned next to each other have the status NB: $BW = \sum(C_B) - T = 98 - 5 = 93$. The system has therefore an availability value of 93 (or $93/100 = 93\%$ expressed as a percentage).

[0023] The function status has the values available (B) or not-available (NB). An operational function is composed of one or more partial systems. Within an operational function overlapping partial systems can also exist, like for example the hand rail, the lighting and the signs of the escape route. For several combinations of partial systems boundary values can be set by partial system. By setting logical equations, the function status can be calculated. A function can be allocated to several hierarchical higher safety classes. For each operational function - security class combination a security class can be defined, to indicate the contribution of the specific operational function to the safety class. For example to define the operational function "cooling tunnels downstream" the Sprinkler system must be available for a minimum of 95% (see also the previous example). The ventilation, with a maximum availability of 30, must be present for 80%, if it is operated on mains voltage. If it is operated on emergency power supply, an availability of 40% has been agreed. The maximum availability of mains voltage is 1, the maximum availability of emergency power supply is also 1 (assumptions for the example):

Overlap	Partial system	Symbol availability value	BW _{max}	Boundary value
	Sprinkler system	BW _{sprinkler}	100	95 (95%)
1	ventilation	BW _{vent}	30	24 (80%)
	mains voltage	BW _{net}	1	1
2	ventilation	BW _{vent}	30	12 (40%)
	emergency power supply	BW _{nood}	10	10

[0024] The function status (FS) is then calculated as follows:

FS = BW_{sprinkler} ≥ 95 AND ([BW_{vent} ≥ 24 AND BW_{net} ≥ 1] OR [BW_{vent} ≥ 12 AND BW_{nood} ≥ 1]).

[0025] The outcome of the calculation can be stored in the log-database (6), for later use.

[0026] Figure 2 shows an extension of the safety system shown in Figure 1. Figure 2 shows aforesaid elements and safety status analyzer 4, which it has been linked with the database and the function analyzer. The safety status analyzer 4 has a means 42 for receiving a security class definition from the database. Safety status analyzer 4 is provided with a means 41 for receiving one or more function statuses from the function analyzer 3. Safety status analyzer 4 is provided with a means 44 for calculating the safety status on the basis of the security class definition and one or more function statuses. Safety status analyzer 4 is provided with a means 43 for generating an output signal 103 on the basis of the calculated function status. The output signal 103 includes the outcome of the calculated safety status, in this example. The outcome of the calculation can be stored in log-database (6), for later use.

[0027] A safety status may have the status values: Not Damaged, Damaged, Seriously Damaged or Broken down. A safety class is build of one or more operational functions. The availability value of an operational function does not have to be taken into account, but only if it is available or not available. The safety status is stipulated based on the number of failing operational functions in the safety class, for example by adding these up. In the matrix mentioned below, an example of the relation between the safety classes and the operational functions is presented by means of the security class definition.

	Failing number of operational functions per safety class		
Safety class definition	1	2	3
1	Damaged (sum = 1)	Damaged (sum = 2)	Seriously Damaged (sum = 3)
2	Damaged (sum = 2)	Seriously Damaged (sum = 4)	Broken down (sum = 6)
3	Seriously Damaged (sum = 3)	Broken down (sum = 6)	Broken down (sum = 9)

[0028] The calculation of the safety status for the safety classes prevention, mitigation, self-help and assistance, allows the most important aspects around the operational security to be covered. These safety classes are used in several laws and legislation, used nationally and international.

A safety class is called in international applications also a 'line-of-defense'.

[0029] Figure 3 shows an extension on the safety system shown in Figure 2. Figure 3 shows the aforesaid elements and the means 5 for calculation of the safety status on the basis of the safety status of one or more safety classes. The safety status is received as an output signal 103 from the safety status analyzer 4. The means 51 are capable of generating an output signal 104 on the basis of the calculated function status. The output signal 104 includes the outcome of the calculated safety status in this example. The outcome of the calculation can be stored in the log-database (6), for later use.

[0030] In this example of a tunnel tube for train traffic, the safety status may get the value GREEN, YELLOW or RED. These chosen values do not have to be considered as limiting for the invention. The number of possible values and the possible values themselves can be defined by safety system. This way only the values green and red could be possible or other colors can be used as values. It is also possible that the safety status is expressed in values differently than colors, for example, such as numerical values, or as a value from the collection {high, low}, or as a value from the

collection {good, moderate, bad}, or as a value from the collection {safe, unsafe}, and more like these. The security of the tunnel tube has been built from four safety classes. The safety status Damaged Seriously at one safety class results in a status passage of GREEN to YELLOW. A tunnel tube has a maximum time limit for the status YELLOW. This maximum time can be set on one certain value, for example on 168 hours. If during the maximum time in status YELLOW, no status passage takes place to GREEN, the status passage to RED automatically takes place. Damaged Seriously of more than one safety class, or Broken down of one safety class results in the status RED, whereby the timer for the status YELLOW continues in the background. If in the status RED, 3 safety classes become available, the status passage to YELLOW takes place, whereby the timer is not started again, but continues as from the previous status YELLOW.

[0031] Under reference to figure 4, a working method is shown for the determination of an operational security. The shown steps 301-304 are carried out in the function generator 3. The shown steps 401-404 will be executed in the safety status analyzer 4. The shown steps 501-503 are carried out in the safety system. Figure 4 shows the reception 301 of a definition of an operational function and one or more boundary values from a database and the reception 302 of one or more availability values of one or more partial systems from a partial system analyzer. Figure 4 shows the calculation 303 of a function status based on the definition of the operational function, the one or more availability values of one or more partial systems and one or more boundary values. Figure 4 shows the reception 401 of a security class definition from the database and the reception 402 of one or more function statuses from the function analyzer. Figure 4 shows the calculation 403 of the safety status based on the security class definition and one or more function statuses. Figure 4 shows the calculation 501 of the safety status based on the safety status of one or more safety classes. Figure 4 shows the visualization 503 of the output signal, for example in the form of a traffic light on a web interface as shown in Figure 5 in 5001 or Figure 7. The output indicator can be generated at several moments, what has been reflected in the steps of generating 304, 404, 502 which comprise an output signal as an indication of the operational security. The outcomes of calculations can be stored at several moments in the log-database. This has been shown in the steps 305, 405 and 504.

[0032] In Figure 5 it has been depicted schematically, how the operational security can be determined. Judgments concerning the operational security of tunnel tube can be done, looking at the function statuses 3001-3005 within the four safety classes 4001-4004 (prevention 4001, mitigation 4002, self-help 4003 and assistance 4004). At (partly) failure of a function the safety statuses become damaged or broken down. For the status Broken down of one safety class it is possible to define a period in which the safety class must be repaired. If the safety class has not been repaired in the period, then the safety status of the operational security gets the lowest value, for example RED. Also at the status Broken down for two or more safety classes, the safety status can get the lowest value. The safety status follows from a chain, in which the status of the partial systems 2011, 2012 and components 2001-2004 propagates by means of the functions 3001-3005 to the safety classes 4001-4004. Traffic light 5001 presents the color RED, YELLOW or GREEN, what presents the safety status of the operational security.

[0033] Figure 6 shows an example of an application architecture on which the safety system according to the invention is executed. The computer systems which are reading the component status, can be external and have been coupled to the DATA APPLICATION SERVER by means of a network, for example an ATM or IP network. These computer systems supply the required data concerning the status of the components. The data from the component status systems are picked up from the SQL database "catalog" that is present for every tunnel. For the automatic picking up and the centralization of these data, for example SQL Server Integration Services (SSIS) may be used. The database 1 of the safety system contains the data for determining the operational security and has been implemented for example as an SQL server 2005 database. On this SQL server also runs the SSIS. The server contains a computer program for determining the operational security. By means of an internet site a web interface is available, that a page with the indicator shows, in the form of a traffic light, for each tunnel. The internet site can be reached by means of a browser on a terminal. For simply visible presentation of the traffic light for each tunnel, use can be made of a terminal for each tunnel which shows the correct page automatically by means of the built in web browser, which is periodical refreshed. The server can be managed by means of a management internet site by the use of web browsers. The management application can be approached with a browser from every workplace which has access to the web server.

[0034] Figure 7 shows a sophisticated traffic light, such as can be presented by a web interface. Preferably, a web page will be available for each tunnel. The page shows the name of the tunnel (in the example this is ZEVENAAR) and for each tube the traffic light and the name of the tube (in the example these are NOORD and ZUID). The traffic light shows the three status colors GREEN, YELLOW and RED, where the current status has a clear color. In addition a green hour meter can be shown (not shown in Figure 7) which indicates the time in status green, if this status is current. A yellow expiring timer for the status YELLOW can be shown (not shown in Figure 7), which indicates the hours, minutes and seconds that still remain, before it is switched to the status RED, if the current status is YELLOW. It is possible give a supporting explanation for the outcome of the safety status at every level in the chain. The safety status of a tunnel with the underlying hierarchy can be shown as a tree structure, as reflected in Figure 7. For each tunnel tube the safety status is presented and four "lights" are shown, which indicate for each safety class if it is available or broken down. In the tree structure it is possible for each safety class to focus on the underlying operational functions. By operational function the status is indicated color indication. For each operational function further focusing can be performed on the

underlying partial systems, where with an analogue indicator the status is indicated by showing the availability value of the partial system (in the form of grey squares), the boundary value (in the form of a vertical hyphen in the squares) and the maximum availability value (in the form of grey and white squares together). In Figure 7 the tunnel tube is operated under emergency power supply, and in that case the boundary value for the system ventilation will show the associated value for functioning under emergency power supply. By partial system it is possible to present the list with components with the associated component status and weighting factor.

[0035] Although the present invention has been explained above, with respect to certain implementation forms of it, it must be understood that the invention is not meant to be limited by these. The invention includes all possible implementation forms, which can be made within the scope, with respect to the measures, which have been in particular brought forward in the attached claims and all equivalents of it.

Claims

1. Safety system for determining an operational security, comprising:

a database (1) comprising definitions for one or more partial systems, weighting factors of components, definitions for one or more operational functions and boundary values of partial systems, whereby an operational function is formed by one or more partial systems;

a partial system analyzer (2) for determining an availability value of a partial system; and
a function analyzer (3) for determining a function status, whereby the function analyzer (3) is linked with the system analyzer (2) and with the database (1), whereby the system analyzer (2) is provided with:

a means (24) for reception of a definition of the system and one or more weighting factors from the database;
a means (21) for detection of a component status (101) of one or more components of the partial system for determining an availability value of the components; and
a means (22) for calculation of the availability value of the partial system on the basis of the weighting factors of the available components, and whereby the function analyzer (3) is provided with:

a means (32) for reception of a definition of an operational function and one or more boundary values from the database;
a means (31) for reception of one or more availability values of one or more partial systems from the system analyzer (2); and
a means (34) for calculation of the function status on the basis of the definition of the operational function, the one or more availability values of one or more partial systems and the one or more boundary values; and
a means (33,43,51) for generation of an output signal (102,103,104) comprising an indication of the operational security on the basis of the calculated function status.

2. Safety system according to claim 1, wherein the partial system analyzer (2) is provided with a means (23) for reduction of the availability value of a partial system on the basis of one or more component rules.

3. Safety system according to claim 1 or 2, wherein the safety system also comprises a safety status analyzer (4) for determination of the safety status of a safety class, the safety status analyzer (4) is linked to the function analyzer (3) and to the database (1), wherein the database (1) also includes one or more security class definitions, and wherein the safety status analyzer (4) is provided with:

a means (42) for reception of a security class definition from the database (1);
a means (41) for reception of one or more function statuses from the function analyzer (3); and
a means (44) for calculation of the safety status on the basis of the security class definition and the one or more function statuses.

4. Safety system according to claim 3, wherein the safety status gets one of the following values: not damaged; damaged; damaged seriously; broken down.

5. Safety system according to any of the claims 3-4, wherein the safety status is calculated for at least one of the following safety classes: prevention; mitigation; self-help; assistance.

6. Safety system according to any of the claims 3-5, wherein the safety system is provided with:

a means (5) for calculation of the safety status on the basis of the safety status (102a) of one or more of the safety classes.

7. Safety system according to claim 6, wherein the safety status gets one of the values: green, yellow or red, and the safety system is provided with a web interface for visualization of the output signal (102,103,104) in the form of a traffic light on the web interface.

8. Safety system according to claim 7, wherein the value of the safety status is depending on one or more of the following calculation rules:

if one safety status gets the value damaged seriously and the value of the safety status was green, then the safety status will get the value yellow;

if the value of the safety status gets the value yellow, then a timer is started, which it is maintained by a clock which is included in the safety system,;

if the value of the safety status was yellow and the safety status does not get the value green within a defined time interval, then the safety status gets the value red;

if more than one safety status get the value damaged seriously, then the safety status gets the value red;

if the value of the safety status was red and at least three safety statuses get the value available, then the safety status gets the value yellow, whereby the timer will continue as from the previous time that the safety status got the value yellow.

9. Safety system according to any of the preceding claims, wherein the safety system also comprises a log-database (6) for storing the indication of the operational security on the basis of the calculated function status.

10. Safety system according to any of the preceding claims, wherein the operational security concerns an operational security of an infrastructure object, for example a tunnel tube for train traffic.

11. Method for determining an operational security, comprising the steps of:

reception (301) in a function analyzer of a definition of an operational function and one or more boundary values from a database;

reception (302) in the function analyzer of one or more availability values of one or more partial systems from a partial system analyzer;

calculation (303) in the function analyzer of a function status on the basis of the definition of the operational function, the one or more availability values of one or more partial systems and the one or more boundary values; and

generating (304,404,502) an output signal comprising an indication of the operational security on the basis of the calculated function status.

12. Method according to claim 11, wherein the working method also includes the steps of:

reception (401) in a safety status analyzer of a security class definition from the database;

reception (402) in the safety status analyzer of one or more function statuses from the function analyzer; and calculation (403) in the safety status analyzer of safety status on the basis of the security class definition and the one or more function statuses.

13. Method according to claim 12, wherein the working method also includes the step of:

calculation (501) of a safety status on the basis of the safety status of one or more safety classes.

14. Method according to claim 13, wherein

the safety status gets one of the following values: not damaged; damaged; damaged seriously; broken down; the safety status is calculated for at least one of the following safety classes: prevention; mitigation; self-help; assistance; and

the safety status gets one of the values green, yellow or red,

and the method also includes the step of visualizing (503) the output signal in the form of a traffic light on a web interface.

- 5 **15.** Method according to any of the claims 13-14, wherein the value of the safety status is depending on one or more of the following calculation rules:

10 if one safety status gets the value seriously damaged and the value of the safety status was green, then the safety status will get the value yellow;
 if the value of the safety status gets the value yellow, then a timer is started, which it is maintained by a clock which is included in the safety system;
 if the value of the safety status was yellow and the safety status does not get the value green within a defined time interval, then the safety status will get the value red;
 if more than one safety status get the value damaged seriously, then the safety status will get the value red;
 15 if the value of the safety status was red and at least three safety statuses get the value available, then the safety status will get the value yellow, whereby the timer will continue as from the previous time that the safety status got the value yellow.

- 16.** Method according to any of the claims 11-15, wherein the method also includes the step of:

20 storing in the log-database of the indication of the operational security on the basis of the calculated function status.

- 17.** Method according to any of the claims 11-16, wherein the operational security concerns an operational security of an infrastructure object, for example a tunnel tube for train traffic.

- 25 **18.** Computer program for determining an operational security, comprising computer code parts which, when executed by a processor, are arranged to perform the steps of the method according to any of the claims 11-17.

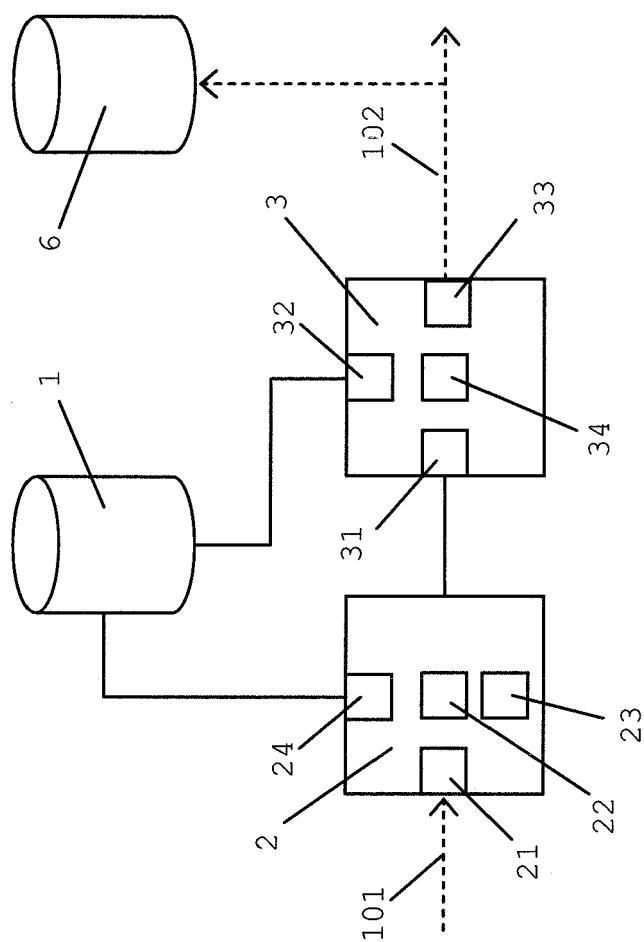


Fig. 1

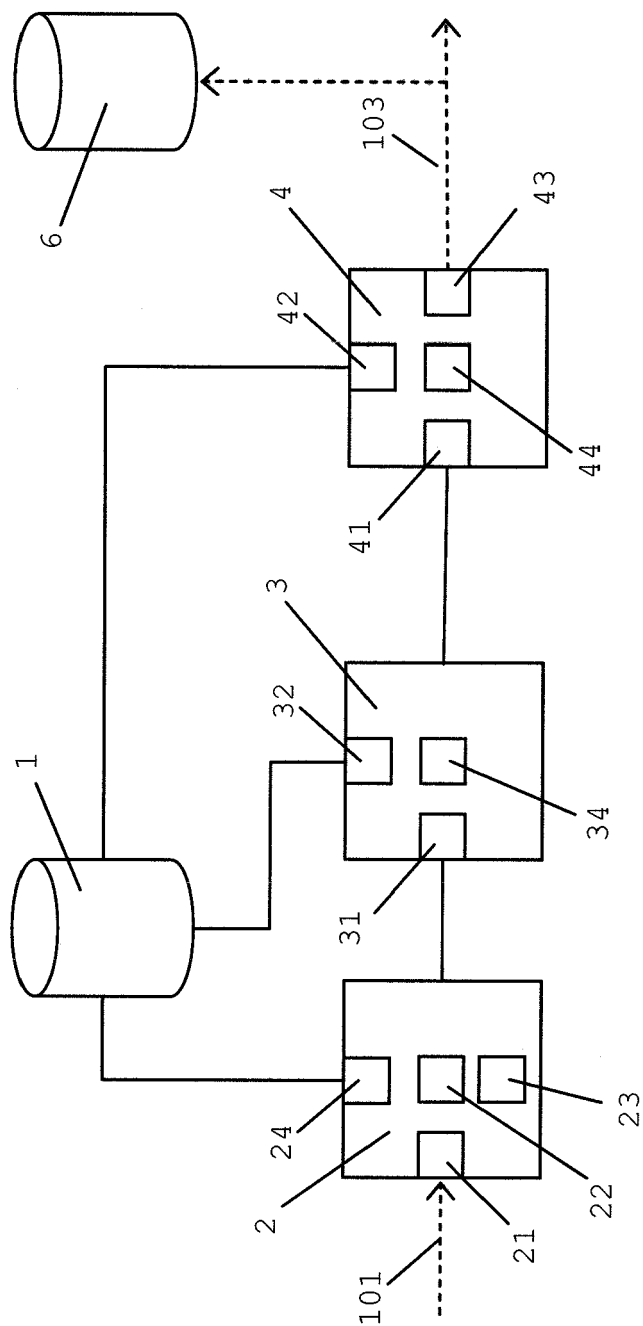


Fig. 2

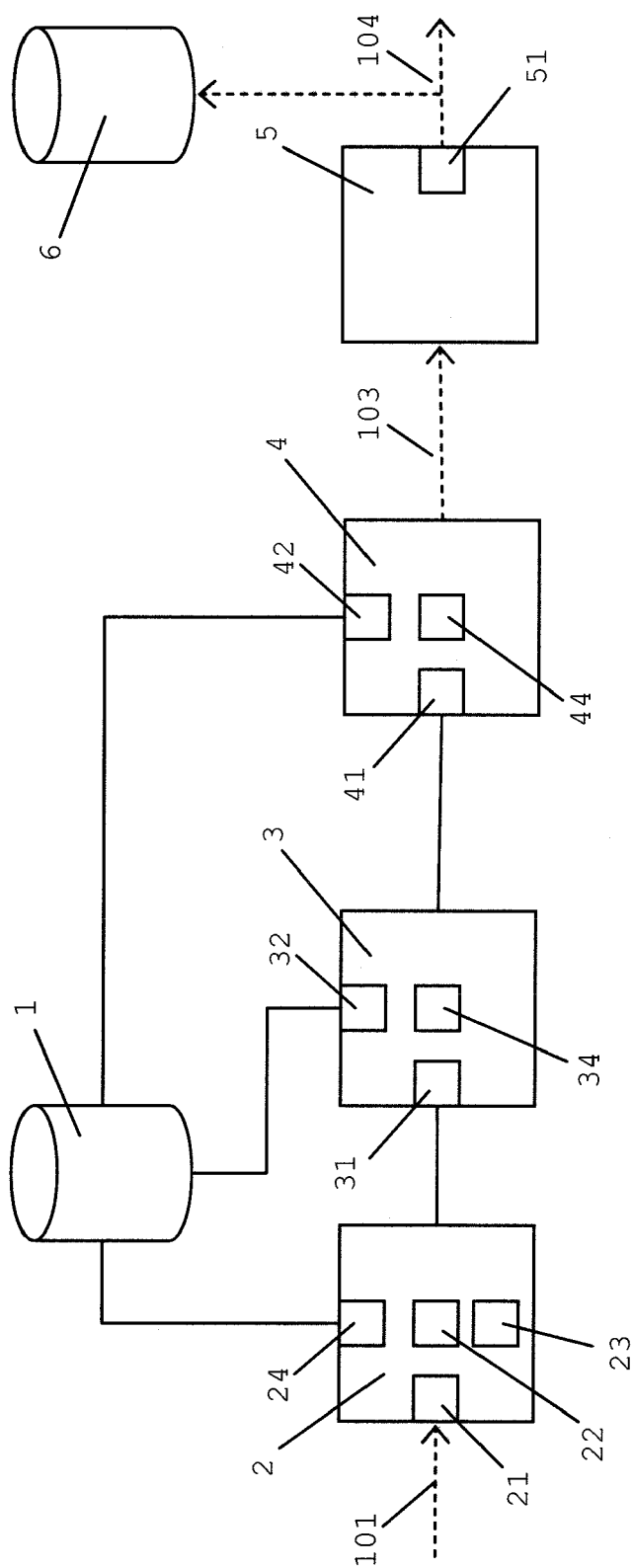
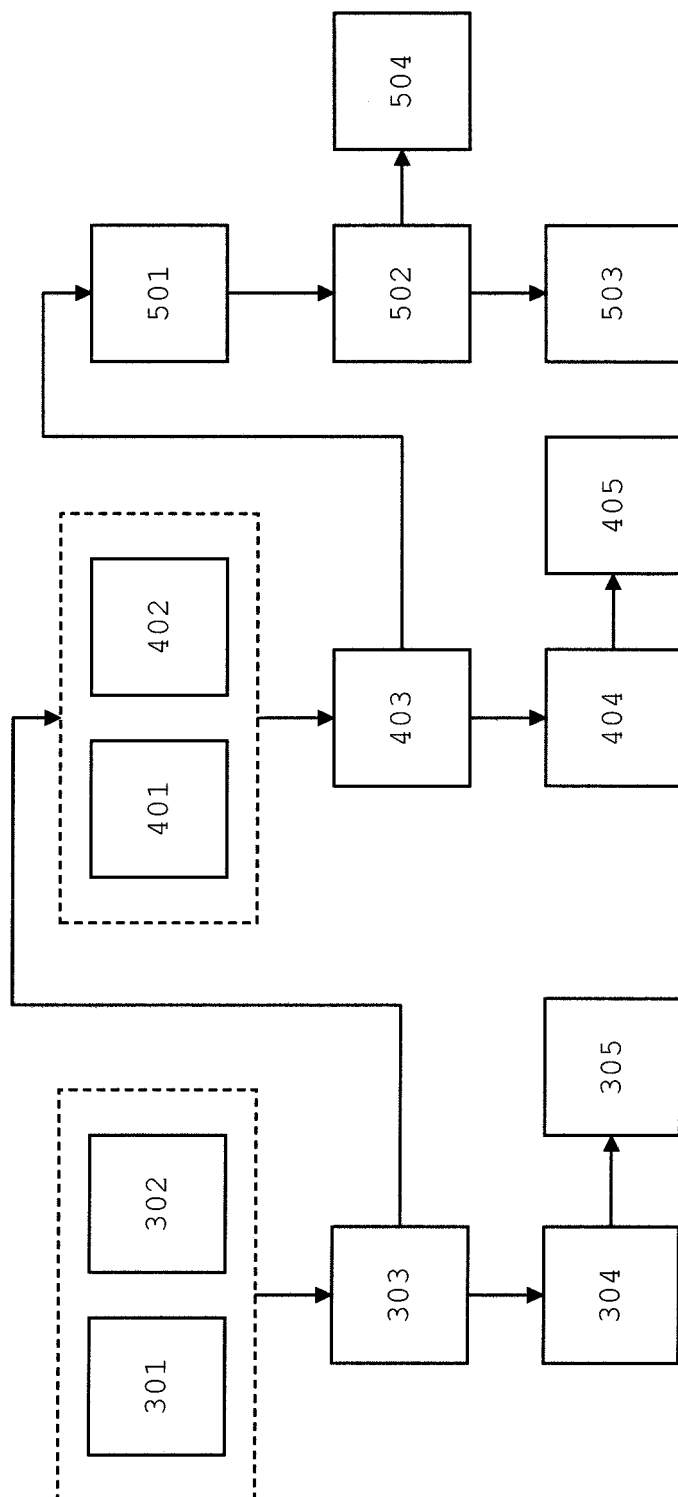


Fig. 3

**Fig. 4**

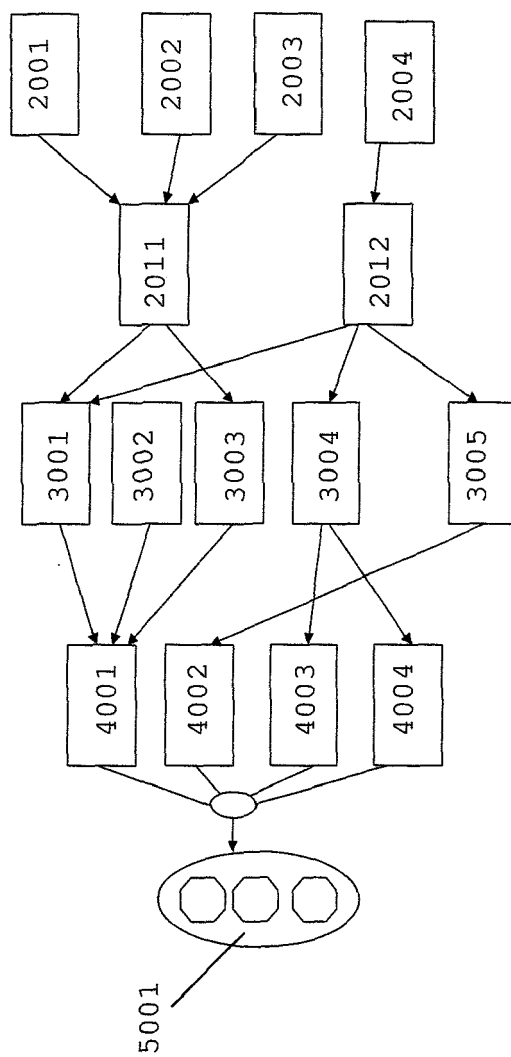


Fig. 5

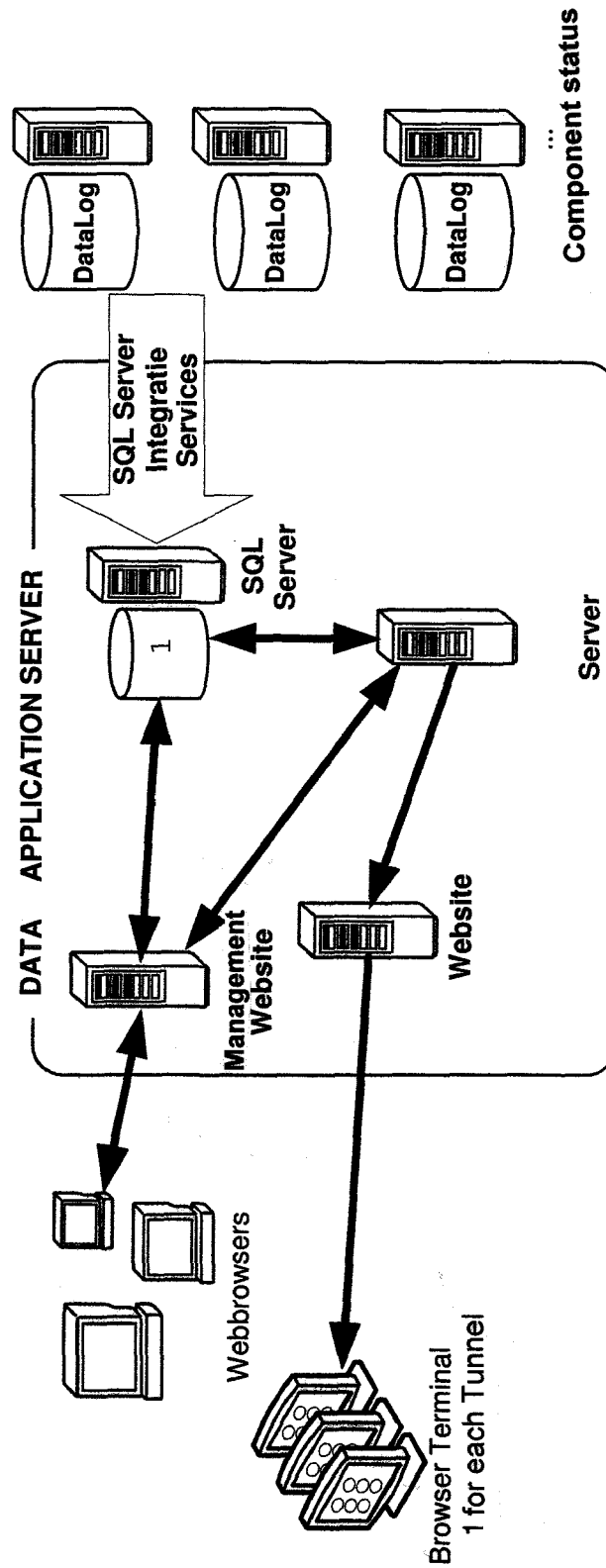


Fig. 6

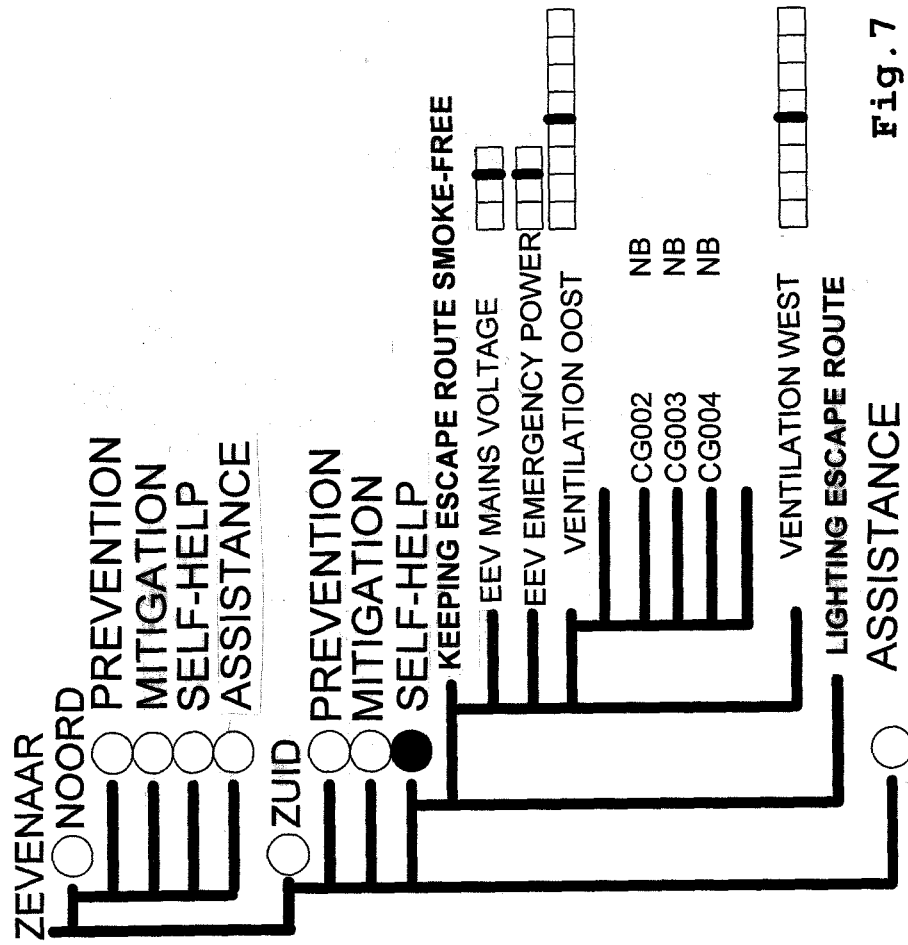


Fig. 7

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

- US 7222003 B2 [0002] [0002]
- US 6972687 B1 [0003] [0003] [0003]