INTERNATIONAL JOURNAL OF CIRCUITS, SYSTEMS AND SIGNAL PROCESSING
DOI: 10.46300/9106.2020.14.132 Volume 14, 2020

Safe position detection based on Safety System-on-Chip (SSoC) for wireless IoT application

Josef Börcsök
ICAS, Institute for Computer Architecture and System Programming
University of Kassel
Kassel, Germany

Muhammad Ikram Hafiz
ICAS, Institute for Computer Architecture and System Programming
University of Kassel
Kassel, Germany

Ahmed Alsuleiman
ICAS, Institute for Computer Architecture and System Programming
University of Kassel
Kassel, Germany

Michael Schwarz
ICAS, Institute for Computer Architecture and System Programming
University of Kassel
Kassel, Germany

Mohamed Abdelawwad
ICAS, Institute for Computer Architecture and System Programming
University of Kassel
Kassel, Germany

***Abstract*— Cyber Physical Systems (CPS) are predestined for use in Industry 4.0 applications. However, the interaction between the virtual and physical world also creates risks that is essential to be controlled. In highly automated industrial systems, for example, robots are used in confined spaces together with working humans. The risk posed by such systems endangers, among others, the people working there. This paper presents an approach to ensure the safety of the situation described above, which makes the workspace of industrial robots safer by implementing a safe workspace detection system. This system comprises several detection sensors implemented in a 2oo3 safety architecture and a Safety System on a Chip (SSoC) based on a safe 1oo2 system architecture. The safety-related redundancy provided by the detection and calculation elements enables a safe position detection of the robotic arm in the 3-dimensional space. The presented system monitors the position of the robotic arm and thus supports the safety of the surrounding objects and the people working there by leading to a safe standstill or to a reduced speed of movement of the robot as soon as the defined and permitted working space is left.**

Keywords: Signals, Signal Processing, Systems, Applied Systems Theory, Systems Theory, Control, Robotics, Safety Systen-on-Chip, Safe Positioning, IIoT, Industrial Robotics

I. Introduction

At present, IIoT and Industry 4.0 are booming, e.g. by using such systems in smart factories. Through this development step, the connections between the physical world and the virtual world are established by Cyber Physical Systems (CPSs) and supported by the Industrial Internet of Things (IIoT) [1]. To realise such smart factories, complex electronic systems are implemented. However, the increasing complexity of electronic systems increases the probability of failure of these systems [2]. For this reason, the prevention or reduction of accidents or failures must be considered. This in turn requires a deeper consideration of the failure mechanisms that can negatively affect the functional safety of these intelligent and complex systems [3, 4].

Safety and reliability of electrical, electronic and programmable electronic (E/E/PE) systems are the prerequisites for modern and highly integrated industrial automation systems in all application areas. By implementing a safety system for a safety-critical application, a high level of safety integrity is required and must be ensured in order to guarantee the safety-critical function of the Equipment Under Control (EUC). The safety system brings the EUC e.g. into a safe state if the safety objective is violated. The methods used to ensure functional safety are used in various sectors such as the process industry, aerospace industry, automotive industry, robotics and medical applications [5–7].

One of the approaches for safe operation in industrial robotic systems according to the ISO/TS 15066 standard is the limitation of force, speed and workspace [8]. With the approach of working within a limit, many applications today monitor a work area for the robotic arm by means of Radio-Frequency Identification (RFID) tags [9], proximity [10, 11], positioning [12, 13] and vision based system [14]. In the positioning approach, the robot system may only be active within its predefined workspace. Outside this area it is inactive. The coordinates of the robotic arm position are detected by the position sensor. In case it exceeds its predefined coordinates, the robot arm must be stopped in order to protect the human workers there. However, any failure of the system, which includes positioning sensors or controller, could lead to a hazardous situation. Electronic components generally have limited stress values and a limited operating lifetime. This means that each electronic element within a functional chain can fail with a certain probability and can then lead to a total failure of the system, which in turn can lead to dangerous situations. Therefore, safety architectures based on redundancy concepts such as 1oo2, 2oo3 are essential for the safe and reliable operation [15–17] of industrial robotic systems.

This paper presents an approach to safe position detection based on 1oo2 for the control unit and 2oo3 for the sensing unit. In this approach the track of the robotic arm within the predefined workspace is recorded by the position detection sensor. The sensor unit is evaluated by a SSoC (Safety System on Chip) which initiates a safe switch-off in case of violation of the defined working area.

In the context of safe positioning of the robotic arm, Section II provides a brief overview on the mathematical fundamentals on safe position detection. Section III introduces the design and architecture of the system that ensures a safe detection and positioning. Section IV describes the safety calculation of the presented safety system. Section V describes the experimental results.

II. CONSIDERATION OF POSITION MONITORING

To illustrate the safe position detection, point P is assumed as the current known position of the robot arm in three dimensions. (as shown in Fig. 1).

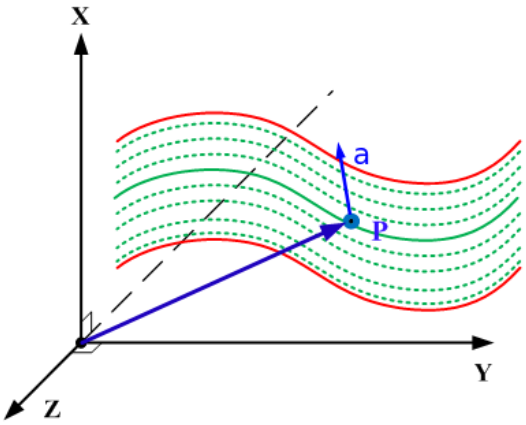


Fig. 1: Position detection principle.

If the robot arm moves, the position of the robot arm can be determined by the double integration of the measured acceleration vector ($\vec{a}$) as:

$$\vec{P} = \begin{pmatrix} p_x(t) \\ p_y(t) \\ p_z(t) \end{pmatrix} = \begin{pmatrix} \int v_x(t) \cdot dt \\ \int v_y(t) \cdot dt \\ \int v_z(t) \cdot dt \end{pmatrix} = \begin{pmatrix} \iint a_x(t) \cdot dt \\ \iint a_y(t) \cdot dt \\ \iint a_z(t) \cdot dt \end{pmatrix} \quad (1)$$

If this detection method is applied to all three spatial directions, a continuous precise determination of the position of the robotic arm can be achieved. If this is additionally realized with a safety-oriented architecture (e.g. 1oo2, 2oo3) of several sensors, the position can be reliably detected and then properly processed by the safety system.

III. APPROACH TO THE DESIGN OF A SAFE POSITIONING DETECTION SYSTEM

A. Safety Requirement of Industrial Robotic Systems

Defining the safety requirement for the industrial robotic system is an essential step in the early phase of the system development. This includes the specification details on the safety functions, the boundary limits and the interfaces of the safety related system (SRS).

The proposed approach offers the functionality to limit the activity of the robot in a certain area based on defining the allowed operation range. If the robot would cross the boundary of the working area or would be active in the forbidden area, a dangerous situation would arise that could lead to serious consequences. Therefore, it must be ensured that the activity of the robotic arm is limited only within the allowed safe working area. Based on the sensor data, the safety system must initiate either a shutdown or, if allowed, a safe and reduced speed of the robotic movement.

B. Challenges and Solutions

Safe and reliable communication is essential in a compact, highly automated and smart manufacturing environment. The requirements and necessities to use robots near to each other or to humans, e.g. in a production or assembly line, are becoming more and more frequent due to their effectiveness and economy. Each robot has its own defined workspace in which it is allowed to move. This interoperability can only be achieved if each robot performs activities exclusively in its defined workspace and cannot reliably leave it.

Unexpected, systematic or accidental failures in such a complex system could lead to serious consequences. In order to avoid accidents involving people, damage to property or environmental influences, it is therefore necessary to take measures and use procedures in the development and operation of these complex machines in order to predictively avoid design weaknesses and to control errors that occur during the operation. Conventionally, the movement of the robots in the workspace is controlled by a PLC. Correct operation is based on reliable input data (sensor data) from the controller and it must be ensured that these sensor data cannot lead to malfunctioning. Today, in many application areas, multi-channel systems are used for the automation of these complex systems. A weak point, however, is always the position detection sensors, which can be the cause of dangerous failures.

The solution presented here describes the implementation of a safety mechanism for safe and reliable position monitoring of a robotic arm compared to conventional systems. The demonstrated method is based on an integrated, safe architecture (SSoC) and a 2oo3 sensor architecture, which monitors and limits the active working of the robots within their programmed workspace to enable the interoperability of collaborative robots in smart manufacturing without risk.

C. Defining the Workspace

The maximum workspace that could be covered by the robotic arm is, in principle, a hemisphere around its base. The volume of the hemisphere (and therefore the limitation of the robot's working space) can be represented in general terms using the following equation:

$$V = \int_0^{\pi} \int_0^{2\pi} \int_0^{R} r^2 sin\theta \cdot dr \, d\theta \, d\varphi \quad (2)$$

The position sensor unit is attached to the robotic arm. When the robot arm moves in its workspace, the sensor unit also moves with it within this hemisphere, as Fig. 2.

Within this hemisphere, any desired working area can be defined for the production infrastructure and the robotic arm can be restricted to work in it. The position sensors provide the acceleration vector($\vec{a}$), which can be used to determine the current position as described in section II.

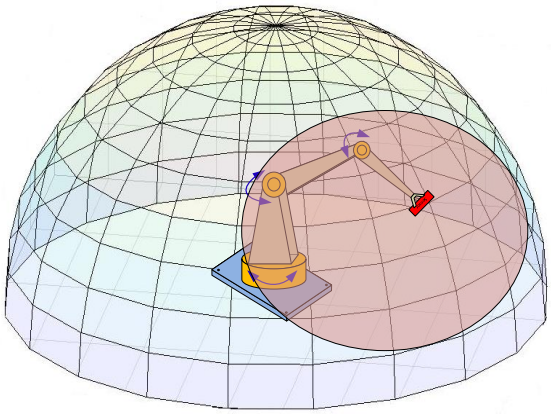


Fig. 2: Illustration of the hemisphere and the permissible working range of the robot arm

D. Architectural Approach of Safe Positioning System

The structure of the safe position detection system essentially consists of two subsystems, as shown in Fig. 3. Subsystem 1 is the safe redundant position sensing system and subsystem 2 is the safe processing unit on a SSoC. These two subsystems are explained in the following section.

1. Model of a Safe Sensing Subsystem

Accelerometers are used to measure the motion and oscillation of a moving element that is exposed to dynamic loads. In the presented model, a digital triaxial accelerometer with 14 bit resolution is used. The working range of each individual accelerometer can be configured [18]. The output signal of the individual accelerometers assigned to the spatial directions is continuously processed by the SSoC.

In the application of this model, a 2oo3 architecture is implemented for a safe and redundant position sensing. The configuration of each spatial direction sensor is chosen where each sensor provides a resolution of 0.25 mg. The sensor subsystem continuously records the coordinates of the robotic arm and sends them to the SSoC for processing.

2. Safety System on Chip (SSoC)

This SSoC subsystem offers on-chip redundancy and consists of a processing unit and a communication unit which are free from interference. The SSoC is designed according to the safety standard IEC 61508 for safety-critical applications to achieve a Safety Integrity Level (SIL) of SIL3. The SSoC is based on a 1oo2D safety architecture. The reliability of the system is achieved by implementing several functional safety features (e.g. independent diagnostic units, etc.) on a single chip and can therefore sufficiently guarantee SIL 3 capability. The two processing units in the control unit have a symmetrical design and rely on the same safety specification, such as their own dedicated memory and communication interfaces. They operate in so-called lockstep mode and perform the same activities per unit time. A diagnostic unit compares all activities and checks for deviations (both temporal and functional). In case of a deviation, the system sets to a predefined safe state.

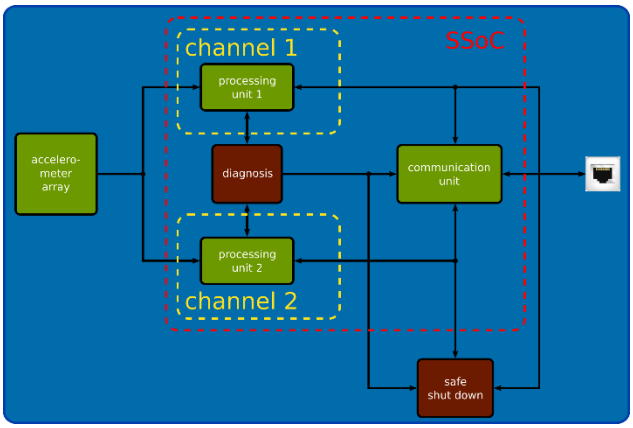


Fig. 3: Safe position detection system.

A third unit is used as a communication unit and it is free from interference to the other units. The 1oo2 safety architecture is connected to this communication unit and thus has an interference free communication channel. Communication with peripheral units (such as the overall control of the robot) can be carried out in two different ways. On one hand, a fast protocol-oriented communication system can be used to exchange the safe sensor data and, on the other hand, the safety-oriented control of the safe shutdown of the motion driver is possible in order to achieve a predefined safe state.

3. Safe actuator

Typically, the system is set to a safe state by redundantly designed shut-down drivers. In the model presented here, in the case of a deviation in the 1oo2 channels, the diagnostic unit will detect a violation of the functionally safe state of the overall system and set the system to the safe state. Furthermore, an additional testable, multi-stage, external watchdog sets a corresponding signal in the event of a failure of the 1oo2 system and thus establishes the safe state of the system. With both signals it is independently possible to set the safety critical system into a predefined safe state.

4. Interfacing the subsystems

As already mentioned, the 2oo3 accelerometer array is connected to the SSoC as shown in Fig. 3. All three spatial direction sensors are connected to both Processing Unit 1 and Processing Unit 2 and transmit synchronously and redundantly position data to both channels in order to calculate the position of the robotic arm in its predefined working space. Each processing unit continuously checks the redundant data of the three acceleration sensors. The calculated position data is then forwarded to the communication unit. This unit connects the safe position detection system with the outside world (the robot's PLC) to safely monitor the robotic system with regard to its workspace. As soon as a violation of the functional safety requirements of the system occurs, this is detected by the diagnostic unit. Appropriate measures establish the safe state and report to the higher-level via the communication unit.

IV. Calculations of the Architectural Model

A high level of safety is necessary for the industrial robotic system. The required safety level sets the conditions for the working environment and decides what safety measures must be implemented. In order to determine the

safety level, different measures and methods must be applied which will not be discussed here in detail. The determination of the safety level (SIL) has certain consequences on the design of the safety system. Apart from the architectural measures, the consideration of the reliability of individual components and other requirements of the appropriate safety standards, the safety integrity level of the total system can be evaluated. In this section the calculation of the model of the safe position detection system is shown as a rough example.

First, an analysis of the individual function blocks (subsystems) of the safe position detection system is carried out. The corresponding unique Safety Integrity Level (SIL) is assigned to the function achieved from each of these independent blocks. The individual functional blocks that form the safe position detection system are illustrated in Fig. 4.

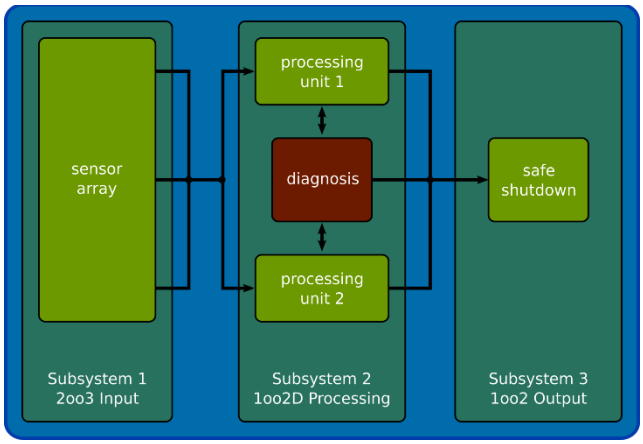


Fig. 4: Functional block diagram of the safety position detection system.

In order to determine the intended SIL-level of the proposed safe position detection system, it is necessary as a first step to define the application case of the safety function. The safety related function of the presented model is the function to prevent the robotic arm from violating the limits of its predefined workspace. Since this system is intended to be implemented in an industrial production environment, it has a continuous operating mode. Therefore, the Probability of Failure per Hour (PFH) has to be considered.

Fig. 4 shows the block diagram of the safe position detection system. The standard determination of the PFH of the system is determined according to equation 3.

$$\mathrm{PFH}_{\mathrm{system}} = \mathrm{PFH}_{\mathrm{sensors}} + \mathrm{PFH}_{\mathrm{SSoC}} + \mathrm{PFH}_{\mathrm{Actuator}} \quad (3)$$

The presented system comprises the 2oo3 sensor system, the 1oo2D SSoC and the 1oo2 actuator. The PFH value of the subsystems can be determined by the following equations [19].

$$PFH_{G,2oo3} = 6\big((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\big)(1-\beta)\cdot \lambda_{DU}\cdot t_{CE} + \beta\cdot\lambda_{DU} \quad (4)$$

$$PFH_{G,1oo2D} = 2(1-\beta)\lambda_{DU}\big((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD}\big)\cdot t'_{CE} + 2(1-K)\cdot \lambda_{DD} + \beta\cdot\lambda_{DU} \quad (5)$$

$$PFH_{G,1oo2} = 2\left[(1-\beta_D)\cdot\lambda_{DD} + (1-\beta)\cdot\lambda_{DU}\right]\cdot (1-\beta)\ \lambda_{DU}\cdot t_{CE} + \beta\cdot\lambda_{DU} \quad (6)$$

Where,

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}\,MTTR \quad (7)$$

$$t'_{CE} = \frac{\lambda_{DU}\left(\frac{T_1}{2}+MRT\right) + (\lambda_{DD}+\lambda_{SD})\,MTTR}{\lambda_{DU}+\lambda_{DD}+\lambda_{SD}} \quad (8)$$

Based on equations 3 - 8, the PFH value of the complete system can be calculated for the position detection system.

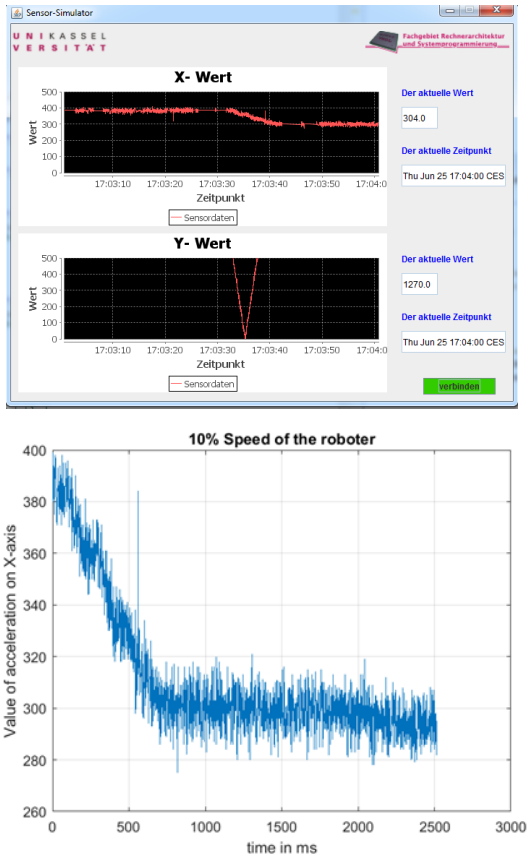


Fig. 5: Displacement of the robotic arm measured and calculated by the SSoC at a 10% standard speed of the robot

V. Experimental Results and Discussions

A. Workspace Measurement

Due to the physical conditions (mass, inertia, braking effect, etc.) the movement of a robot arm cannot be stopped immediately at the limit of its predefined hemisphere. The speed and reaction time result in a braking distance that the robot moves after the stop command has been sent. The maximum possible braking distance must be included in the definition of the permissible work area, or the calculation

algorithms must include it in the calculation of the permissible position.

In this section the measurements of the safe position detection system are presented. The working range of the robotic arm is defined by the values specified in the GUI and the robotic arm is operated at various different speeds. An algorithm is designed that evaluates the raw data from the accelerometers and determines the angular position. The position measurements for different speeds were calculated and plotted with a simulation tool. The results and the screenshots from the developed GUI are shown in Fig. 5 to Fig. 7.

.

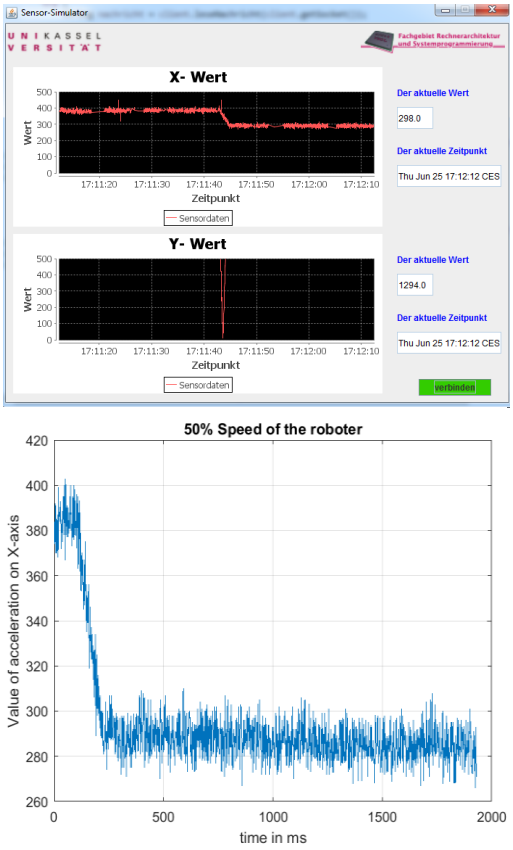


Fig. 6: Displacement of the robotic arm measured and calculated by the SSoC at a 50% standard speed of the robot.

B. *System Setup And Demonstration*

To demonstrate the concept described in this work, the realized safety-based hardware is installed on the robotic arm and validated for its (safe) functionality. In the initial state the sensor system is positioned on a fixed and known reference point. The desired working area of the robotic arm to be protected can be set via the graphical user interface and the laser installed on the hardware is used to show the output function of the safety system. The basic safety function of this configuration is defined by the fact that the laser beam may only be switched on within the work area defined in the GUI and must be switched off if the work area is violated. The position detection system must continuously and safely detect the position of the robot arm in the entire possible working area and this data must be safely calculated in the SSoC as position data. Finally, based on these calculations, the activity of the robotic arm must be controlled and limited to its defined workspace. The described principle is illustrated in Fig. 8.

Fig. 8 shows that when the desired inclination of the robotic arm is defined in the GUI, it actively performs its activities within this inclination. In this demonstration, the predefined workspace is set via the GUI. In (a) the robot arm moves from the defined start position in the direction of the negative Z-axis and the position detection sensors continously senses its coordinates. While the robot arm is within the predefined workspace, the laser beam is switched on. In (b), as the robotic arm reaches the predefined boundary of its active workspace, this is detected by the safe position detection system and the laser beam is switched off.

The demonstration shows that the position of the robotic arm can be safely and accurately determined with the help of the safe position detection system. With this principle a workspace can be defined within which predefined functions may be executed and outside of which these functions are deactivated. This can be functions attached to the robotic arm - in this case the laser - or the robotic arm itself. In the case of an error in the system that could cause the robotic arm to leave the allowed workspace, the safe position detection system shuts down the drive system and brings it into a safe state, or reduces speed to ensure the safety of the working environment in which the robot is working collaboratively.

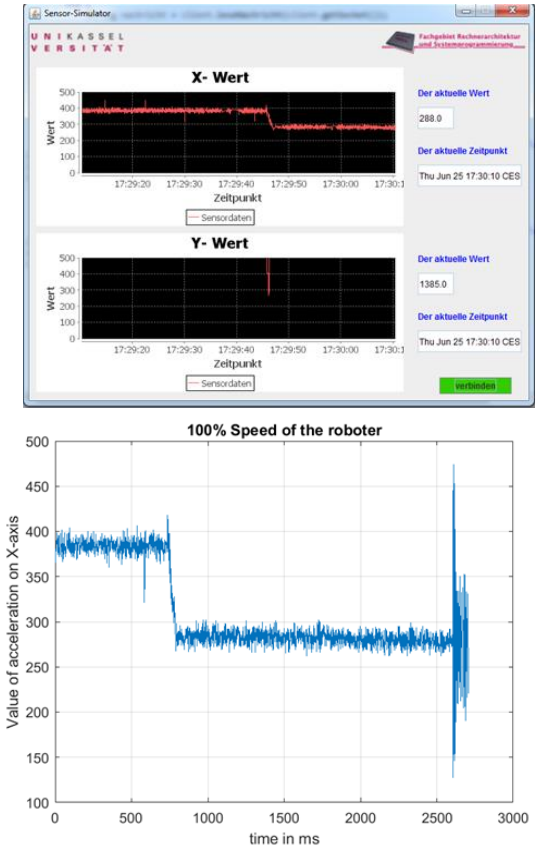
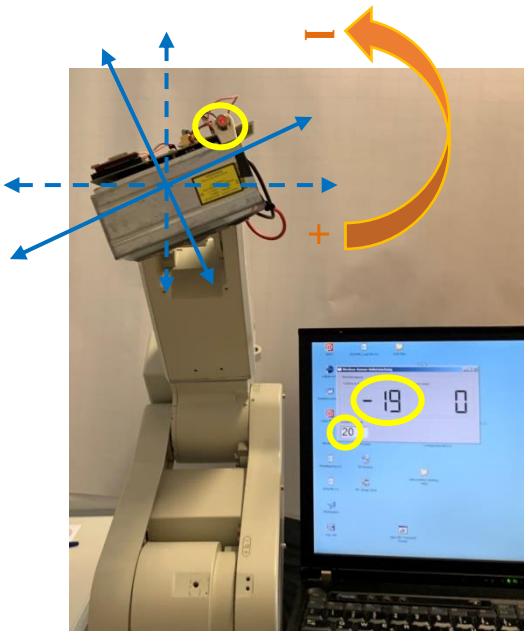
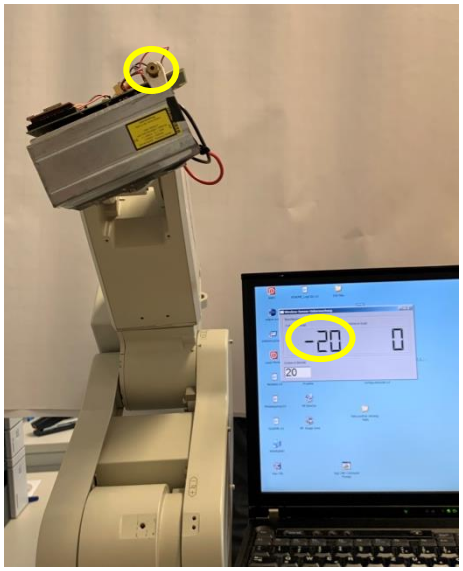


Fig. 7: Displacement of the robotic arm measured and calculated by the SSoC at a 100% standard speed of the robot.



(a)



(b)

Fig. 8: Setup and demonstration of safety positioning system.

CONCLUSION

In this paper a safe position detection system is presented for industrial robotic applications. The system is based on an integrated 1oo2 safety architecture and a 2oo3 architecture for the discrete accelerometer sensors. The safe position detection system ensures that e.g. the operating range of the robotic arm is limited to the permissible, predefined workspace. Due to its design and architecture, the system can achieve SIL 3 according to the generic safety standard IEC 61508.

In future, such an existing robotic system could easily be extended and enable to achieve a desired safety level. Economically such a procedure is interesting for the manufacturers and operators of highly automated industrial systems, if they adapt their production environment in view of future oriented - industry 4.0.

REFERENCES

[1] V. Jirkovský, M. Obitko, and V. Mařík, "Understanding Data Heterogeneity in the Context of Cyber-Physical Systems Integration," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 660–667, 2017, doi: 10.1109/TII.2016.2596101.

[2] B. Long, Z. Dai, S. Tian, and H. Wang, "A Hierarchical Modeling and Fault Diagnosis Technique for Complex Electronic Devices," in *2009 IEEE Circuits and Systems International Conference on Testing and Diagnosis*, 2009, pp. 1–4.

[3] E. Gracic, A. Hayek, and J. Borcsok, "Implementation of a fault-tolerant system using safety-related Xilinx tools conforming to the standard IEC 61508," in *2016 International Conference on System Reliability and Science (ICSRS 2016) proceedings: November 15-18, 2016, Paris, France*, Paris, 2016, pp. 78–83.

[4] J. Börcsök, *Electronic safety systems: Hardware concepts, models, and calculations*. Heidelberg: Hüthig, 2004.

[5] X. Jean, L. Mutuel, and V. Brindejonc, "Assurance methods for COTS multi-cores in avionics," in *2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC)*, 2016, pp. 1–7.

[6] R. M. Frazzini, "Historical Risk Mitigation in Commercial Aircraft Avionics as an Indicator for Intelligent Vehicle Systems," in *2007 IEEE International Symposium on Technology and Society*, 2007, pp. 1–8.

[7] P. Kazanzides, "Safety design for medical robots," in *2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 2009, pp. 7208–7211.

[8] *DIN ISO/TS 15066:2017-04, Roboter und Robotikgeräte_- Kollaborierende Roboter (ISO/TS_15066:2016)*, Berlin.

[9] C. Thormann and A. Winkler, "Localization of Workpieces by Robot Manipulators Using RFID Technology," in *2019 24th International Conference on Methods and Models in Automation and Robotics (MMAR)*, Międzyzdroje, Poland, 2019, pp. 52–57.

[10] M. Wali-ur-Rahman, S. I. Ahmed, R. Ibne Hossain, T. Ahmed, and J. Uddin, "Robotic Arm with Proximity and Color Detection," in *2018 IEEE International Conference on Power and Energy (PECon 2018): Berjaya Times Square Hotel, Kuala Lumpur*, Kuala Lumpur, Malaysia, 2018, pp. 322–326.

[11] D. Nakhaeinia, P. Laferriere, P. Payeur, and R. Laganiere, "Safe Close-Proximity and Physical Human-Robot Interaction Using Industrial Robots," in *2015 12th Conference on Computer and Robot Vision (CRV): 3-5 June 2015, Halifax, Nova Scotia, Canada*, Halifax, NS, Canada, 2015, pp. 237–244.

[12] A. McGregor, G. Dobie, N. R. Pearson, C. N. MacLeod, and A. Gachagan, "Determining Position and Orientation of a 3-Wheel Robot on a Pipe Using an

Accelerometer," *IEEE Sensors J.*, vol. 20, no. 9, pp. 5061–5071, 2020, doi: 10.1109/JSEN.2020.2964619.

[13] P. Neto, J. N. Pires, and A. P. Moreira, "Accelerometer-based control of an industrial robotic arm," in *RO-MAN 2009: The 18th IEEE International Symposium on Robot and Human Interactive Communication : [proceedings] : September 27 - October 2, 2009, Toyama International Conference Centre, Toyama, Japan*, Toyama, Japan, 2009, pp. 1192–1197.

[14] S. Kang and K. Kim, "Motion Recognition System for Worker Safety in Manufacturing Work Cell," in *2018 18th International Conference on Control, Automation and Systems (ICCAS)*, 2018, pp. 1774–1776.

[15] J. Borcsok, A. Hayek, and M. Umar, "Implementation of a 1oo2-RISC-architecture on FPGA for safety systems," in *2008 IEEE/ACS International Conference on Computer Systems and Applications*, 2008, pp. 1046–1051.

[16] F. E. Nadir, I. H. Baraka, M. Bsiss, and B. Amami, "Influence of failure modes and effects analysis on the average probability of failure on demand for a safety instremented system," in *2016 4th IEEE International Colloquium on Information Science and Technology (CiSt)*, 2016, pp. 867–871.

[17] J. Börcsök, *Functional Safety: Basic Principles of Safety-related Systems*, 1st ed. Heidelberg, Neckar: Hüthig Verlag, 2006. [Online]. Available: http://deposit.dnb.de/cgi-bin/dokserv?id=2797636&prov=M&dok_var=1&dok_ext=htm

[18] Bosch Sensortec, "Digital, triaxial acceleration sensor - BMA180 data sheet," 2010.

[19] *IEC 61508-6:2010 - Functional safety of electrical/electronic/programmable electronic safety related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*, IEC, 2010.