

SYSTEM AND METHOD FOR CONTROLLING A ROBOT

The invention relates to a system and a method for controlling a robot. The invention further
5 relates to a robot with such a system. The proposed system and method serve in particular to
increase the functional safety during operation of the robot.

Today, robots with movable parts (one or more robot manipulators, etc.) are increasingly used
in areas where the robots complete tasks interacting with humans. Here, it is necessary to
10 design the robots such that they have a high functional safety and a high safety integrity.

The object of the invention is to provide a system and a method for controlling a robot that
allow an improved functional safety and safety integrity of the robot during operation.

15 The invention will become apparent from the features of the independent claims.
Advantageous further developments and embodiments are the subject matter of the dependent
claims. Other features, possible applications and advantages of the invention will become
apparent from the following description, as well as the explanation of exemplary
embodiments of the invention shown in the figures.

20

A first aspect of the invention relates to a system for controlling a robot. The robot comprises
an interface that provides data $DAT(t)$, captured by one or more sensors, that indicate a current
state $ZUS(t)$ of the robot, a first processor, connected to the interface, that is set up to use a
first algorithm to check, on the basis of the data $DAT(t)$ and a prescribed state space $\underline{Z}$, which
25 indicates exclusively permitted states of the robot, whether it holds that: $ZUS(t) \in \underline{Z}$, wherein
in the event of: $ZUS(t) \notin \underline{Z}$ a first stop signal is generated, a unit, connected to the first
processor via a data link, for generating a second stop signal, wherein the second stop signal
is generated when the unit receives the first stop signal or when the data link is interrupted, a
second processor, connected to the interface and the first processor or only to the first
30 processor, that is set up to use a second algorithm to check, on the basis of the data $DAT(t)$
and the prescribed state space $\underline{Z}$, whether it holds that: $ZUS(t) \in \underline{Z}$, wherein in the event of
 $ZUS(t) \notin \underline{Z}$ the data link between the first processor and the unit is interrupted, and a control

unit, connected to the unit, for controlling the robot that controls the robot into a prescribed safe state when the second stop signal is present.

5 Herein, the term “current state $ZUS(t)$ of the robot” is understood broadly. It comprises in particular a static and/or dynamic mechanical and/or electric current state $ZUS(t)$ of the robot. The term further comprises states, where the robot interacts mechanically or electrically with its environment. Corresponding sensors for capturing the parameters defining the current state $ZUS(t)$ and for generating the corresponding data $DAT(t)$ are known in the prior art. In particular, the current state $ZUS(t)$ is to be understood as a multidimensional vector having
10 individual state parameters. The data $DAT(t)$ indicate the values of the state parameters defining the state $ZUS(t)$. The current state $ZUS(t)$ and the associated data $DAT(t)$ are both time dependent, wherein t indicates the time.

The data $DAT(t)$ defining the current state $ZUS(t)$ are provided to the first processor via an
15 interface. In addition, the first processor is provided with the state space $\underline{Z}$ or the boundary for the state space $\underline{Z}$, wherein the state space $\underline{Z}$ indicates exclusively permitted states of the robot. The state space $\underline{Z}$ can also be provided to the first processor as a parametric description of the permitted states. The first processor executes a first algorithm that checks, on the basis of the data $DAT(t)$ and the prescribed state space $\underline{Z}$, whether the current state $ZUS(t)$ is an
20 element of the state space $\underline{Z}$. If this check reveals that the current state $ZUS(t)$ is not an element of the state space $\underline{Z}$, a first stop signal is generated. The first stop signal is preferably an electric or optical signal.

The first processor is further connected to the unit via a data link for generating a second stop
25 signal. This data link is advantageously designed for signal routing of electric and optical signals. This data link is advantageously designed as an Ethernet connection. In particular, this data link is set up and designed to transmit the first stop signal, generated by the first processor, to the unit. According to the invention, the unit is further designed and set up such that, if it receives a first stop signal sent by the first processor or if the unit determines that the
30 data link to the first processor is interrupted, the unit generates a second stop signal. For this purpose, the unit is advantageously set up to monitor the presence of an uninterrupted data link between the first processor and the unit, for example, on the basis of data transmission via a safety data protocol.

According to the invention, the second stop signal is transmitted to the control unit of the robot and prompts the control unit to control the robot into a prescribed safe state. Herein, the control unit in particular controls the actuators of elements of the robot that are driven by actuators. Advantageously, the control unit is the central control unit of the overall robot, which thus controls or regulates all controllable functions and states of the robots. The control unit can further comprise locally distributed control units, that, for example, each comprise the control electronics units locally assigned to the actuators.

Herein, the term “safe state” is understood broadly. For example, it comprises braking all movable parts of the robot to a prescribed position or braking all movable parts of the robot to a standstill without prescription of a position, or reducing the movement speed of the movable parts of the robot to a prescribed speed etc. In addition, the “safe state” can comprise a safe electric and/or data-related state. For example, after receiving the second stop signal, the control unit can prompt a data backup and/or electrically isolate specific subunits of the robot system etc. In one variant, the second stop signal is transmitted to actuator units of the robot. The safe state is advantageously prescribed according to the task of the robot and advantageously meets the condition that, in the safe state, the robot does not pose any risk for its environment or the robot itself.

According to the invention, the second processor is connected to the interface and the first processor or only to the first processor, so that the second processor receives the data $DAT(t)$ defining the current state $ZUS(t)$ either from the interface or from the first processor, as well. The second processor executes a second algorithm, which is used to check, on the basis of a prescribed state space $\underline{Z'}$, whether the current state $ZUS(t)$ is an element of the state space $\underline{Z'}$. If it is determined that the current state $ZUS(t)$ is not an element of the state space $\underline{Z'}$, the second processor prompts an interruption of the data link between the first processor and the unit. For this purpose, the second processor advantageously controls an interruption element, for example, a switch, that advantageously physically interrupts the data link. As an alternative to a physical interruption of the data link, an interruption of the data link can, for example, also be generated by generating a short circuit of all electric lines of the data link against a prescribed fixed potential.

The state spaces $\underline{Z}$ and $\underline{Z}'$ are advantageously selected such that it is ensured that checking of a state $ZUS(t)$ by the first processor and the second processor leads to a consistent result. The state spaces $\underline{Z}$ can also $\underline{Z}'$ be identical.

- 5 An advantageous further development of the proposed system is characterized in that the second processor is set up on the first processor for monitoring the execution of the first algorithm, wherein the second processor, upon establishing a faulty execution of the first algorithm, advantageously interrupts the data link between the first processor and the unit.
- 10 Monitoring of the first processor by the second processor advantageously includes firstly monitoring whether the first processor executes the first algorithm at all or not, as well as secondly monitoring whether the first processor executes the first algorithm without fault. In the event of a non-execution of the first algorithm (for example, because the algorithm encountered a fault or the processor is damaged) by the first processor or in the event of a
15 faulty execution of the first algorithm by the first processor, the data link between the first processor and the unit is advantageously interrupted by the first processor. As mentioned above, this event results in the generation of a second stop signal and, as a consequence, in the robot assuming the safe state.
- 20 An advantageous further development of the proposed system is characterized in that the first processor is set up on the second processor for monitoring the execution of the second algorithm, wherein the first processor, upon establishing a faulty execution of the second algorithm (which advantageously includes a non-execution), generates a first stop signal and/or a warning signal. If the first stop signal is generated, it is transmitted to the unit, where
25 it generates the second stop signal, as a consequence of which the robot assumes the safe state. The warning signal is advantageously transmitted to an output unit, which is set up and designed as an optically and/or acoustically perceptible signal for outputting the warning signal. If the second processor in this further development interrupts the data link between the first processor and the unit due to a fault in the execution of the second algorithm, then the
30 control of the robot is functionally safe. If a fault occurs in the execution of the second algorithm by the second processor that, however, does not result in an interruption of the data link between the first processor and the unit, in this further development, this is detected by the first processor, so that the first processor generates a first stop signal and transmits it to

the unit via the data link, so that this generates a second stop signal that prompts the robot to be transferred into a safe state.

5 An advantageous further development of the proposed system is characterized in that, that there is a switch controlled by the second processor to interrupt the data link between the first processor and the unit. The switch is advantageously designed as an electric or optical switch. In a switching status that corresponds to the interruption of the data link, the switch can also generate a short circuit of the electric data line. The data link is advantageously physically interrupted by the switch. The data link is advantageously a symmetrically encoded data link.
10 These data links ensure safe data transmission.

The second processor is advantageously arranged on a unit, such as, for example, a plug-in card or an extension module, that is provided as an extension of the first processor as a standard.

15 A particularly advantageous further development of the proposed system is characterized in that a second chip set of the second processor is connected to a first chip set of the first processor via a PCI, PCI-X or PCIe connection or similar technical solutions. The term “PCI” (“Peripheral Component Interconnect”) herein refers to a bus standard for connecting
20 peripheral devices to a chip set of a processor. The second processor is advantageously arranged on a PCI card that is inserted on the main board of the first processor. The first and the second chip set are advantageously arranged on an integrated processor chip.

Also advantageously, the first and the second processor are different processor types.

25 Also advantageously, the first algorithm and the second algorithm are different algorithms or at least different programming in one and the same algorithm. By different processor types or differently executed algorithms, the functional safety of the system for controlling a robot can be significantly increased. If the first algorithm and the second algorithm are different, this
30 generally requires different state spaces $\underline{Z}$ and $\underline{Z}'$. As already described above, these are advantageously selected such that it is ensured that checking of a state $ZUS(t)$ by the first processor and the second processor leads to a consistent result.

In particular, the proposed system allows to realize continuously increasing requirements for robot controls regarding the functional safety by means of a simple and cost-efficient system.

If the second processor is designed as a PCI card, the following advantages are obtained in particular:

1. reduced installation effort, as no cables are required and an integrated energy supply can be used,
2. there is no risk of confusion with other, for example, Ethernet connections, as no additional connections are required,
3. a high data throughput is enabled, which in turn allows the exchange of complex data without significant time delay, so that complex safety checks are possible, and
4. use of both processors (first and second processor) to increase the computing performance is possible due to the high data throughput.

The connection between the first processor and the unit is advantageously implemented as an Ethernet connection. An Ethernet controller for a fieldbus for controlling the robot is advantageously arranged on the second processor, but is logically assigned to the first processor. Thus, a standard controller can be used from the first processor, so that no changes to the software used on the first processor for the data link are required (transparent coupling). An analogue switch, controlled by the second processor, is advantageously provided for interrupting the Ethernet connection between the first processor and the unit. This analogue switch can physically interrupt the Ethernet connection. Thus, bypassing of the switch-off by the Ethernet controller is not possible. Due to the analogue switch being controlled by the second processor, a real independent hardware path for a second channel in the system is available. This results in reduced loading times compared to solutions with distributed computing of safe data packages for controlling the robot. The safe signal is generated by switching off or interrupting the communication between the first processor and the unit. The second processor is advantageously not required to contribute output data to the control unit within a bus cycle. In particular, the proposed system allows the safe switch-off of the robot to be addressed in a simple manner. The robot must be able to address the event of an interrupted communication anyway, as it may be caused by faults in the connection cable. In this event, the robot automatically assumes the safe state.

The proposed system as a whole allows a control of a robot with increased functional safety.

Another aspect of the present invention relates to a robot with a system as described above.

- 5 Another aspect of the present invention relates to a method for (safely) controlling a robot. The proposed method comprises the following steps.

In one step, data $DAT(t)$ indicating a current state $ZUS(t)$ of the robot, captured by one or more sensors, are provided by an interface. In another step, a first algorithm, executed on a first processor, is used to check, on the basis of the data $DAT(t)$ and a prescribed state space $\underline{Z}$ or the boundary for the state space $\underline{Z}$, which indicates exclusively permitted states of the robot, whether it holds that: $ZUS(t) \in \underline{Z}$, wherein in the event of: $ZUS(t) \notin \underline{Z}$ a first stop signal Sig1 is generated. In another step, a unit, connected to the first processor via a data link, generates a second stop signal Sig2 when the unit receives the first stop signal Sig1 or when the data link is interrupted. In another step, a second processor, connected to the interface and the first processor or only to the first processor, uses a second algorithm, executed on the second processor, to check, on the basis of the data $DAT(t)$ and a prescribed state space $\underline{Z}'$, whether it holds that: $ZUS(t) \in \underline{Z}'$, wherein in the event of $ZUS(t) \notin \underline{Z}'$ the data link between the first processor and the unit is interrupted. In another step, a control unit, connected to the unit, for controlling the robot controls the robot into a prescribed safe state when the second stop signal Sig2 from the control unit is present.

Advantages and advantageous further developments of the proposed method will become apparent by means of a similar and analogous transfer of the statements made in connection with the proposed system.

The object of the invention is further achieved by a computer system with a data processing apparatus, wherein the data processing apparatus is designed such that a method, as described above, is executed on the data processing apparatus.

30

In addition, the object of the invention is achieved by a digital storage medium with electronically readable control signals, wherein the control signals can interact with a programmable computer system in such a way that a method, as described above, is executed.

The object of the invention is further achieved by a computer program product with program code for executing the method, as described above, stored on a machine-readable medium, if the program code is executed on a data processing apparatus.

5

Finally, the invention relates to a computer program with program codes for executing the method, as described above, if the program runs on a data processing apparatus. For this purpose, the data processing apparatus can be designed as any known computer system known from the prior art.

10

Other advantages, features and details will become apparent from the following description, in which at least one exemplary embodiment is described in detail, with reference to the drawings, if applicable. Like, similar and/or analogue parts are indicated by like reference numerals.

15

In the drawings:

Fig. 1 shows a schematic diagram of a variant of the proposed system.

20

Fig. 1 shows a schematic diagram of a variant of the proposed system for controlling a robot 102. The robot 102 here has a multi-membered robot manipulator driven by an actor. The system further comprises an interface 101 that provides data $DAT(t)$, captured by several sensors 100, that indicate a current state $ZUS(t)$ of the robot manipulator. In the present exemplary embodiment, the state $ZUS(t)$ indicates forces and torques occurring at the individual members of the robot manipulator, wrenches acting externally on the individual members, as well as positions, orientations, speeds and accelerations of the individual members.

25

30

The interface 101 is connected to the first processor 103. The data $DAT(t)$ indicating the current state $ZUS(t)$ are thus provided to the first processor 103. The first processor 103 executes a first algorithm that checks, on the basis of the provided data $DAT(t)$ and a prescribed state space $\underline{Z}$, which indicates exclusively permitted states of the robot 102 or the robot manipulator, whether the current state $ZUS(t)$ is an element (ϵ) of the state space $\underline{Z}$:

$ZUS(t) \in \underline{Z}$. If it is determined that it holds that: $ZUS(t) \notin \underline{Z}$, a first electric stop signal Sig1 is generated.

5 The system further comprises a unit 105, connected to the first processor 103 via a data link 104, that serves for generating a second electric stop signal Sig2, wherein the second stop signal Sig2 is generated by the unit when the unit 105 receives the first stop signal Sig1 or when the unit 105 establishes that the data link 104 is interrupted.

10 The interface 101 is further connected to a second processor 106 that has a different chip set or a processor with a different processor architecture than the first processor 103. The first 103 and second 106 processor are thus of a different design. The interface 101 simultaneously provides the second processor 106 with the data DAT(t). The second processor 106 is set up to use a second algorithm to check, on the basis of the data DAT(t) and a prescribed state space $\underline{Z}'$, whether it holds that: $ZUS(t) \in \underline{Z}'$, wherein in the event of $ZUS(t) \notin \underline{Z}'$ the data link
15 104 between the first processor 103 and the unit 105 is interrupted by controlling an analogue switch 114. The first algorithm is different from the second algorithm, however, both algorithms perform the checks described above.

20 Finally, the system comprises a control unit 107, connected to the unit 105, for controlling the robot 102, which controls the robot 102 into a prescribed safe state when it receives the second stop signal Sig2.

25 Although the invention has been further illustrated and explained by way of preferred exemplary embodiments, the invention is not limited by the disclosed examples and other variations can be derived therefrom by the person skilled in the art, without departing from the scope of the invention. It is thus understood that a plurality of possible variations exists. It is also understood that embodiments presented by way of example are really merely examples that should not be construed as limiting the scope, the possible applications or the configuration of the invention in any way. The above description and the description of the
30 figures rather enable the person skilled in the art to concretely implement the exemplary embodiments, wherein the person skilled in the art, having knowledge of the disclosed inventive concept, can make numerous changes, for example, with respect to the function or the arrangement of individual elements, mentioned in an exemplary embodiment, without

departing from the scope defined by the claims and their legal equivalences, such as further explanations in the description.

List of reference numerals

	100	Sensors
	101	Interface
5	102	Robot
	103	First processor
	104	Data link between the first processor and the unit
	105	Unit
	106	Second processor
10	107	Control unit
	114	Interruption unit/switch

CLAIMS

1. A system for controlling a robot (102), comprising:
 - an interface (101) that provides data $DAT(t)$ captured by one or more sensors (100),
5 wherein the data $DAT(t)$ indicate a current state $ZUS(t)$ of the robot (102),
 - a first processor (103), connected to the interface (101), that is set up to use a first algorithm to check, on the basis of the data $DAT(t)$ and a prescribed state space $\underline{Z}$ or a boundary for the state space $\underline{Z}$, which indicates exclusively permitted states of the robot (102), whether it holds that: $ZUS(t) \in \underline{Z}$, wherein in the event of:
10 $ZUS(t) \notin \underline{Z}$ a first stop signal Sig1 is generated,
 - a unit (105), connected to the first processor (103) via a data link (104), that serves for generating a second stop signal Sig2, which generates the second stop signal when the unit (105) receives the first stop signal Sig1 or when the unit (105) establishes that the data link (104) is interrupted,
 - 15 - a second processor (106), connected to the interface (101) and the first processor (103) or only to the first processor (103), which is set up to use a second algorithm to check, on the basis of the data $DAT(t)$ and a prescribed state space $\underline{Z'}$ or a boundary for the state space $\underline{Z'}$, whether it holds that: $ZUS(t) \in \underline{Z'}$, wherein in the event of $ZUS(t) \notin \underline{Z'}$ the second processor (106) prompts an interruption unit
20 (114) to interrupt the data link (104) between the first processor (103) and the unit (105), and
 - a control unit (107), connected to the unit (105), for controlling the robot (102), which control unit controls/regulates the robot (102) into a prescribed safe state when the second stop signal Sig2 is present.
- 25 2. The system according to claim 1,
 wherein the second processor (106) is set up for monitoring the execution of the first algorithm on the first processor (103), wherein the second processor (106), upon establishing a faulty execution of the first algorithm interrupts the data link (104).
- 30 3. The system according to claim 1 or 2,
 wherein the first processor (103) is set up for monitoring the execution of the second algorithm on the second processor (106), wherein the first processor (103), upon

establishing a faulty execution of the second algorithm, generates a first stop signal Sig1 and/or a warning signal.

4. The system according to claim 3,
5 wherein an output unit is present, which is set up and designed as an optically and/or acoustically perceptible signal for outputting the warning signal.
5. The system according to any one of claims 1 to 4,
10 wherein the interruption unit (114) is a switch controlled by the second processor (106).
6. The system according to any one of claims 1 to 5,
wherein a second chip set of the second processor (106) is connected to a first chip set of the first processor (103) via a PCI, PCI-X or PCIe connection.
- 15 7. The system according to any one of claims 1 to 6,
wherein the first processor (103) and the second processor (106) are different processor types.
8. The system according to any one of claims 1 to 7,
20 wherein the first algorithm and the second algorithm are different algorithms.
9. A method for controlling a robot (102), with the following steps:
 - by means of an interface (101) providing data $DAT(t)$ indicating a current state $ZUS(t)$ of the robot (102), captured by one or more sensors (100),
 - 25 - using a first algorithm, executed on a first processor (103), to check, on the basis of the data $DAT(t)$ and a prescribed state space $\underline{Z}$ or a boundary for the state space $\underline{Z}$, which indicates exclusively permitted states of the robot (102), whether it holds that: $ZUS(t) \in \underline{Z}$, wherein in the event of: $ZUS(t) \notin \underline{Z}$ a first stop signal Sig1 is generated,
 - 30 - by means of a unit (105), connected to the first processor (103) via a data link (104), generating a second stop signal Sig2, which generates the second stop signal when the unit (105) receives the first stop signal Sig1 or when the data link (104) is interrupted,

- by means of a second processor (106), connected to the interface (101) and the first processor (103) or only to the first processor (103), using a second algorithm, executed on the second processor (106), to check, on the basis of the data DAT(t) and a prescribed state space $\underline{Z'}$ or a boundary for the state space $\underline{Z'}$, whether it holds that: $ZUS(t) \in \underline{Z'}$, wherein in the event $ZUS(t) \notin \underline{Z'}$ the data link (104) between the first processor (103) and the unit (105) is interrupted, and
- by means of a control unit (107), connected to the unit (105), for controlling the robot (102), controlling/regulating the robot (102) into a prescribed safe state when the second stop signal Sig2 from the control unit (107) is present.

10

10. A robot with a system according to any one of claims 1 to 8.