Hindawi
Complexity
Volume 2021, Article ID 6670625, 10 pages
https://doi.org/10.1155/2021/6670625

Research Article

Cyber-Security Assessment of Industry 4.0 Enabled Mechatronic System

Piotr Kotuszewski, Krzysztof Kukielka, Paweł Kluk, Andrzej Ordys, Karol Bieńkowski, Jan Maciej Kościelny, Michał Syfert, Paweł Wnuk, Jakub Możaryn, and Bartłomiej Fajdek

Faculty of Mechatronics, Warsaw University of Technology, ul. Sw Andrzeja Boboli 8, Warszawa 02-225, Poland

Correspondence should be addressed to Andrzej Ordys; andrzej.ordys@pw.edu.pl

Received 11 December 2020; Revised 30 August 2021; Accepted 1 October 2021; Published 22 October 2021

Academic Editor: Aydin Azizi

This paper reports on development of a laboratory set-up, for testing the concept and the components of Industry 4.0 enabled mechatronic system. A simple mock manufacturing lane is connected to a collaborating robot. There are three different programmable logic controllers (PLC) and various other elements which need to talk to each other using a variety of communication protocols. The controllers, and consequently the schedule of operations, can be programmed remotely. Moreover, the information is exchanged through the cloud service which could also assume the role of a soft-PLC. From the perspective of cyber-security, this set-up enables defining benchmarks and performing tests for resilience of the control structure. Some test scenarios are discussed in the paper.

1. Introduction

1.1. Industry 4.0. In the modern, fast-growing world, enterprises face many challenges such as dealing with large amounts of data, speed of making the right decisions, or flexibility of production processes [1]. The main reason for this is the highly competitive production environment. Very important is the concept of production flexibility, which means abandoning mass production and, instead, targeting individual products to customer's request [2]. Such a change results in a shorter product life cycle and increases the overall product range. However, it is required to change technological devices and machines to more flexible ones, adapted to different operating modes. Robotic and more broadly mechatronic devices play a pivotal role in this process. In addition, innovative tools and platforms should be provided for mutual cooperation of all areas of business operations [1]. To understand the needs of and subsequent creation of new and modification of existing manufacturing processes, a new concept of industry, i.e., Industry 4.0, describing the changes in the manufacturing, leading to so-called 4th industrial revolution, has emerged [3, 4].

As a result of this latest industrial revolution, factories are to be created where intelligent networks connect processes, machines, products, suppliers, and customers [2]. The production lines of the future can be supervised and managed remotely, and the final product is adapted to the needs of a given client on an ongoing basis [5].

1.2. Cyber-Physical Systems. Cyber-physical systems have been identified as one of the key research areas by the European Union Research programmes as well as by National Science Foundation, USA. This is a vibrant and relevant field of research which is likely to dominate in control systems design for the years to come, as it stems from rapid progress in communication, computing, and networking. Technologies underpinning the cyber-physical systems include sensors and wireless sensor networks, communication protocols, distributed control systems, and cloud computing.

Such systems are one of the pillars of Industry 4.0 manufacturing processes. Current trends in manufacturing systems include Internet of Things (IoT), cloud computing, mobile devices, and big data [2].

There are many examples of application areas, for instance, automotive systems-optimization of power train of hybrid vehicles [6], collaborating robotic systems for smart production [7], robotic systems for medical applications [8], distributed power generation (e.g., wind turbines) [9], and smart homes [10], to mention just a few.

1.3. Industrial Internet of Things (IIoT). One of the paradigms of Industry 4.0 is the development and implementation of Industrial Internet of Things. This modification of the Internet of Things technology is intended for industrial applications.

The basic idea of the Internet of Things is to collect data. In the case of the Industrial Internet of Things, this is the collection of large amounts of process data and their transmission to data centers [1].

Data from various sources are collected and analyzed in the cloud. Data sources include devices such as sensors, actuators, PLCs, industrial robots, production equipment (e.g., CNC milling machines), and mobile robots [11].

The Industrial Internet of Things is just taking the shape of useful technology in industry. To analyze the data, the IIoT device connects to the cloud [11]. This is a big challenge, because it is necessary to integrate the new technology into the existing infrastructure and, additionally, ensure data security.

A similar trend, although not always using the name of cyber-physical systems, has been observed in industrial control systems. This trend is to control installations remotely, using sensors and actuators connected with the controller via a wireless network. The rationale is to reduce the costs of workforce and, also, to remove the necessity of humans to be present in locations where the control action takes place (e.g., manufacturing lines in the space). Furthermore, more emphasis is currently placed on the control algorithm itself being located on the computing cloud (Control as a Service (CaaS)). Such solution, whilst providing undoubtful benefits in terms of cost, flexibility, ease of modifications, and maintenance, also poses certain problems which need to be addressed, for instance, resilience of control actions and security of information flow and information processing.

1.4. Cloud Computing. According to the NIST publication [12], cloud computing is defined as "a model that allows network access to computing resources (e.g., networks, servers, memory, applications, and services) that can be quickly delivered and based on the use of services provided by the service provider." The principle of operation is to transfer the burden of IT services from the local computer to the server with the possibility of permanent access through client computers [4]. This results in greater reliability, because regardless of what happens to the client computer, all services will continue to work.

Cloud-based control of systems and Control as a Service (CaaS) have become a focus of interest relatively recently. In [13], expectations and challenges related to such systems are outlined. In [14, 15], the term Control as a Service in relation to a programmable logic controller (PLC) used for industrial automation tasks (soft-PLC) is explored. The focus is on communication requirements and on the scalability of the controller.

1.5. Cyber-Security. In parallel, there is a growing interest in research on cyber-security of such configurations.

Standard, IT based methods of providing cyber-security are being proposed. Those include separation of business and production networks by strong passwords and firewalls.

In [16, 17], forms of encryption of information sent to and from the controller are proposed to eliminate possible cyber-attacks. Then, the design of the encryption mechanism in such a way that it would not be necessary to deencrypt the information in order to perform standard operations of the controller (addition and multiplication) is discussed.

In [18], a cyber-physical test-bed which can be used to test the Modbus TCP protocol in response to cyber-attacks is described. The test-bed uses a real-time power grid simulator. Some possible scenarios of cyber-attacks are discussed.

1.6. Contribution of This Paper. Our interest is in investigating whether the information about the process variables and the control actions could be additionally used to more precisely detect possible cyber-attacks. There exist well developed techniques of "fault detection and isolation," which are widely applied to continuous processes, especially in process industry (petrochemical, energy generation). Fault-related residuals are being detected on the basis of the analysis of process data. We propose to use similar approach to analyze robotic/manufacturing systems. Another group of methods which we intend to use is related to "control performance assessment and benchmarking" [19, 20]. In this approach, the changes in controller performance are detected as signalizing possible faults or cyber-attacks on the system. We propose to extend those techniques to cover mechatronic systems, characterized by a combination of discrete-event and continuous-event control.

Hence, the main focus and the main novelty proposed in this paper are in applying the above methods to robotic/mechatronic systems in order to test their ability to detect cyber-attacks in such systems.

For that purpose a laboratory stand is being prepared at Warsaw University of Technology which would emulate all major components of Industry 4.0 manufacturing mechatronic systems. In the subsequent sections, the concept and the build of this mechatronic stand are presented. Next, its cyber-physical functionalities are discussed, including communication links and discussion of nodes where cyber-attacks could penetrate. Further, possible configuration of the system to test effects of different cyber-attacks is discussed. Finally, some initial results are presented.

2. Description of the Experimental Set-Up

In the Institute of Automatic Control and Robotics of the Warsaw University of Technology, a laboratory stand was created, presenting issues related to Industry 4.0. The

conceptual diagram of the stand is presented in Figure 1, whereas Figure 2 shows a photo view of the actual equipment.

In general terms, the stand is provided with two operator panels used to define what is to be produced at the station and to monitor the work of the station. All control elements of the station are connected with each other and the whole system is connected to the Internet, which allows remote access to the station.

The stand explores the possibility of production-on-demand, personalized production.

With reference to Figure 3, product personalization means here the choice of which discs will be connected to each other; the lower disc with the RFID tag is deposited with the upper disc, whose upper surface is of a certain color. With the help of the operator panel, or remotely, the production scheme is defined, i.e., the operator selects which color of the upper disc is to be placed on the next product. The discs with RFID tags are issued by the station 1. The issued discs are placed in the indexing table seats. The vision system verifies the color on the disc in the inner socket (upper disc) and saves this information to the database. After the release of all the disks and their identification, the discs of the desired color are placed on the appropriate discs on the table. Next, the robot transfers the produced item (two discs) to the packing and further to the customer, according to the desired color specification. At the same time, the next pair of discs is assembled, possibly with different color.

The stand can be divided into two parts: part one is the FANUC cooperating robot and part two is the indexing table and manipulators for manipulating simple details (Figure 3). The PLCs responsible for controlling the laboratory and for the exchange of data between controllers, the robot, and the cloud-based platform are mounted on the industrial racks.

In addition to being a good representation of the production-on-demand, the stand also enables various tests and benchmarks related to the communication between the substations and cyber-security of the installation. This is facilitated by

(i) Using three different industrial controllers, which need to communicate among themselves as well as communicate with their assigned sensors and actuators

(ii) Using different ways of communication, which could be via direct digital link, or via Ethernet, or via wireless link through the cloud

(iii) Ability to remotely define the production plan and, moreover, to connect to the cloud for reprogramming of the controllers

There are three PLC controllers from different manufacturers: Allen-Bradley Compact GuardLogix 5380, Beckhoff CX5140, and Wago 750-880. The devices connected to them are a valve island from Festo, two control panels for Beckhoff and Allen-Bradley PLC controllers, and two servo drives (from Beckhoff and Allen-Bradley).

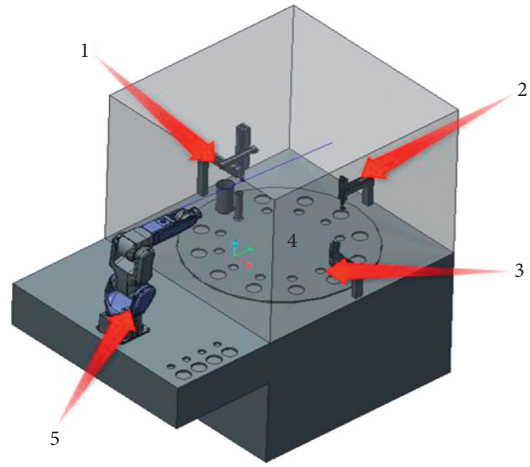

Figure 1: The concept of the set-up presenting the issues of Industry 4.0; pneumatic servo-manipulator, 1; pneumatic manipulators with vision system, 2; pneumatic manipulators, 3; the indexing table with slots for discs and RFID system, 4; the collaborating robot, 5.

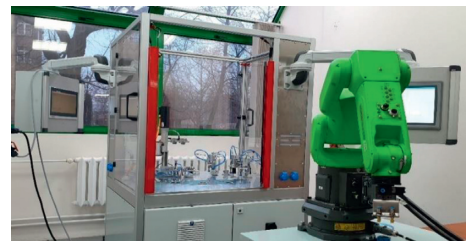

Figure 2: General view of the entire station.

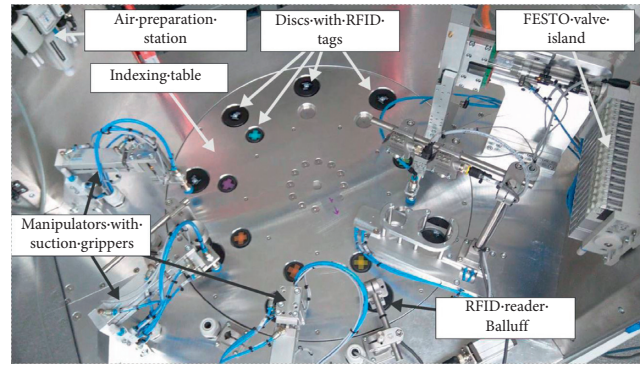

Figure 3: The indexing table with colored disks.

Controller Beckhoff is connected with both Allen-Bradley and Wago, whereas the latter two are not connected. In this way, Beckhoff becomes the main PLC, because it is able to synchronize all of them.

The above experimental stand enables tests of various algorithms related to the cyber-security. An example of a simple algorithm implemented on the stand will be presented below. The example will concern mainly one of the elements available at the stand, the pneumatic manipulator. The details of operation of such a manipulator are shown in Figure 4.

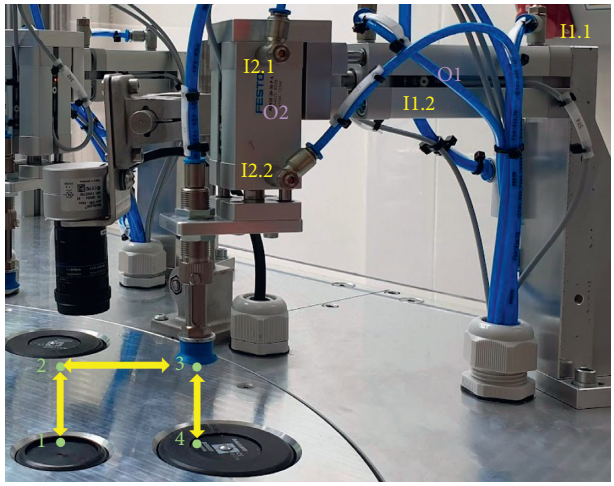

Figure 4: Pneumatic manipulator used on the stand.

The manipulator consists of a base, two pneumatic cylinders, and a pneumatic gripper mounted on the second cylinder. The actuators allow the gripper to move in two axes. In this situation, it is possible to operate the disks that are placed in the sockets of the indexing table. The position of the manipulator's actuators is controlled by pneumatic solenoid valves. Their state is changed via the digital output signals O1 and O2. Information about the current position of the manipulator is obtained from the limit sensors located in the end positions of each of the actuators (signals I1.1, I1.2, I2.1, and I2.2). The correct movement related to shifting the small colored disc on the large disc takes place between the marked points 1-2-3-4 and the return movement between points 4-3-2-1.

3. Description of Communication Links

3.1. Communication between the PLCs. Communication between PLCs should allow not only to easily exchange data (presumably also between networks) but also enable the synchronization of tasks and command drivers. For example, if one of the devices connected to the Wago driver successfully completes its task, it should be able to provide the Allen-Bradley driver with information about it, which at the same time will give the driver a signal that it should perform the next program point.

The Beckhoff TwinCAT 3 software is very comprehensive, which gives configuration options and many communication protocols and interfaces to choose from. In the version shown above, the Beckhoff CX5140 and Allen-Bradley Compact GuardLogix 5380 are connected via Ethernet/IP, while the Beckhoff CX5140 and Wago 750-880 are connected via Modbus/TCP.

Choosing two different network protocols will give the ability to test communication between protocols as well as the resistance of individual protocols to external interference and attacks.

Beckhoff controller is also connected to the cloud, which contains a database with detailed information about the operation of the system.

3.2. Application of Techniques of Industry 4.0. In developing this laboratory stand, it was important to use elements of Industry 4.0 such as communication via the Ethernet/IP standard, RFID tags, visualization using the HMI interface, remote, wireless stand management via VPN, and remote desktop. The devices have been connected and configured to exchange data with a local or a remote database.

(i) TCP/IP (Transmission Control Protocol/Internet Protocol) is a layered model of a set of protocols needed to send information. This model consists of four layers: application, transport, Internet, and network interface.

(ii) Ethernet/IP uses the Ethernet standard at the physical layer, encapsulating data according to UDP or TCP protocols at the transport layer and data link and implements Common Industrial Protocol (CIP) at the application layer in the network communication structure according to the simplified OSI model, TCP/IP [15].

(iii) Common Industrial Protocol (CIP) is a communication protocol designed for applications in industrial automation. It includes functions: control, security (CIP Safety), synchronization (CIP Sync), motion (CIP Motion), configuration, and information. CIP is independent of the method of data exchange, the network protocol, which allows easy data flow between different networks and thus also outside of Ethernet/IP.

(iv) Modbus/TCP: Modbus is used to transfer information between devices and allows remote programming of devices and supports distributed I/O. Modbus TCP is a Modbus standard adapted to the Ethernet standard [1]. Modbus TCP due to its openness and due to licensing is supported by many devices of different companies

(v) The RFID (Radio Frequency Identification) system consists of a read/write head and a data carrier (data carrier/RFID tag). The RFID system is used for remote recognition of objects, devices, and products. The RFID head consists of an antenna that sends and receives a signal. RFID tags are constructed from integrated circuit, antenna, and housing. Data carriers may be read-only (RO), write once read many (WORM), or rewrite (RW). Depending on the power supply methods, there are passive tags powered by the waves sent by the reader, active tags with battery power, and semi-passive tags with power only for the integrated circuit. In this laboratory stand, the tags are passive and have RW functions.

(vi) The IO-Link master (Master IO-Link-750-657 Wago) is a device used in IO-Link communication to exchange data between the controller and actuators or measuring devices called the IO-Link device. IO-Link is a common open communication standard (IEC 611131-9 standard).

Master IO-Link can connect to the controller using various protocols, e.g., Profibus, Profinet, Ethernet/IP, DeviceNet, EtherCAT, and CC-Link. The IO-Link masters from various companies can be used with all actuating/measuring devices that support this standard on the market. More specifically, IO-Link is described in [21].

3.3. Remote Management. Configuring the operation of the stand is partially performed remotely through the use of tunnel Virtual Private Network (VPN) L2TP/IPSEC. This enables remote connection and communication with those devices which are network connected. The controllers are programmed from the level of the desktop computer on which the PLC manufacturers' software has been installed. By using the Remote Desktop Protocol (RDP), it is possible to remotely operate that computer from the level of the graphical interface of Windows 10. With the help of a tunnel VPN, it is possible to connect to the computer and freely program the PLCs from any place where there is a fast enough access to the Internet and (thanks to the popularity of the protocol) from almost any device (laptops with Windows 10 and Linux and an Android smartphone were tested).

Regardless of the desktop, the Beckhoff CX5140 on which Windows 10 CE is installed also supports the RDP protocol and allows remote configuration.

Both the VPN and RDP connections are encrypted and password protected.

3.4. Data Flow in the System. Allen-Bradley and Wago controllers write data to the register of the Beckhoff controller. This register contains sensor states and program variable states, which are important for the functioning of the entire station. Data flow is illustrated in Figure 5.

In addition to the possibility of serving a larger number of workstations, the cloud also provides a certain degree of redundancy for stored data, providing security in their storage in case of failure.

The test stand has been connected to the Google Cloud database as part of a free limited test package. The MySQL instance has been launched; the other ready-made solutions also enable the launch of MS SQL and PostgreSQL instances. The configuration of the connection to the cloud database turned out to be the key element. When the system was built, it was decided to use a simple way to limit connections to a narrow pool of clients' IPs, thus creating basic authorization. Adding certificates (CA) to the configuration of encryption is not a major problem; however, it requires expansion of the system with additional Open Database Connectivity (ODBC) drivers locally and configuration of the encrypted connection. This configuration makes it significantly more difficult to start data acquisition using the TwinCAT system, because the system itself does not support Secure Sockets Layer (SSL).

Another potential solution that provides encryption and increased security is to use Secure Socket Shell (SSH) tunneling with machines in Google Cloud. That method uses private IPs, thereby increasing security compared to methods using public database instance IPs. The choice of a method and configuration of the connection is critical for securing data flow. The latter described method shows the highest security potential by implementing the following elements:

(i) Allowing disabling access to the database via public IP

(ii) Allowing running an encrypted SSL connection using certificates of authenticity (CA)

(iii) Virtual Private Cloud (VPC) is used for connecting local parts to the cloud system

(iv) Cloud database IP is only available from the private network

Adding a database in the cloud complicates the system and requires an open connection to the external network. Its implementation requires a thorough design of the network architecture as well as the implementation of all possible cyber-security measures to protect against unauthorized interference from outside.

4. Possible Configurations of the Tests of Cyber-Security

The configuration of the laboratory, the components used, and the wide spectrum of communication channels available enable various tests related to resilience of control algorithms. The following could be possible reasons for this manufacturing line not to work properly:

(i) Malfunction of one of the controllers, for instance, the RFID tagged discs are not placed properly on the table, or the robot is not collecting the produced items on time

(ii) Falsification of readings of sensors, for instance, the color determined by the camera

(iii) Errors in communication between the PLCs, hence the information about the combination of the RFID code and the color of the second disc may not be properly transmitted; also, information about completing stage 1 may not reach the controller responsible for stage 2

(iv) Errors and falsification of information transmitted remotely (via remote terminal and/or from the cloud, for instance, the production demand for the next element, or the colors of the discs stored in the database

For each of the described anomalies, the reasons could be in the faults developed within the system itself or, indeed, could result from cyber-attacks.

The set-up enables testing different configurations, e.g.,

(i) Some parts are connected via Ethernet, some by direct cable digital link

(ii) Remote access form the Internet to certain parts of the system can be set up

(iii) Some of the communication channels are duplicated by other means of communication, or opposite

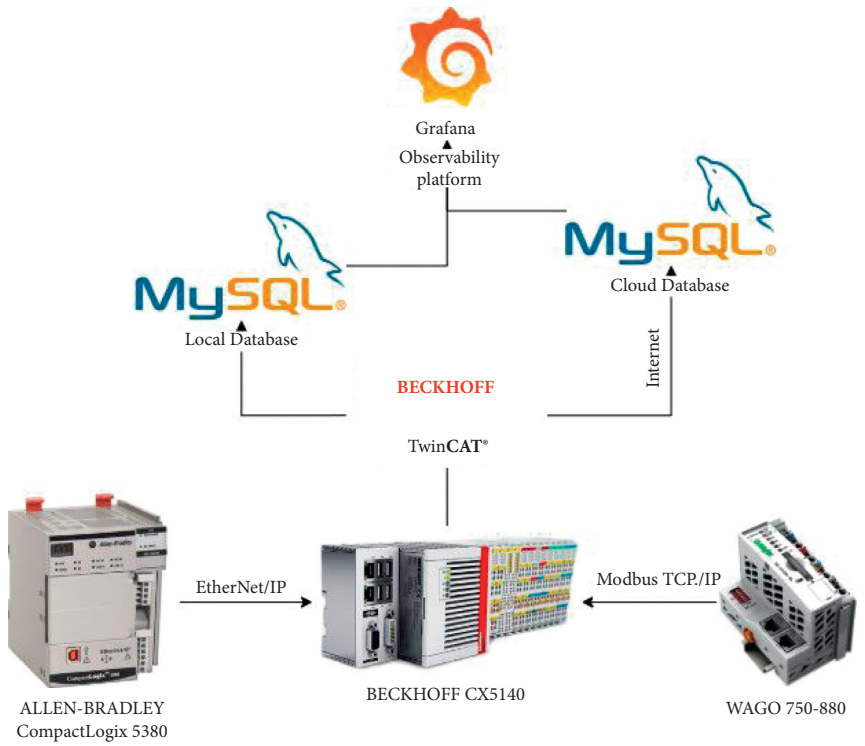

Figure 5: Data flow in the system.

(iv) Some of the devices are designed not to communicate with others

(v) The PLC controller(s), one or more, can be replaced by a soft-PLC located on the cloud

Resilience of the control structure, in different configurations, could be assessed.

5. Initial Results

The controller service program has been developed, which enables simulation of a flexible production process. With the help of switches, it is possible to simulate failure and/or execution of one product unit. Depending on the color of the ordered discs, other relevant signals are issued, which in turn simulate the launch of different machines in certain modes of operation.

Figure 6 presents the algorithm of operation for the station when production-on-demand is carried out. Firstly, for each RFID tag of the lower (bigger) discs, a corresponding desired color of the upper disc is determined from the operator panel or from the remote control panel and saved (locally or in the cloud) in the production schedule. The manipulators should properly place the colored discs so that, at the end, each of the RFID (lower) discs has on top of it a smaller (colored) disc with a color as selected by the user.

According to the program, if the controller is not working, it goes into standby mode. There should be no production downtime in the actual production process, so it can additionally be assumed that after all personalized orders are completed, the process goes to mass production of some standard catalog units.

The cloud communication support program can be divided into two parts. The first part is responsible for collecting data from the controller and sending them to the cloud. The second part is responsible for receiving data from the application in the cloud. Visualization of the entire data flow is shown in Figure 7 (prepared in Node-RED application).

In order to send data to the cloud, two blocks should be used: an input block to read data from the controller's memory and an output block to transfer this data to the cloud.

Initial tests/experiments have been performed on the stand. Due to the high complexity of the whole system, only a simple case of possible cyber-attack on the pneumatic actuator is discussed in this paper. The work of the actuator has been described earlier, in Section 2 of the paper.

The algorithm proposed below for the detection of potential attacks is based on the analysis of the current state of digital inputs (information from the limit switches). Table 1 shows the possible digital input states for the manipulator positions for the correct disk ratio. This set of acceptable signal values in each step will be used in the algorithm as a set of reference data.

The developed algorithm, based on residual's generation, consists in comparing the current state of digital inputs (the current position of the actuators) with the reference state, which is presented in Table 1. Additionally, the current state is used in the next step as the previous state and these two states are used for comparison. This allows not only to determine whether a given state is correct but also whether the sequence of steps is correct and whether the manipulator correctly shifts the disc. When a given

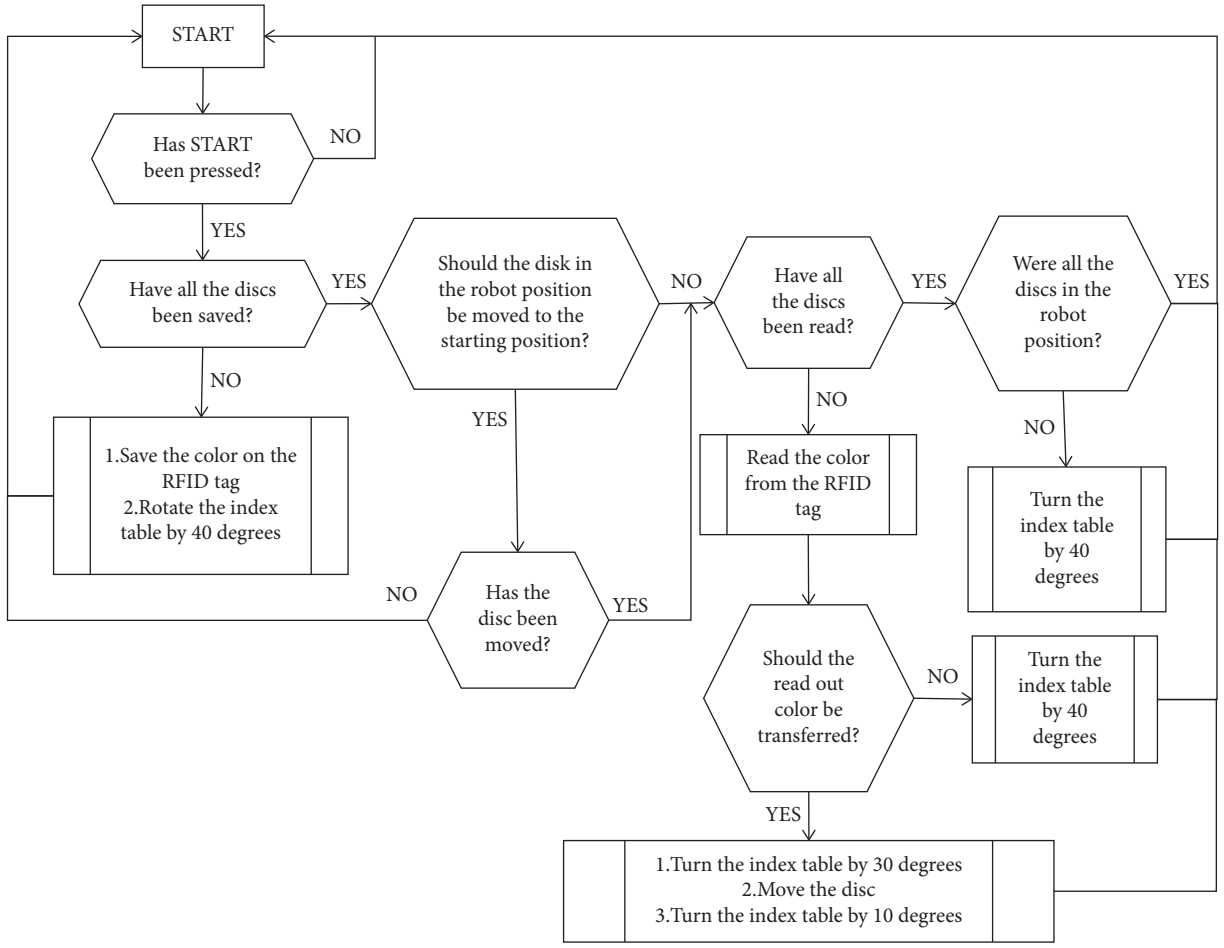

Figure 6: Algorithm of operation of the station.

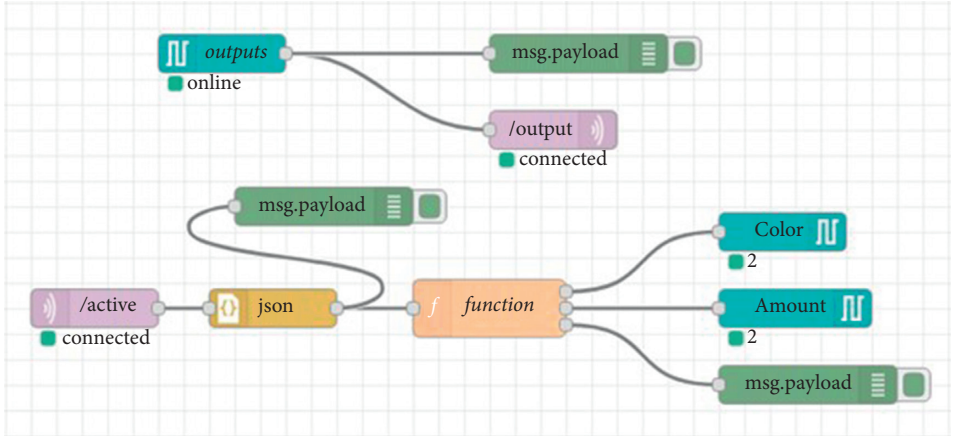

Figure 7: Block diagram of the cloud communication support program.

state is not identified among the correct states, or if the state is correct but is not executed in the correct order, then it may be suspected that there has been an external interference in the operation of the manipulator. Such interference can be, for example, a cyber-attack.

Figure 8 shows a block diagram of the algorithm implemented to detect potential cyber-attacks.

As a result of the algorithm's operation, four possible conditions of the manipulator's operation are identified:

(1) The state (as indicated by received signals) is correct, no undesirable change of signals occurred

(2) The state is correct and has not changed compared to the state from the previous step (such information

Table 1: Correct state of digital signals for particular positions of the manipulator.

Nr.	I1.1	I1.2	I2.1	I2.2
1	0	1	0	1
2	0	1	1	0
3	1	0	1	0
4	1	0	0	1
3	1	0	1	0
2	0	1	1	0
1	0	1	0	1

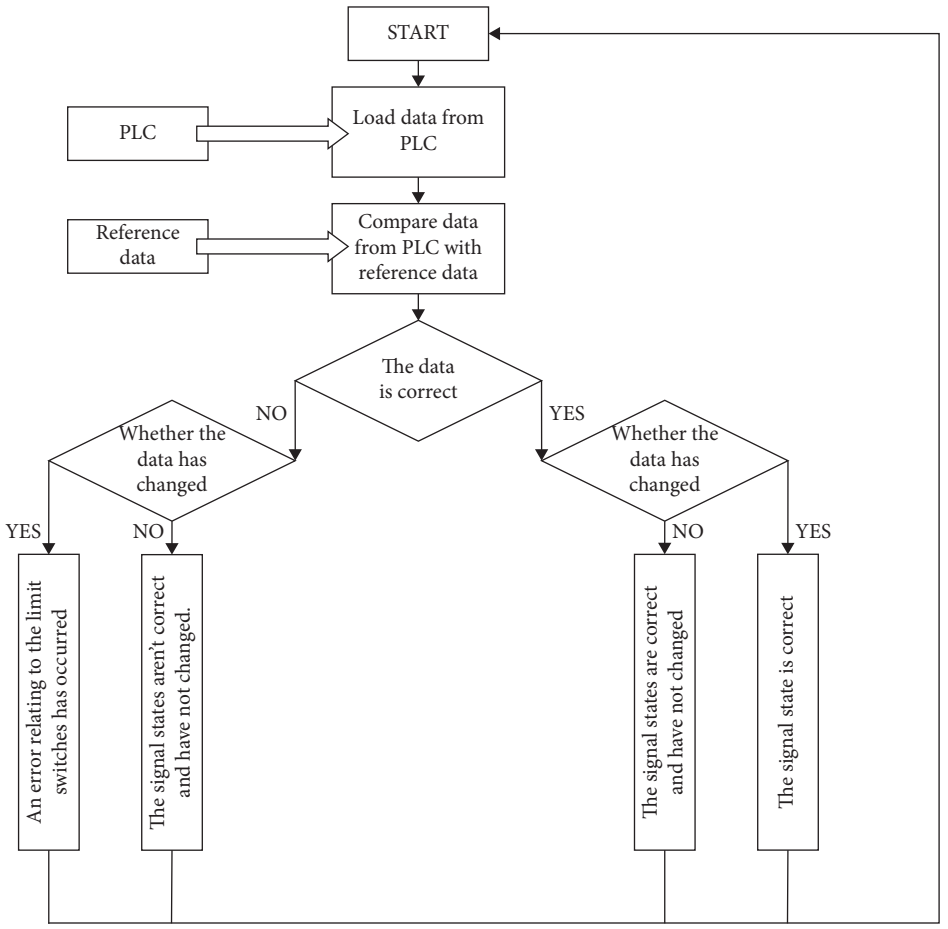

Figure 8: Scheme of the algorithm for detecting changes in the operation of the manipulator.

was introduced due to possible slower changes of signals than the operation of the algorithm itself)

(3) The state is incorrect, an undesirable change in the manipulator's operation

(4) The signal condition is not correct and has not changed from the previous step

The algorithm developed in this way was implemented and tested on the stand described above. An example of the algorithm's performance is shown in Figure 9.

The above example demonstrates that the algorithm based on calculation of residuals can be used for detection of possible malfunctions of a manufacturing system, caused for instance by cyber-attacks.

While testing the operation of the system, several problems have been identified and analyzed.

The first problem is that incorrect operation of one controller or incorrect setting of elements for which this controller is responsible may cause an error on another controller or prevent the stand from continuing to work at all. An example of such a situation is the absence of the RFID tag in the appropriate position, which would prevent further operation of the program because it would wait indefinitely for reading information from the tag. Pneumatic cylinders can be another example of this when they are not in the home position. Moving the actuators from their position prevents correct operation of the controller's logic, because signals which are sent from the limit switches attached to the

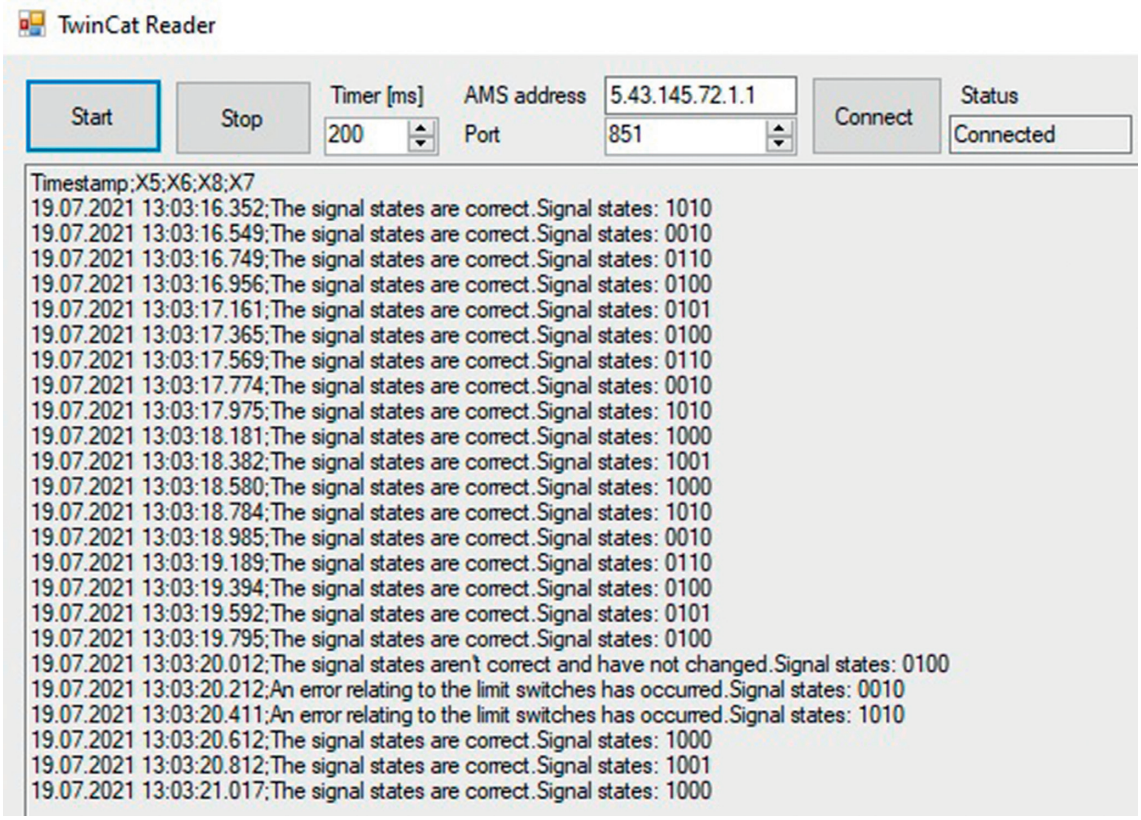

Figure 9: An example window showing the results of the algorithm.

actuators in this case do not allow proceeding to the next stage of the program.

Another problem that has been noticed when programming the drivers is that of not sending the values of variables that contain information about completing the task properly. This problem can occur if communication between the controllers is not working properly. In this situation, the movements of actuators can be made a number of times that is different than required by the program's logic. This problem is minimized due to the use of industrial communication protocols which use a three-way handshake to establish communication and use checksums guarantee packets which are sent in full.

The stability of the data acquisition system has been tested in the event of the database connection being interrupted. A problem has been encountered in the form of difficulties in resuming records after regaining connection stability.

There have also been tests of the speed of downloading data from various instances of the database (cloud and local) by running a refresh of information in the Grafana environment every one second. Simple queries gave satisfactory results, while more complex queries could result in queues of many queries.

The stand can be set-up and controlled remotely. Hence, we invite colleagues to collaborate on testing of cyber-attacks, algorithms for detection and elimination of such attacks, and/or algorithms for resilient control of the system under attacks.

6. Conclusions

This paper presents a new laboratory stand, devoted to design of Industry 4.0 enabled production systems and to testing their resilience to cyber-attacks. The main components of the laboratory have been presented with emphasis on possible connections and ways in which subsystems communicate. Configurations of the tests for cyber-security have been discussed.

Furthermore, some results of tests performed on the stand, utilizing the methodology of assessing the values of residua, have been presented. Based on the above, factors influencing the detection of possible cyber-attacks have been discussed.

As possible directions of future work, we would like to consider the following:

(i) Distinguishing between the cyber-attacks and the faults of equipment. Redundancy in the communication channels and a possibility to duplicate the control actions; by running them locally on the controllers as well as on the cloud would facilitate such a task. In the current configuration, the controller code is hosted directly on the controller. However, it could be duplicated on the cloud and the results of the two can be compared.

(ii) Design the control/sequencing algorithms in such a way that even in cases of some malfunctions/attacks the system can still operate or, at least, it can stop

operating smoothly and safely, without producing wrong products and causing any damage. Many methods and tools have been discussed in the literature in the context of fault tolerant control. They could be a useful starting point for such investigations.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

Andrzej Ordys acknowledges support from the National Agency of Academic Exchange (NAWA), "Polish Returns," Grant No. PPN/PPO/2018/1/00063/U/00001. Krzysztof Kukielka, Andrzej Ordys, Jan Maciej Kościelny, Michał Syfert, Paweł Wnuk, Jakub Możaryn, and Bartłomiej Fajdek acknowledge support from the POB Research Centre Cybersecurity and Data Science of Warsaw University of Technology within the Excellence Initiative Program-Research University (ID-UB).

References

[1] P. Wittbrodt and I. Łapuńka, *Przemysł 4.0-Wyzwanie Dla Współczesnych Przesiębiorstw Produkcyjnych, Innowacje W Zarządzaniu I Inżynierii Produkcji, Tom II*, Oficyna Wydawnicza PTZP, Opole, Poland, 2017.

[2] D. Gerwin, "Manufacturing flexibility: a strategic perspective," *Management Science*, vol. 39, no. 4, 1993.

[3] S. Wang, J. Wan, D. Li, and C. Zhang, "Implementing smart factory of industrie 4.0: an outlook," *International Journal of Distributed Sensor Networks*, vol. 2016, Article ID 3159805, 2016.

[4] J. Schlechtendahl, F. Kretschmer, A. Lechler, and A. Verl, "Communication mechanisms for cloud based machine controls," in *Proceedings of the 47th CIRP Conference on Manufacturing Systems*, Elsevier, Windsor, Canada, April 2014.

[5] M. Olszewski, "Mechatronizacja produktu i produkcji–przemysł 4.0," *Pomiary Automatyka Robotyka*, vol. 20, no. 3, pp. 13–28, 2016.

[6] X. Krasniqi and E. Hajrizi, "Use of IoT technology to drive the automotive industry from connected to full autonomous vehicles," *IFAC-PapersOnLine*, vol. 49, no. 29, pp. 269–274, 2016.

[7] M. A. R. Garcia, R. Rojas, L. Gualtieri, E. Rauch, and D. Matt, "A human-in-the-loop cyber-physical system for collaborative assembly in smart manufacturing," *Procedia CIRP*, vol. 81, pp. 600–605, 2019.

[8] A. R. Patel, R. S. Patel, N. M. Singh, and F. S. Kazi, "Vitality of robotics in healthcare industry: an internet of things (IoT) perspective," in *Internet of Things and Big Data Technologies for Next Generation Healthcare*, C. Bhatt, N. Dey, and A. Ashour, Eds., vol. 23, pp. 91–109, Studies in Big Data, Springer, Berlin, Germany, 2019.

[9] B. Satuyeva, C. Sauranbayev, I. A. Ukaegbu, and H. S. V. S. K. Nunna, "Energy 4.0: towards IoT applications in Kazakhstan," *Procedia Computer Science*, vol. 151, pp. 909–915, 2019.

[10] D. Mocrii, Y. Chen, and P. Musilek, "IoT-based smart homes: a review of SystemArchitecture, software, communications, privacy and security," *Internet of Things*, vol. 1-2, pp. 81–98, 2018.

[11] A. Verl, A. Lechler, S. Wesner et al., "Armin lechler, stefan wesner, andreas kirstädter, jan schlechtendahl, lutz schubert, sebastian meier, an approach for a cloud-based machine tool control," in *Proceedings of the Forty Sixth CIRP Conference on Manufacturing Systems 2013*, Elsevier, Setubal, Portugal, May 2013.

[12] P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, Recommendations of the National Institute of Standards and Technology, Gaithersburg, Maryland, 2011.

[13] L. Monostori, "Cyber-physical production systems: roots, expectations and R&Dchallenges," in *Proceedings of the 47th CIRP Conference on Manufacturing Systems*, Windsor, Canada, April 2014.

[14] T. Goldschmidt, M. K. Murugaiah, C. Sonntag, B. Schlich, S. Biallas, and P. Weber, "Cloud-based control: a multi-tenant, horizontally scalable soft-PLC," in *Proceedings of the 2015 IEEE 8th International Conference on Cloud Computing*, pp. 909–916, New York, NY, USA, July 2015.

[15] J. Schlechtendahl, F. Kretschmer, Z. Sang, A. Lechler, and X. Xu, "Extended study of network capability for cloud based control systems," *Robotics and Computer-Integrated Manufacturing*, vol. 43, pp. 89–95, 2017.

[16] F. Farokhi, I. Shames, and N. Batterham, "Secure and private cloud-based control using semi- homomorphic encryption," *IFAC-PapersOnLine*, vol. 49, no. 22, pp. 163–168, 2016.

[17] K. Junsoo, C. Lee, H. Shim et al., "Encrypting controller using fully homomorphic encryption for security of cyber-physical systems," *IFAC-PapersOnLine*, vol. 49, no. 22, pp. 175–180, 2016.

[18] B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-purry, and D. Kundur, "Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed," in *Proceedings of the 2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR)*, pp. 1–6, Charleston, SC, USA, May 2015.

[19] A. W. Ordys, D. Uduehi, and M. Johnson, "Process control performance assessment, from theory to implementation," *Monograph Series: Advances in Industrial Control*, Springer Verlag London, Berlin, Germany, 2007.

[20] A. Ordys and M. J. Grimble, "Benchmarking and tuning PID controllers," in *PID Control in the New Millennium: Lessons Learned and New Approaches*, V. Visioli, Ed., Springer-Verlag, Berlin, Germany, 2012.

[21] F. Almada-Lobo, "The industry 4.0 revolution and the future of manufacturing execution systems (MES)," *Journal of Innovation Management*, vol. 3, no. 4, pp. 16–21, 2015.