(12) **Oversettelse av europeisk patentskrift**

(11) **NO/EP 3428756 B1**

(19) NO

NORGE

(51) Int Cl.

G05B 23/02 (2006.01)
G06F 21/50 (2013.01)

Patentstyret

(21)	Oversettelse publisert	2019.10.14
(80)	Dato for Den Europeiske Patentmyndighets publisering av det meddelte patentet	2019.06.19
(86)	Europeisk søknadsnr	17180526.0
(86)	Europeisk innleveringsdag	2017.07.10
(87)	Den europeiske søknadens Publiseringsdato	2019.01.16
(84)	Utpekte stater	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
(73)	Innehaver	Siemens Aktiengesellschaft, Werner-von-Siemens-Straße 1, 80333 München, Tyskland
(72)	Oppfinner	Falk, Rainer, Primelweg 9, 85586 Poing, Tyskland Fries, Steffen, Eberweg 3, 85598 Baldham, Tyskland
(74)	Fullmektig	ONSAGERS AS, Postboks 1813, Vika, 0123 OSLO, Norge

(54) Benevnelse **INTEGRITY MONITORING IN AUTOMATION SYSTEMS**

(56) Anførte publikasjoner

EP-A1- 2 980 662
EP-A1- 3 101 491
US-A- 5 621 158
DE-A1-102014 117 282
DE-A1- 10 135 586

Vedlagt foreligger en oversettelse av patentkravene til norsk. I hht patentloven § 66i gjelder patentvernet i Norge bare så langt som det er samsvar mellom oversettelsen og teksten på behandlingsspråket. I saker om gyldighet av patentet skal kun teksten på behandlingsspråket legges til grunn for avgjørelsen. Patentdokument utgitt av EPO er tilgjengelig via Espacenet (http://worldwide.espacenet.com), eller via søkemotoren på vår hjemmeside her: https://search.patentstyret.no/

Description

Integrity monitoring in automation systems

TECHNICAL FIELD

Various examples of the invention generally concern monitoring the integrity of an industrial automation system. Various examples of the invention concern, in particular, monitoring based on a comparison between state data of the automation system and sensor data, which describe an environmental impact of the automation system. Various examples of the invention concern monitoring integrity in order to detect the impairment of integrity due to third-party access.

BACKGROUND

EP 3 101 491 A1 describes a security system for an industrial control infrastructure. Thereby, a digital thumbprint is created, which captures sections of a data structure. Thereby, the thumbprint also denotes environmental data that are held in components of a control device. This digital thumbprint is compared to a saved thumbprint to determine a probability of modification or falsification.

EP 2 980 662 A1 describes the identification of a threat situation for an automation component of the control and field level. In this case, a target program behaviour is compared with an actual program behaviour determined in the operation of the automation component. In memory areas, sensor data are located, which define an actual program behaviour.

DE 10 2014 117 282 A1 discloses an automation system that compares operating data of a control system with a pre-known specification.

US 5,621,158 A discloses a comparison between measurement values of sensors with reference values. The reference values are selected depending on a load ratio that is defined as the ratio of a current load to a maximum load. Depending on the comparison, the system is rated as normal or abnormal.

DE 101 35 586 A1 describes the reconfiguration of a sensor system to achieve improved accuracy in the event of a failure. For this purpose, the sensor system uses a sensor to measure system states of an application system. Failure states are determined from a comparison of the measured system states with a state estimated by a system model.

With increasing automation, industrial automation systems are becoming more widespread. For example, automation systems are used in the production of machines or workpieces. Automation systems can implement process-related systems. Industrial automation systems are also used in the field of traffic monitoring or traffic management, for example, in connection with traffic control systems in cities, in building automation, rail transport or air traffic. Industrial automation systems can also be used in power generation, for example, in power plants or substations, as well as in energy transmission and energy distribution (smart grid).

Modern automation systems are characterized by a high degree of connectivity. For example, automation systems typically include a variety of components, such as sensors, actuators, computing units, or control units. These components of automation systems are typically connected to each other via a network and are therefore connected on a communicative level. It is often also possible for the automation system to be accessed from outside - for example via the Internet - or for an automation system to transmit data via the Internet, for example, diagnostic data for predictive maintenance.

Therefore, in connection with automation systems, there is often a risk of unauthorized third-party access (hacking). Such unauthorized third-party access can lead to malfunctions, data loss, functional limitations, and even total failure of the corresponding automation system.

Therefore, protecting the integrity of automation systems is a necessary goal to ensure reliable operation. In particular, there is a need to protect the integrity of industrial automation systems as a whole beyond the protection of individual sub-functions of the automation systems.

In reference implementations, the integrity impairment due to unauthorized third-party access is monitored, for example, on the basis of state data from the IT systems of an automation system, which describe the operating state of the automation system. Based on an evaluation of such state data, an attack on the integrity of the IT components of the automation system can be detected. For example, irregularities can be detected in the state data. The automation of the detection of such irregularities is described in the context of intrusion detection systems. Intrusion detection systems specifically search for known attack patterns, for example, in the operating software of the automation system or in connection with communication interfaces of the automation system.

However, such reference implementations have certain limitations and disadvantages. For example, such reference implementations can have limited accuracy. Often, such intrusion detection systems can only detect IT-related attacks or tampering.

SHORT SUMMARY OF THE INVENTION

Therefore, there is a need for improved techniques to monitor the integrity of automation systems. In particular, there is a

need for techniques to detect third-party access to automation systems. There is a need for such techniques, which remedy or alleviate at least some of the disadvantages and limitations mentioned above.

This task is achieved by means of the features of the independent patent claims. Preferred embodiments have the features of the dependent patent claims.

An exemplary method entails obtaining state data from an industrial automation system. The state data describes the operating state of the automation system. The method also entails obtaining sensor data that describes an environmental impact on the automation system. The method also entails performing a comparison between the state data and the sensor data, as well as monitoring the integrity of the automation system based on the comparison.

For example, it would be possible to detect third-party access to the automation system and monitor associated impacts on integrity. Unauthorized third-party access can be reliably detected.

For example, the industrial automation system could implement a power plant, an energy distribution grid, a transformer station, a production line for workpieces or machinery, a refinery, a pipeline, a sewage treatment plant, a traffic control system, a medical device, or the like. Sometimes, such an automation system is also called a cyber-physical system (CPS). Examples of automation systems include: an industrial plant; a production hall; a substation; a robot; a forklift truck; an autonomous transport system; a machine tool; a milling cutter; a press; a process engineering system; and a 3D printer.

For example, the state data can include log files of an operating software of the automation system. For example, the state data can come from one or a plurality of controllers of the automation system. The state data could include: a self-test result of an operating software of the automation system, checksums, memory snapshots, etc.

The sensor data can be obtained from one or a plurality of sensors. For example, the sensors can be part of the automation system, meaning they are connected to communication via a common communication interface with other components of the automation system. In other examples, however, it would also be possible that the sensors are not part of the automation system, but rather are kept separate so that simultaneous access to both the automation system as well as the sensors cannot easily be obtained.

The sensor data can therefore be indicative for the environmental impact of the automation system. Depending on the type or type of environmental impact, a wide variety of sensors can be used. For example, environmental impact could include heating or cooling the environment of the automation system; in such a case, it would be possible for temperature sensors to be used. In other examples, it would be possible for environmental impact to include the switching of traffic lights or traffic management systems in general; here, for example, video data that depict the traffic management systems could be obtained as sensor data. In connection with power generation, for example, sensor data that are indicative for electrical parameters, such as voltage or current flow or phase shift, could be obtained.

By performing the comparison between the state data and the sensor data, a deviation of the environmental impact from an expected reference can be detected in particular. Such a deviation of the environmental impact can occur, for example, if marginal conditions of environmental impact change, which

are based outside the automation system. In such a case, it is not necessarily required to detect an impairment of integrity. However, it would also be possible for such a deviation of the environmental impact from the reference due to, for example, unauthorized third-party access the integrity of the automation system. Then, by monitoring the deviation, the unauthorized third-party access can be detected.

By comparing the health data with the sensor data, a particularly high degree of reliability can be achieved for monitoring integrity. In particular, such a common analysis can enable a positive confirmation of integrity. In addition, integrity can be monitored based on a variety of data sources, thereby increasing overall reliability. Third-party access can be reliably detected. In particular, an impact of third-party access on integrity can be detected. Integrity impairment can be detected. Unauthorized third-party access can be reliably detected. Manipulations can also be detected at the analogue control system of an actuator or on sensors of the automation system, for example, a manipulation of a control electronics system. This will achieve a new quality of integrity monitoring.

In an example, the state data comprise a state of operating software of the automation system. This is how IT-related information about the automation system can be obtained. In particular, the condition of the operating software can be characteristic of the operating state of the automation system.

The state data can include at least one element of the following group: a component registration of a multitude of active components of the automation system; a component activity of a multitude of components of the automation system; an fault state of an operating software of the automation system; a parameter of a communication interface of the

automation system; as well as resource allocation of computer hardware of the automation system.

By means of such and other types of state data, the condition of the operating software of the automation system can be reliably and extensively mapped. By taking into account a plurality of complementary types of state data, an individual attack on individual function blocks of the automation system can be detected in particular. This is due to the experience that a simultaneous attack on a plurality or many function blocks with a falsified however, coherent and consistent behaviour only seldom occur. Therefore, an impairment of integrity can be detected particularly reliably due to third-party access.

Such types and other types of state data can also be, in particular, indirectly indicative of an activity of actuators of the automation system, which cause the environmental impact. Sometimes, it can be desirable to take the activity of the actuators of the automation system particularly explicitly into account when monitoring integrity. In such a case, it is also helpful to obtain control data for one or a plurality of actuators of the automation system, wherein these actuators cause the environmental impact. Then, the comparison is carried out between the state data, the sensor data and the control data.

In this way, it is possible to attribute a certain unexpected environmental impact particularly well, for example, on malfunctions of the actuators; malfunctions of the actuators do not necessarily have to be caused by third-party access, but can also be caused by damage, etc. This can increase the overall accuracy of monitoring integrity. In particular, the integrity of the system can be monitored, even independently of third-party access.

In some examples, the comparison takes into account a deviation of the environmental impact from a reference. In particular, a deviation from the normal behaviour can be found in the context of the comparison. Such a deviation from the normal behaviour can be determined particularly easily - especially compared to reference implementations, in which the environmental impact is to be comprehensively predicted. Due to the complexity of automation systems, it can sometimes be impossible or only possible to a limit extent to fully predict environmental impact. In such scenarios, it can be helpful if, instead of predicting the environmental impact, only a deviation of the environmental impact from the reference is taken into account. Anomaly detection can therefore be carried out.

Thereby, it would be possible for example that the reference is determined on the basis of a specified deterministic model and as a function of the state data. For example, the deterministic model could provide the reference based on simple assumptions, which are, for example, fixedly specified and stored in a memory. Such a model could, for example, predict that, in the case of a large number of memory accesses of an operating software of the automation system, typically an increased number of finished workpieces are obtained per unit of time. The number of workpieces completed per unit of time could be checked by a suitable sensor; in this way, a deviation between sensor data and state data could be used to determine an impairment of integrity. Another example of such a model concerns, for example, the frequency of control operations in the operation of gas turbines; if a gas turbine is often regulated between different power values, the temperature in a storage of the gas turbine could rise. The temperature profile in the area of the storage of the gas turbine can be monitored by a temperature sensor and this predicted relationship can be verified within the scope of the model by comparing the state data with the sensor data. In particular, if a simulation model of the automation system, also known as a digital twin, is

available, the simulation model can be used as a reference during ongoing operation. This is particularly advantageous because a simulation model (digital twin) created during the design of the automation system can be used for integrity monitoring during operation.

For example, it would be possible for the given model to indicate a plausibility range of the sensor data as a function of the state data. This means that instead of accurately predicting the expected sensor data, a certain range of acceptable sensor data is used. This can make it particularly possible normal operation of an impairment of integrity such of an automation system (100) for example;

The method could also include obtaining reference state data from the automation system in a learning phase. The reference state data can describe the operating state of the automation system. The method can also include obtaining reference sensor data in the learning phase. The reference sensor data can also describe the environmental impact of the automation system. Then, an empirical model of the environmental impact can be determined on the basis of carrying out a comparison between the reference state data and the reference sensor data. It is then possible to determine the reference based on the empirical model.

In such an approach, it can be possible to flexibly link a large number of sources of state and sensor data with each other by means of the model. In particular, it is possible to also link together those sources for which a deterministic model cannot simply be derived - especially modular systems can be supported in this way. This can also be the case, for example, with weakly correlated data. This can also be the case if there is a large dimensionality of different data. This can also be the case if, for example, the sensor data is highly noisy, and the signal-to-noise ratio of the sensor data is low.

For example, the empirical model is determined using machine learning techniques. For example, an artificial neural network could be trained, for example by means of reverse propagation. A Kalman filter could also be used. In this way, it can be made possible to reliably determine the model or the reference without much effort and also flexibly to the individual case - for example, a modular system, which is frequently extended or modified.

The learning phase can be carried out, for example, in connection with a supervised operation. For example, it would be possible to access the automation system of external systems during the learning phase. This ensures that the reference state data or the reference sensor data is not falsified. It is also possible for the learning phase to be continuously repeated through the operation of the automation system. In this way, a sudden deviation from the reference could be detected, for example, due to third-party access. Furthermore, it is proposed to update the reference model in the case of authorized access to one or a plurality of components of the automation system, for example, a change in configuration data, a reconfiguration of a production plant (plug-and-work), or an updating device firmware. Furthermore, it is proposed to temporarily stop the method according to the invention for integrity monitoring during such authorized access. In another variant, during such authorized access, the method according to the invention performs monitoring in accordance with a second reference model. The selection of the reference model or the temporary stop can be performed automatically by analysing the operating mode of the automation system (e.g. operating mode, maintenance mode, fault mode).

In various examples, it would also be possible to monitor the operation of another industrial automation system. Then, the reference could be determined on the basis of the monitoring of

the operation of the further industrial automation system. For example, corresponding state data and sensor data could also be obtained for the further industrial automation system and a comparison could be carried out between the state data and the sensor data of the further industrial automation system.

By means of such techniques, a networking between different automation systems can be taken advantage of in such a way that the compromising of a single automation system from this group of automation systems can be detected by comparing it with the remaining automation systems.

The process of carrying out the comparison between the state data and the sensor data furthermore can furthermore comprise carrying out an anomaly detection of sensor data correlated with the state data. This means that in the context of a machine-trained anomaly detection, for example, a deviation of an expected pattern of the sensor data can be detected based on the state data.

If integrity is detected and/or when third-party access to the integrity of the automation system is detected, various actions can be taken. For example, a signal could be output via a user interface, such as a switching signal or an alarm signal. The automation system or at least components of the automation system can be transferred automatically or after confirmation by the operating personnel to a safe state or a protective state. A log file could also be created, depending on the monitoring process. The protocol file can correlate a status of the monitoring process with serial numbers of products of the automation system. This also allows a product to be checked retrospectively to see whether the integrity of the production machines was satisfied during the manufacture of that product.

In an example, a computer program product includes program code that can be run by one or more processors. Running the program

code causes the at least one processor to carry out a method. The method entails obtaining state data from an industrial automation system. The state data describes the operating state of the automation system. The method also entails obtaining sensor data that describes an environmental impact on the automation system. The method also entails performing a comparison between the state data and the sensor data, as well as monitoring the integrity of the automation system based on the comparison.

In an example, a computer program includes program code that can be run by at least one processor. Running the program code causes the at least one processor to carry out a method. The method entails obtaining state data from an industrial automation system. The state data describes the operating state of the automation system. The method also entails obtaining sensor data that describes an environmental impact on the automation system. The method also entails performing a comparison between the state data and the sensor data, as well as monitoring the integrity of the automation system based on the comparison.

In one example, a control unit comprises at least one processor, which is set up to carry out the following steps: obtaining state data from an industrial automation system, wherein the state data describes the operating state of the automation system; and obtaining sensor data that describes an environmental impact of the automation system; and performing a comparison between the state data and the sensor data; and based on the comparison: to monitor the integrity of the automation system.

The examples described above can be combined with each other in further examples.

SHORT DESCRIPTION OF THE FIGURES

FIG. 1 schematically illustrates an automation system in accordance with various examples.

FIG. 2 schematically illustrates a control unit of an automation system in accordance with various examples.

FIG. 3 schematically illustrates a control unit in accordance with various examples.

FIG. 4 is a flowchart of an exemplary method.

FIG. 5 schematically illustrates the obtaining of state data, control data and sensor data in accordance with various examples.

FIG. 6 schematically illustrates the comparison of state data, control data and sensor data by means of a model in accordance with various examples.

FIG. 7 illustrates a schematic time history of a component activity of a component of an automation system described by exemplary state data, as well as an environmental impact of the automation system that is correlated with the component activity.

FIG. 8 schematically illustrates reference state data, reference control data and reference sensor data in accordance with various examples.

FIG. 9 schematically illustrates state data, control data and sensor data from a plurality of automation systems in accordance with various examples.

DETAILED DESCRIPTION OF EMBODIMENTS

The characteristics, features and advantages of this invention, as well as the way in which these are achieved, as described in the above, are explained in a clearer and more comprehensible manner in further detail in relation to the following description of the exemplary embodiments and in conjunction with the drawings.

In the following, the present invention is explained in more detail on the basis of preferred embodiments taking the drawings into consideration. In the figures, identical reference numbers are used to refer to similar or identical elements. The figures are schematic representations of different embodiments of the invention. Elements depicted in the figures are not necessarily shown to scale. Rather, the various elements depicted in the figures are reproduced in such a way that their function and general purpose become comprehensible to the person skilled in the art. Connections and couplings between functional units and elements shown in the figures can also be implemented as an indirect connection or coupling. A connection or pairing can be wired or wirelessly implemented. Functional units can be implemented as hardware, software, or a combination of hardware and software.

Techniques to monitor the integrity of industrial automation systems are described in the following. There can be different reasons that cause an impairment of integrity. An exemplary reason for the impairment of integrity is third-party access to the corresponding automation system, meaning in particular, third-party access.

The techniques described herein are based on a combined monitoring of state data describing an operating state of the automation system, as well as sensor data describing an environmental impact of the automation system. For example, the expected environmental impact can normally be derived from the state data. Such modelling information can then be used to

achieve a comparison of the actual behaviour with the expected behaviour and to determine integrity changes.

The techniques described herein are based in various examples on taking sensor data and state data - which are, for example, IT-related - into account and evaluated together. A check for consistency or plausibility can be made from a comparison of the sensor data with the state data. This results in a new quality of integrity monitoring, as manipulations of sensors or actuators can also be detected, for example. Furthermore, a high degree of robustness is achieved because an unnoticed attack requires consistent manipulation of a large number of integrity data on different systems simultaneously. Furthermore, different types of integrity impairment - for example, manipulation of sensors or actuators, manipulation of the wiring, manipulation of configuration data, manipulation of firmware, manipulation of the control communication, etc. - can be detected and processed together. This can detect the integrity of automation systems of a variety of types. The integrity monitoring techniques described herein relate, in particular, not only to specific IT sub-functions of components of an automation system, but also relate to a comprehensive approach.

The techniques described herein can be flexibly scaled. Expandability is given. Additional sensor data and/or state data can be flexibly taken into account as required. Critical areas of an automation system can also be monitored with greater effort than comparatively uncritical areas. For example, more sensor data or state data could be obtained for critical areas, for example per unit of time.

The techniques described herein also make it possible to retrofit existing automation systems. For example, additional sensors could be specifically used to provide sensor data. This makes it possible to continue to use basically unprotected

operating software, automation components and machine tools or production systems. In general, components of an automation system can be reused that have little or no protection against third-party access themselves.

For example, based on the available techniques, it would be possible to create a log file that logs the result of the monitoring. For example, timestamps could be used. This information could then be used to monitor batches of generated products of the automation system with respect to integrity impairment. In this way, it can also be checked in the aftermath whether the integrity of individual batches of products could be affected, for example, due to inadmissible third-party access or even unauthorized third-party access.

Unauthorized third-party access is often characterized in that an inadmissible modification of an automation system takes place. This can also be done by users who have access authorization, for example, for a service mode, for a component of the system and can, for example, modify the firmware or configuration data of a component. The solution according to the invention improves the resilience, since also inadmissible changes of the plant configuration are recognizable, which are carried out by service technicians or via weak or unprotected service interfaces.

FIG. 1 illustrates schematic aspects with relation to an automation system 100. The automation system 100 comprises a variety of components 101 - 106, 111 - 112, 18 - 119, 120. The components can also be referred to as so-called Internet-of-Things devices.

For example, the components could implement 101 - 106 actuators that cause environmental impact. Such an environmental impact could be, for example, the operation of a production line or the control of traffic control systems.

For example, the components could designate 111 - 112 sensors that measure the environmental impact of the actuators 101 - 106 at least partially.

For example, the components 118 - 119 could implement control functionality that controls one or a plurality of the other components 101 - 106, 111 - 112; this means that the components 118 - 119 can provide resources to a computer hardware. A central control unit 120 is also planned.

In connection with FIG. 1, furthermore, also external sensors 151, 152 are shown; these sensors 151, 152 are not part of the automation system to this extent 100 since they are not connected on a communicative level to the remaining components 101 - 106, 111 - 112, 118 - 120. Such sensors 151, 152 could be installed, for example, specifically with the objective of integrity monitoring and, for example, be installed physically protected. This has the advantage that such a sensor 151, 152 cannot be manipulated by a compromised automation component via the communication connection. In one variant, these system-independent sensors can be given a different weight during evaluation.

In FIG. 1 shows that a third-party access 90 to the integrity of the automation system 100 can occur. For example, the target of third-party access 90 could be an impairment of the functioning of the automation system 100. Third-party access 90 can be inadmissible or even unauthorized.

Techniques are described in the following that make it possible to detect such third-party access 90 and, if necessary, to ward it off.

Corresponding logic can be implemented, for example, in connection with a control unit 160. In the scenario of fig. 1,

the control unit 160 is again not part of the automation system 100. For example, the controller 160 could be part of a backend system. For example, cloud computing or edge computing could be used to operate the control unit 160.

FIG. 2 illustrates aspects relating to the central control unit 120. In some examples, the control unit 120 might also be set up to implement integrity monitoring. The control unit 120 comprises at least one processor 121, for example, a multi-core processor. A memory 122 is provided. There could be program code stored in memory 122. The processor 121 can load and execute the program code from the memory 122. Running the program code can cause the central control unit 120 to perform techniques related to one or a plurality of the following elements: obtaining and/or analysing state data of automation system 100; obtaining and/or analysing sensor data that describes an environmental impact on the automation system; performing a comparison between the state data and the sensor data; and monitoring the integrity of the automation system; and monitoring third-party access to automation system, for example, with the goal of impairing or violating integrity.

FIG. 3 illustrates aspects with relation to the backend control unit 160. The control unit 160 comprises at least one processor 161, for example, a multi-core processor. A memory 162 is provided. There could be program code stored in memory 162. The processor 161 can load and execute the program code from the memory 162. Running the program code can cause the control unit 160 to perform techniques related to one or a plurality of the following elements: obtaining and/or analysing state data of automation system 100; obtaining and/or analysing sensor data that describes an environmental impact on the automation system; performing a comparison between the state data and the sensor data; and monitor the integrity of the automation system.

FIG. 4 is a flowchart of an exemplary method. For example, the method in accordance with the example in FIG. 4 could be carried out by the control unit 120 or by the control unit 160.

Initially, state data is obtained in block 1001. The state data describes the operating state of an automation system. For example, the state data could be obtained from one or a plurality of control units of the automation system or also directly from actuators or sensors of the automation system.

For example, the state data comprise a state of operating software of the automation system. The state data could include at least one element of the following group: a component registration of a variety of active components of the automation system; and a component activity of a variety of components of the automation system; an fault state of an operating software of the automation system; a parameter of a communication interface of the automation system; as well as resource allocation of computer hardware of the automation system.

For example, component registration could list all active components that are registered at a central control unit of the automation system. Logged-off components can be listed accordingly. This provides an overview of which components of the automation system can generally influence the environment.

For example, the component activity could designate a load level or an operating cycle of different components. For example, an amplitude of activity could be described in connection with actuators. In this way, it can be possible to estimate a strength of environmental impact due to actuators of the automation system.

For example, the fault state can correspond to a log file of the operating software. For example, unexpected cancellations

of program software can be stored in it. Faulty memory accesses could also be stored. Averted third-party access could also be stored. All running processes could also be represented.

The parameter of the communication interface of the automation system can, for example, indicate an activity of the communication interface and possible communication partners. For example, the amount of data exchanged could be stored. For example, encryption used might be indexed. For example, the active communication connections and the associated applications could be stored.

For example, resource usage of computer hardware can describe memory utilization or fixed memory utilization, or a load on available processors.

In block 1002, sensor data is obtained. For example, the sensor data can be obtained from one or a plurality of sensors of the automation system. In addition or as an alternative, it would also be possible for the sensor data to be obtained from one or a plurality of external sensors. The sensor data can quantify a physical measured variable or observable one. The measured variable can describe an environmental impact of the automation system. For example, one or a plurality of the following physical observables could be described by the sensor data: temperature; traffic flow; products produced; committee; pressure; volume; speed; position; electricity; tension; generated electrical energy; etc.

Then, in block 1003, a comparison is performed between the state data from block 1001 and the sensor data from block 1002. For example, a correlation between the state data and the sensor data could be performed. A fusion of sensor data and state data could be carried out.
In principle, further data could also be taken into account in the context of the comparison in block 1003. For example, it

would also be possible to obtain control data for one or a plurality of actuators of the automation system, which cause the environmental impact. Then the control data could also be taken into account when comparing in block 1003.

When comparing, a deviation of the environmental impact from a reference could be taken into consideration. This reference can be determined depending on the state data. For example, a deterministic model or also an empirical model could be used.

Finally, in block 1005 (optional), countermeasures and/or alerts can be triggered depending on the monitoring from block 1004. For example, depending on the monitoring, a log file could be created that correlates the status of the monitoring with serial numbers of products of the automation system. In this way, it could also be checked in the aftermath whether individual products or product batches can have been affected by the impairment of integrity. It would also be possible to issue an alert via a user interface depending on the monitoring and/or automatically transfer the operation of the automation system to a state of protection. For example, it can be possible to limit the environmental impact in the state of protection, so that people etc. cannot be harmed. It would also be possible to disable a communication interface of the automation system 100 so that a possible third-party access cannot be actively performed.

FIG. 5 schematically illustrates aspects with relation to a fusion of different data of the automation system. From FIG. 5, it is evident that state data 181 and/or control data 182 are obtained from a subset of actuators 101, 103, 105. The state data 181 can describe and operating state of the respective actuator 101, 103, 105. The control data 182 can describe a way or a strength of the environmental impact of the respective actuator 101, 103, 105.

In addition, from the sensors 111, 112, 151, 152 sensor data 183 are obtained. The sensor data describes the environmental impact of the automation system 100.

In the example of FIG. 5, state data 181 are furthermore collected by the hardware resources 118; 119. In addition, 120 state data 181 is recorded from the central control unit.

All these data 181, 182, 183 are provided to the control unit 160. The latter can then carry out a fusion of the data, meaning a comparison between the various data 181, 182, 183. Based on this comparison, the integrity of automation systems can be monitored. That is also in connection with FIG. 6.

FIG. 6 illustrates aspects with relation to comparing various data 181, 182, 183. FIG. 6, in particular, illustrates a functionality, for example, of the control data 160 or of the control unit 120 with relation to monitoring integrity, wherein, for example, impairment of the integrity due to impermissible or even unauthorized third-party access 90 can be detected.

From FIG. 6, it is evident that a model 250 is used for the comparison. As a result, a result signal 189 is obtained. For example, the result signal 189 can be indicative of whether or not there is an impairment of integrity and/or third-party access 90. The result signal 189 could indicate a corresponding probability. The result signal can trigger warnings and/or countermeasures.

In some examples, a deterministic model 250 can be used. The deterministic model 250 can be predetermined and can be created, for example, on the basis of physical connections or the architecture of the automation system 100. For example, it would be possible for the model 250 to indicate a plausibility range of the sensor data as a function of the state data 181.

The comparison can then be carried out to verify whether the sensor data indicate an environmental impact within this area of plausibility; if this is not the case, integrity can be assumed to be compromised. Such techniques are illustrated in connection with FIG. 7.

FIG. 7 illustrates aspects with relation to comparing state data 181 and sensor data 183. For example, the 250 model could implement a corresponding functionality.

In the example of FIG. 7, the state data 181 indicate the activity 301 of an actuator as a function of time. In the example of FIG. 7, the activity of the actuator 301 fluctuates between two values (solid line).

In FIG. 7, the reference 310 is also shown, which is obtained based on the model 250 on the basis of the activity 301 (dotted line). A corresponding plausibility range 311 is shaded. A deviation from the plausibility range 311 could be detected, for example, in connection with an anomaly detection.

In FIG. 7, the time progression of the environmental impact 306 measured by the sensor data 183, for example, the temperature in the surroundings of the corresponding actuator, is shown. It is evident that at a certain point in time the distance 312 between the measured environmental impact 306 on the one hand and the reference 310 on the other hand leaves the plausibility range 311; there, an impairment of integrity can be assumed, for example, due to third-party access 90.

A corresponding model 250 cannot only be derived deterministically, for example, by a digital twin simulation model created during the construction of a machine or plant. Machine learning techniques could also be used. This is shown in connection with FIG. 8.

FIG. 8 illustrates aspects with relation to determining the reference 310 or the model 250. In FIG. 8, it is shown that, during an operating phase 191, the data 181, 182, 183 are obtained the system 100 or the sensors 151, 152, Integrity monitoring occurs during the operational phase.

During two learning phases 192, 193 reference state data 181A, 181B, as well as reference sensor data 183A, 183B are obtained. Reference control data 182A, 182B can also be obtained as an option. In general, only one learning phase is required.

For example, learning phase 193 could be defined in the context of a rollout of automation system 100. Monitored operation can take place there. The learning phase 192 could correspond to the normal operation of the automation system 100, for example, describing historical data 181A, 182A, 183A.

It is then possible that an empirical model 250 based on a comparison between these reference data 181A, 182A, 183A, 181B, 182B, 183B is determined. Then, the reference 310 can be determined, in particular, as a deviation from normal operation. There is no need to elaborately determine a deterministic model. In addition, different sources of data can be flexibly taken into account, thus promoting the extensibility of the 250 model. For example, the empirical model determination of the model 250 could take place by using machine learning techniques.

Alternatively or in addition to such a definition of reference data in the period with respect to the learning phases 192, 193, it would also be possible to derive reference 310 from the operation of another automation system. Corresponding techniques are illustrated in connection with FIG. 9.

FIG. 9 illustrates aspects with relation to determining the reference 310 or the model 250. In FIG. 9, it is shown that, in

addition to monitoring the operation of the automation system 100, the operation of another automation system 100' can also be monitored. Corresponding reference state data 181', reference control data 182' and reference sensor data 183' can be obtained from the further automation system 100'. In this way, the reference 310 can be determined.

Of course, the features of the previously described embodiments and aspects of the invention can be combined with each other. In particular, the features can be used not only in the described combinations, but also in other combinations or on their own, without leaving the field of the invention.

For example, the techniques described herein can also be used to monitor the integrity of other systems, for example, generally of sensor-actuator systems, such as autonomous machines, etc.

While several examples have been described above related to the impairment of the integrity of automation systems due to third-party access, in some other examples however, it would also be possible to monitor the integrity based on other triggering events.

PATENTKRAV

1. Fremgangsmåte som omfatter:

- å oppnå tilstandsdata (181) som er relatert til et industrielt automasjonssystem (100), der tilstandsdataene (181) beskriver den operasjonelle tilstanden (301) til automasjonssystemet (100),

- å oppnå sensor-data (183) som beskriver en miljøpåvirkning (306) for automasjonssystemet (100),

karakterisert ved

- å utføre en sammenligning mellom tilstandsdataene (181) og sensordataene (183), og

- på basis av sammenligningen: å overvåke integriteten til automasjonssystemet (100),

der fremgangsmåten også omfatter:

- oppnå kontrolldata (182) for én eller flere aktuatorer (101-106) i automasjonssystemet (100) som forårsaker miljøpåvirkningen (306),

der sammenligningen blir utført mellom tilstandsdataene (181), sensordataene (183) og kontrolldataene (182).

2. Fremgangsmåte ifølge krav 1,

der tilstandsdataene (181) omfatter en tilstand for driftsprogramvare for automasjonssystemet (100).

3. Fremgangsmåte ifølge krav 1 eller 2,

der tilstandsdataene (181) omfatter minst ett element fra den følgende gruppen:

- en komponentregistrering for et flertall av aktive komponenter (101-106, 111, 112, 118, 119) i automasjonssystemet (100),

- en komponentaktivitet for et flertall av komponenter (101-106, 111, 112, 118, 119) i automasjonssystemet (100),

- en feiltilstand for driftsprogramvare i automasjonssystemet (100),
- en parameter for et kommunikasjonsgrensesnitt i automasjonssystemet (100), og
- en ressursallokering for datamaskinmaskinvare i automasjonssystemet (100).

4. Fremgangsmåte ifølge ett av de foregående krav,

der sammenligningen tar hensyn til et avvik i miljøpåvirkningen (306) fra en referanse (310).

5. Fremgangsmåte ifølge krav 4,

som også omfatter:

- å bestemme referansen (310) på bakgrunn av en forhåndsdefinert deterministisk modell (250) og som en funksjon av tilstandsdata (181).

6. Fremgangsmåte ifølge krav 5,

der den forhåndsdefinerte modellen (250) indikerer et rimelighetsområde (311) for sensordataene (183) som en funksjon av tilstandsdataene (181).

7. Fremgangsmåte for ifølge ett av kravene 4-6,

som også omfatter:

- å oppnå referansetilstandsdata (181A, 181B) som er relatert til automasjonssystemet (100) i en læringsfase (192, 193), der referansetilstandsdataene (181A, 181B) beskriver den operasjonelle tilstanden (301) til automasjonssystemet (100),
- å oppnå referansesensordata (183A, 183B) i læringsfasen (192, 193), der referansesensordataene (183A, 183B) beskriver miljøpåvirkningen (306) til automasjonssystemet (100),

- å bestemme en empirisk modell (250) for miljøpåvirkningen (306) på basis av utførelse av en sammenligning mellom referansetilstandsdataene (181A, 181B) og referansesensordataene (183A, 813B), og
- å bestemme referansen (310) på basis av den empiriske modellen (250).

8. Fremgangsmåte ifølge krav 7,

der den empiriske modellen (250) blir bestemt ved å benytte maskinlæringsteknikker.

9. Fremgangsmåte ifølge ett av kravene 4-8,

som også omfatter:

- å overvåke driften av et ytterligere industrielt automasjonssystem (100'),
- å bestemme referansen (310) på basis av overvåkningen av driften av det ytterligere industrielle automasjonssystemet (100').

10. Fremgangsmåte ifølge ett av de foregående krav,

der prosessen med utførelse av sammenligningen omfatter å utføre en anomalideteksjon av sensordata (183) korrelert med tilstandsdataene.

11. Fremgangsmåte ifølge ett av de foregående krav,

som også omfatter:

- på basis av overvåkningen: å danne en log-fil som korrelerer en status for overvåkningsprosessen med serienumre på produkter i automasjonssystemet (100).

12. Fremgangsmåte ifølge ett av de foregående krav,

som også omfatter:

- på basis av overvåkningen: å utgi en advarsel via et brukergrensesnitt og/eller endre driften av automasjonssystemet (100) til en beskyttende tilstand.

13. Kontrollenhet (120, 160) som omfatter minst én prosessor som er innrettet til å utføre de følgende trinnene:

- å oppnå tilstandsdata (181) som er relatert til et industrielt automasjonssystem (100), der tilstandsdataene (181) beskriver den operasjonelle tilstanden (301) til automasjonssystemet (100),

- å oppnå sensordata (183) som beskriver en miljøpåvirkning (306) for automasjonssystemet (100),

karakterisert ved

- å utføre en sammenligning mellom tilstandsdataene (181) og sensordataene (183), og

- på basis av sammenligningen: å overvåke integriteten til automasjonssystemet (100) for også å utføre det følgende trinnet:

- å oppnå kontrolldata (182) for én eller flere aktuatorer (101-106) i automasjonssystemet (100) som forårsaker miljøpåvirkningen (306),

der sammenligningen blir utført mellom tilstandsdataene (181), sensordataene (183) og kontrolldataene (182).

14. Kontrollenhet (120, 160) ifølge krav 13,

der den minst ene prosessoren er innrettet til å utføre fremgangsmåten ifølge ett av kravene 2-12.

15. Datamaskinprogram som omfatter programkode som kan bli eksekvert av minst én prosessor og forårsaker at den minst ene prosessoren utfører fremgangsmåten ifølge ett av kravene 1-12.

FIG 1

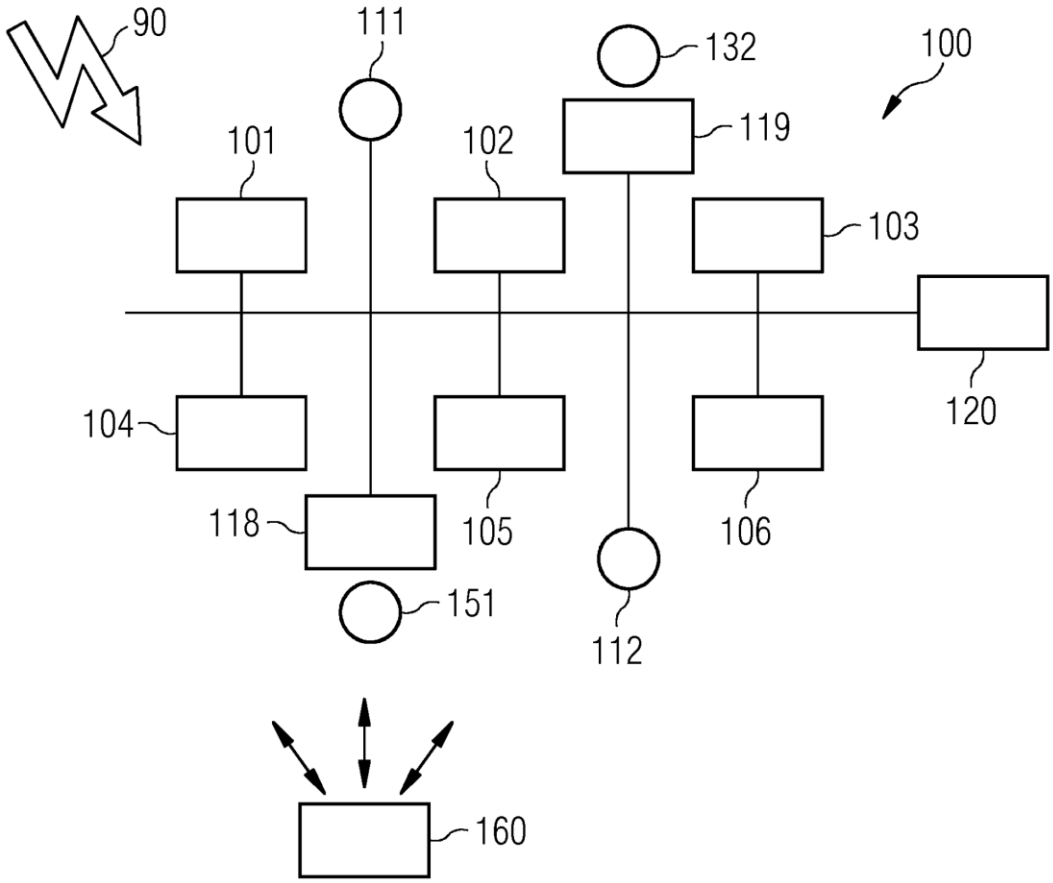
90
111
132
100
119
101
102
103
120
104
118
105
106
151
112
160

FIG 2

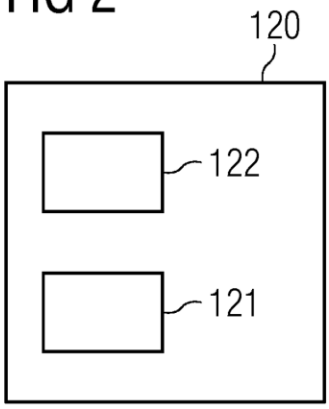
120
122
121

FIG 3

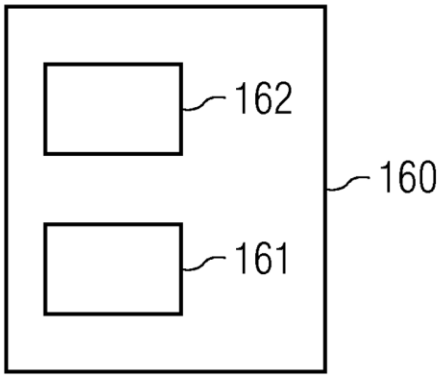

FIG 4

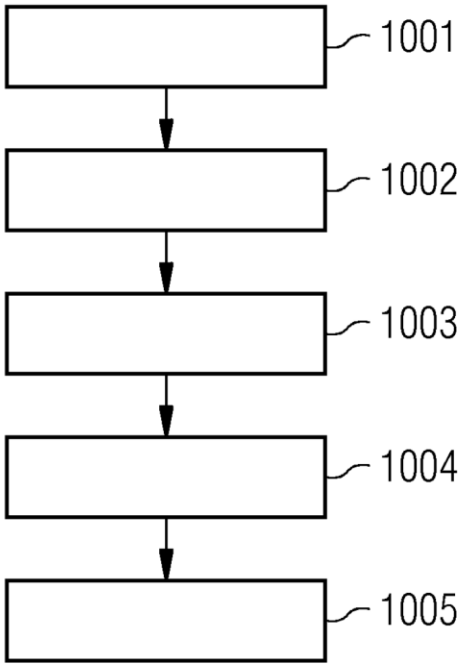

FIG 5

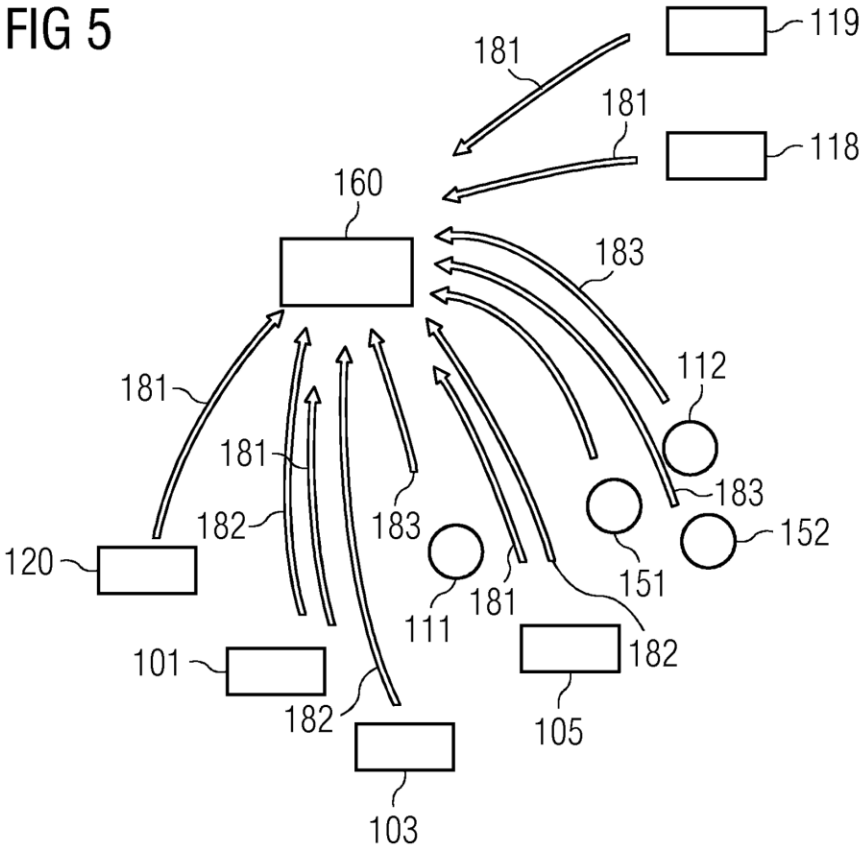
119
181
181
118
160
183
112
181
181
183
183
152
182
120
111
181
151
182
101
182
105
103

FIG 6

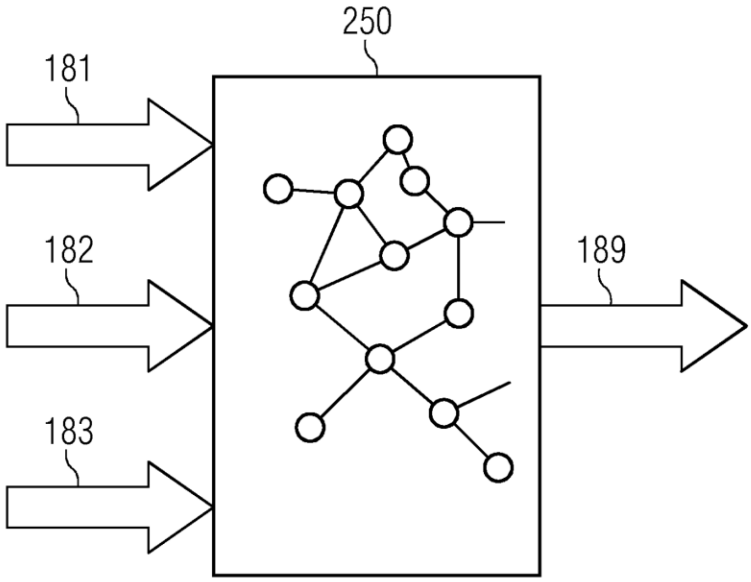
250
181
182
189
183

FIG 7

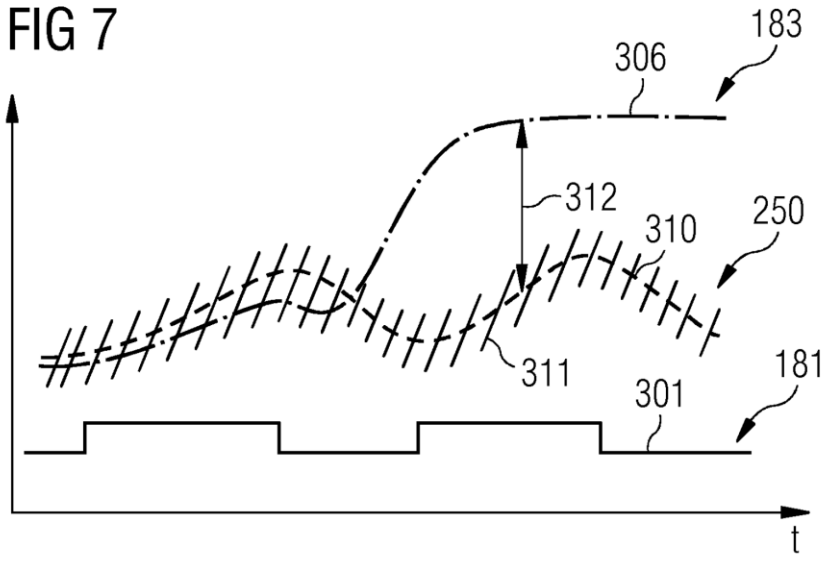

FIG 8

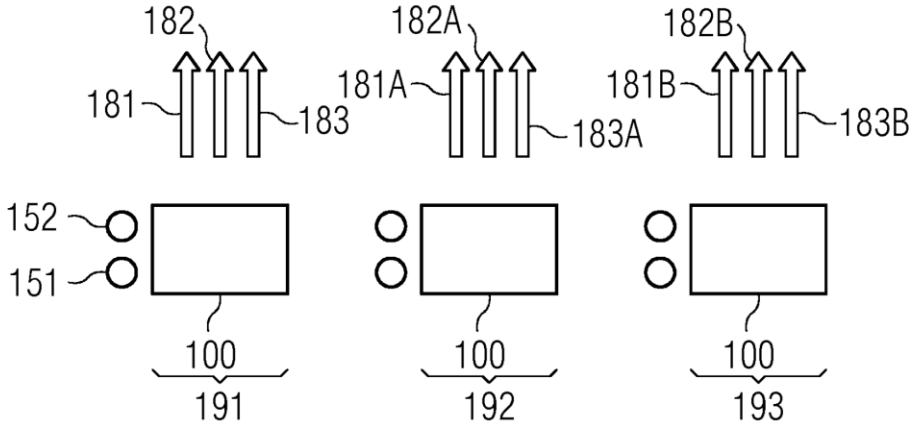

FIG 9