Cybersecurity Issues in Motion Control – An Overview of Challenges

Živana Jakovljević, *ETRAN Member & Member, IEEE,* Dušan Nedeljković, *ETRAN Member*

***Abstract*—The fourth industrial revolution known as Industry 4.0 brings digitalization of manufacturing processes to a new level through ubiquitous interconnection and real-time information flow between information technologies (IT) and operational technologies (OT) as parts of Industrial Control Systems (ICS). This information flow is not limited to but expands beyond factory walls enabling manufacturing systems to adapt quickly and efficiently to changing customer demands and diversified products. The adaptation is carried out through physical and/or functional reconfiguration of manufacturing systems where Industrial Internet of Things (IIoT) based on Cyber-Physical Systems (CPS) represents the key technical enabler. These changes result in a transition from centralized to distributed control systems architecture where the whole control task is achieved through intensive cooperation between smart devices (e.g., sensors and actuators) with integrated communication and computation capabilities. However, introducing IIoT in ICS brings about new cybersecurity issues due to increased communication between system elements and connection to the global network, making ICS vulnerable to different cyber-attacks with potentially catastrophic consequences. Recently, the research in ICS cybersecurity has intensified leading to significant results for continuous time and discrete events-controlled systems. However, cybersecurity issues in motion control systems that are frequently employed in different manufacturing resources such as machine tools and industrial robots were not sufficiently explored. This work provides an overview of the cybersecurity related challenges in motion control tasks.**

***Index Terms*—Industry 4.0; Cybersecurity; Cyber-Physical Systems; Industrial Internet of Things; Motion Control.**

I. Introduction

INDUSTRY 4.0 as the technological response to the need for mass customization production implies full digitalization of manufacturing processes and completely digitalized information flow within company and beyond company walls [1]. This kind of digitalization requires ubiquitous communication inter and intra all levels of automation pyramid and traditional border between information technologies (IT) and operational technologies (OT) becomes fully permeable for automatic information flow [2]. Following this approach, Industrial Control Systems (ICS) are no longer isolated islands, and within Industry 4.0 they become part of the interconnected world with all the costs and benefits that this integration leads to.

One of the main gains of manufacturing digitalization is that real-time flow of information between IT and OT enables the effective and efficient adaptation of manufacturing systems to different customer needs and diversified products. This adaptation is achieved through physical and/or functional reconfiguration of manufacturing systems [3]. For both, the key technical enabler is Industrial Internet of Things (IIoT) based on Cyber-Physical Systems (CPS). Using CPS based devices such as intelligent sensors, the information necessary for functional reconfiguration of manufacturing systems is readily obtained in real-time.

In the case of physical reconfiguration, the role of CPS is even more prominent. Namely, physical reconfiguration (Fig. 1) requires modular equipment which is easily integrated not only at the mechanical subsystem, but also at the control subsystem level. CPS based equipment is tailored to this need since in these devices each mechanical module such as pneumatic cylinder or linear axis is augmented with its own local controller - LC [4], transforming mechanical modules to smart devices with integrated computational and communication capabilities. This shift leads to significant changes in the design of control systems where the traditional centralized control system architecture gives the way to distributed control systems. Instead of connecting all control loop elements (e.g., sensors and actuators) of one machine to the centralized controller, in the equipment based on smart devices the control of the whole machine is achieved through cooperation and intensive communication of modules' LCs that carry out allocated tasks.

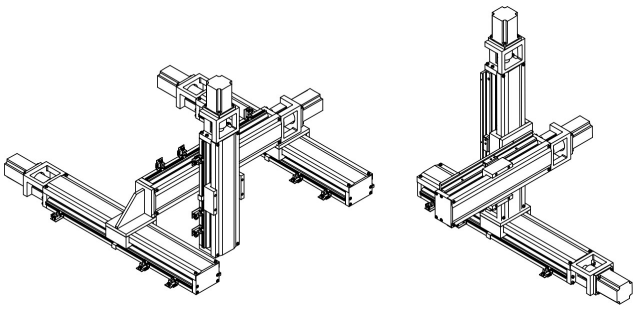

Fig. 1. Reconfigurable machine composed of several axes capable of executing different trajectories.

The main cost of the IIoT introduction in ICS refers to cybersecurity related issues. Namely, with the connection of OT to global network and intensification of communication between its elements, ICS become open to cyber-attacks by

Prof. Dr. Živana Jakovljević is with the Faculty of Mechanical Engineering, University of Belgrade, 16 Kraljice Marije, 11000 Belgrade, Serbia (e-mail: zjakovljevic@mas.bg.ac.rs), ORCID ID (https://orcid.org/0000-0002-7878-2909).

Dušan Nedeljković, MSc (ME) is with the Faculty of Mechanical Engineering, University of Belgrade, 16 Kraljice Marije, 11000 Belgrade, Serbia (e-mail: dnedeljkovic@mas.bg.ac.rs), ORCID ID (https://orcid.org/0000-0001-5909-4812).

 ISBN 978-86-7466-970-9

different adversaries. The consequences of cyber-attacks on ICS can be devastating and can lead to catastrophic damage to the equipment, environmental and safety issues, even to the loss of human lives.

For these reasons, in the last decade the research in the field of cybersecurity for ICS has intensified. A lot of efforts were directed to the cyber defense mechanisms in discrete event [5, 6] and continuous time controlled [7, 8] systems. However, cybersecurity issues in motion control systems that are frequently employed in different manufacturing resources such as machine tools for conventional and unconventional processes, industrial robots, pick and place devices, were not adequately addressed. Considering that communication intensive distributed control in these resources is readily met on shop floors, the lack of cybersecurity mechanisms can be considered as critical. In this paper we overview the cybersecurity related challenges in motion control tasks.

The remainder of the paper is structured as follows. Section 2 discusses cyber threats in ICS and proposes the taxonomy of cyber-attacks on ICS. Section 3 refers to the architecture of motion control systems and analyzes different points in which these systems can be distributed. Section 4 considers cybersecurity challenges in distributed motion control, whereas conclusions and future work guidelines are provided in Section 5.

II. Cyber Threats in Industrial Control Systems

Although recently there have been significant research results in cybersecurity for ICS, their application in real world plants is sporadic. Consequently, a number of successful attacks on ICS have been carried out.

Stuxnet attack that was launched on the Iranian uranium enrichment infrastructure in 2010 [9] represents a turning point in cybersecurity for ICS. It made all stakeholders aware that the consequences of cyber-attacks on ICS can be devastating, and vast funding was directed into the research in this field. Stuxnet affected installed Siemens WinCC SCADA (Supervisory Control and Data Acquisition) systems and PLCs (Programmable Logic Controller) from Siemens S7 product range. The PLCs were responsible for controlling centrifuges in the plant. Stuxnet recorded original data flow from PLCs to centrifuges during normal system operation for the time-period corresponding to a full operation cycle. After deliberate modification aiming the defects in operation, the data were communicated back from PLCs to centrifuges resulting in the breakdown of the devices.

One of the first malware designed for ICS, in particular for synchrophasor based real-time control and monitoring in smart grid, is BlackEnergy whose v1.0 was created in 2007 [10]. It is designed for distributed denial of service attacks, but also can be utilized for cyber-physical intelligence, spamming and deception attacks. This malware was used in several cyber-attacks, and the most famous is the attack on three Ukrainian electricity distribution companies in December 2015 [11]. The attack entered the system using spear-phishing emails and reconnaissance attack that followed obtained users' credentials and working habits. Using the acquired intelligence, companies' SCADA systems were compromised and several breakers within the electric grid were open. As a result, there was a six-hour long blackout in three provinces affecting over 225,000 people.

Another successful cyber-attack on ICS, fortunately without consequences, was launched on Oldsmar's water treatment system, Florida, USA in 2021 [12]. After remotely accessing the system control computer, adversary gradually increased sodium hydroxide content from 100 ppm to 11,100 ppm, the latter level being contagious for humans. However, the operator timely noticed the change in NaOH share, and the negative consequences for 15,000 inhabitants were avoided.

An attack on Colonial Pipeline, the largest fuel pipeline in the USA, was also carried out in 2021 [13]. Again, phishing email was utilized for cyber-physical intelligence that acquired almost 100 GB of data. Afterwards the pipeline system is put offline and ransom for not putting the stollen system data on the internet is required. The attack stopped operation of this critical national infrastructure that carries 2.5 million barrels a day and provides 45% of oil fuel supply for East Coast [14] for six days.

From the given overview of the most famous cyber-attacks on ICS it can be observed that adversaries launch different types of attacks, usually in cooperation, to successfully conduct their malicious intents. Therefore, the classification of cyber-attacks can be very important for understanding their working principles and further development of protection mechanisms.

In previous works several classifications of cyberattacks on ICS were presented [15, 16, 17, 18], but they were usually closely connected to the considered type of ICS such as smart grid [16], CPS [18] or to the considered class of attacks, e.g., denial of service [17]. In this paper, we propose the taxonomy of attacks on ICS that is presented in Fig. 2. At the highest level this taxonomy includes [19]:

1. Denial of Service (DoS) attacks,
2. Cyber-Physical Intelligence (CPI) attacks,
3. Deception attacks.

DoS attacks compromise the availability of data where the data source becomes temporarily or permanently unavailable resulting in data loss or latency. These attacks as a rule do not require a priori knowledge about the attacked system – only knowledge about implemented protocols is necessary. DoS attacks can be [20]:

- Message removal – adversary directly prevents message arrival to the destination.
- Message flooding – adversary sends too many messages or too large messages to a device and prevents the device to timely receive necessary messages from other system elements.
- Resource Exhaustion – adversary takes over all resources on a device (e.g., IEEE 802.15.14 channels) and prevents other devices from connecting.
- Application Crash – adversary sends to the device specially created message that causes the break of its application (e.g., stack overflow).

 ISBN 978-86-7466-970-9

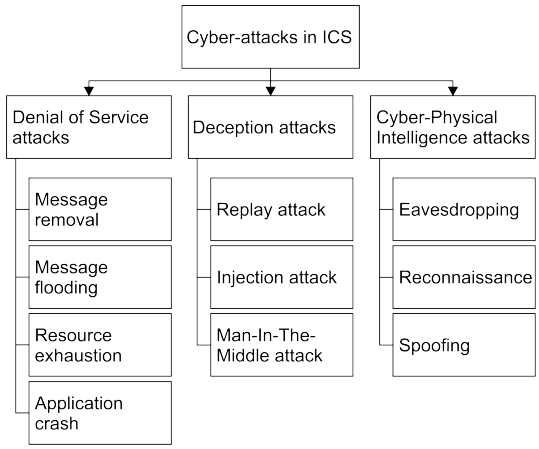

Fig. 2. Taxonomy of cyber-attacks on ICS.

Deception attacks change the data that is exchanged between devices or insert false messages on communication links and in this way compromise data integrity. These attacks are stealthy and perfidious, usually cannot be easily detected and can lead to very bad consequences for the system performance. To generate a successful deception attack, an adversary needs information about the attacked system and a model of its functioning. Deception attacks can be classified into:

- Replay attacks – adversary records data exchanged between devices in one period and replays it in another.
- Injection attacks – adversary injects false data in communication link between devices.
- Man-In-The-Middle (MITM) attack – adversary takes over communication link between devices and modifies the data in its own way.

CPI attacks acquire data and carry out system identification of the attacked system; they compromise the confidentiality of the system. They precede stealthy (deception or DoS) attacks. CPI attacks are classified into following categories:

- Eavesdropping – adversary takes over communicated packages.
- Reconnaissance – adversary takes over communicated messages and discovers vulnerabilities of the target either in an active engagement or as a passive observer; the goal is to get intelligence that will be used to create stealthy attacks.
- Spoofing – adversary successfully presents itself as another device that has privileges to communicate with the attacked device and gets access to communication links; this attack represents a basis of all deception attacks.

Generally, in ICS the deception attacks are considered as the most dangerous since they can lead to different changes in system functioning and remain undetected for a long time-period. DoS attacks if launched in properly selected time instants can also lead to different consequences and remain stealthy. Finally, the success of both deception and DoS attacks completely depends on the intelligence obtained using CPI attacks.

III. Distribution of Motion Control Tasks

Motion control represents the key element of control systems in the machines that can execute complex and programmable trajectories such as machine tools and industrial robots. For example, the control unit of a machine tool consists of Human-Machine Interface (HMI), Programmable Logic Controller (PLC) and Numerical Control Kernel (NCK). HMI is utilized for part program input or transfer from other elements of ICS such as Manufacturing Execution System (MES), program simulation before running, supervision of machine during automatic operation, machine control in manual operation, etc. PLC carries out all functions of the machine that are not related to its trajectory, such as turning on/off the spindle, emulsion feed start and stop, tools magazine control. Finally, NCK, as the most complex and important element of control unit, carries out the tasks related to the motion control of the machine.

As already discussed in introduction, to facilitate the reconfigurability of machines, it is necessary to introduce the modularity of its control software and hardware that closely follows already existing modularity of mechanical subsystem. In the case of machines with motion control, it is natural to introduce (Fig. 3):

i) High level controller (HLC) that carries out HMI and some of the PLC and NCK functions and
ii) Low-level controllers (LLC) for each of the axes. LLCs are responsible for some of the NCK functions and PLC functions related to the axes (e.g., limit switches).

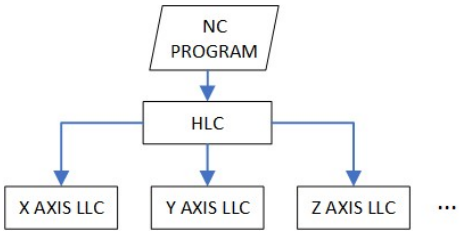

Fig. 3. Distribution of motion control tasks to individual axes.

The allocation of NCK functions to HLC and LLC is highly related to the structure of NCK. There are two types of NCK depending on the point at which Acceleration/Deceleration (Acc/Dec) is introduced into the trajectory segments [21]:

- Acc/Dec Control After Interpolation (ADCAI),
- Acc/Dec Control Before Interpolation (ADCBI).

ADCAI based NCK (Fig. 4a) consists of several software modules. The first module – interpreter parses the program and transforms it into internal data format suitable for subsequent processing. It calculates the desired trajectory segments (start and end points, radius and center points of arcs, etc.) taking into account workpiece and local coordinate systems, tool compensations and similar elements of the part program. Interpreted data are passed to the rough interpolator

 ISBN 978-86-7466-970-9

which calculates the motion of each axis in the form of the incremental reference positions that the axis should reach to achieve the commanded trajectory of the machine in synchronization with other axes. After rough interpolation, data is passed to Acc/Dec module that modulates the trajectory of each axis separately to enforce gradual change of the velocity (e.g., trapezoid or S shaped profile). Next module carries out fine interpolation to adjust the sampling interval of rough interpolator with sampling interval of position control loop that can be closed at higher rate. Finally, the required incremental reference positions of the axis are passed to position controller for execution.

In ADCBI (Fig. 4b) on the other hand, the rough interpolation and Acc/Dec control are carried out in different order, i.e., Acc/Dec control is performed before rough interpolation on the whole trajectory segment and not on the individual axis segment as in the ADCAI. Furthermore, a look-ahead module is introduced before Acc/Dec control to avoid unnecessary slowdowns between subsequent sections. The role of this module is to inspect interpreted command several segments ahead and to calculate feasible speeds at the beginning and the end of the segments depending on their length with the goal to achieve the commanded feedrate. The rough interpolator is followed by the fine interpolator and position controller.

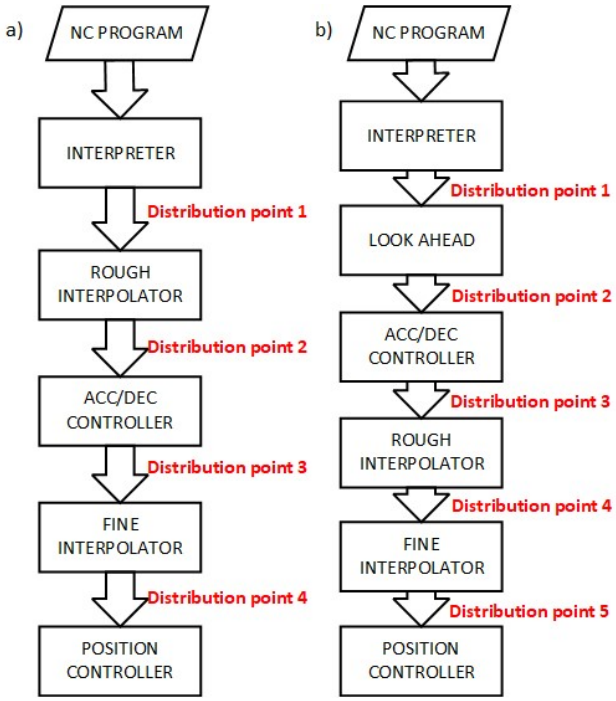

Fig. 4. The structure of NCK and possible distribution points: a) ADCAI, b) ADCBI.

It can be observed that regardless of the position of Acc/Dec control NCK has a modular structure in which the first modules, up to the rough interpolator, carry out the functionalities related to the whole machine, whereas the downstream modules consider each axis separately. From this structure it implies that natural points for distribution of control tasks between HLC and LLC are between subsequent software modules (Fig. 4).

A thorough analysis of the communication bandwidth and real-time requirements for distribution of control tasks between HLC and LLCs has shown that the most convenient distribution points are distribution point 2 for ADCAI and distribution point 4 for ADCBI (Fig. 4) [22]. These points are exactly after rough interpolator where the control system tasks transfer from those related to the whole machine to the tasks related to the individual axes. At these points, the data related to the incremental positions per one instance of interpolation period are passed between modules.

Traditionally all NCK modules, including position controller, are installed on a single control unit that passes relevant data to servo drivers which close velocity loops. However, contemporary servo drivers have the possibility to close position loop as well. This leads to the shift from centralized to NCK distributed at distribution point 4 for ADCAI and distribution point 5 for ADCBI [23] and in industrial practice networked motion control systems can be encountered more and more. These systems include [24]:

- Motion controller,
- Servo drivers,
- I/O modules, and
- Real-time Ethernet (RTE).

In networked motion control motor drives and I/O modules are integrated into the machines in plug-and-play manner using RTE and machine operates through intensive communication between these devices.

IV. Cybersecurity Challenges in Distributed Motion Control

Following the analysis of the distributed motion control presented in previous section, two levels of communication can be identified (Fig. 5) within distributed motion control in digitalized manufacturing:

i) Transfer of the program that contains trajectory (NC program) from the system at higher level of automation pyramid, e.g., MES to the HLC,
ii) Intensive communication between HLC and LLCs during machine operation at the selected distribution point.

Both levels of communication can be an attractive target for cyber-attacks. When the transfer of program to HLC is considered, the most significant cyber threats refer to deception attacks. Replay attack can lead to repetition of trajectory resulting in e.g., additional manufacturing of previously made part and economic consequences thereof. Injection and MITM attacks can alter the programs and lead to different changes in motion trajectory with respect to the originally created. Even if small, these changes can have significant effects on the system performance. For example, they can result in manufacturing of scrap due to dimension and tolerances unconformities. Furthermore, the program changes can lead to severe damages of the equipment or even to the safety issues e.g., if the robot collides with the

 ISBN 978-86-7466-970-9

environment due to the introduced program alterations, or if the changes in feedrate lead to the tool breakage in machining processes.

The consequences of DoS attacks at the level of transfer of program to HLC are far less severe since these attacks result in the latency of program execution start. In addition, DoS attacks at this level can be relatively easily detected as a problem in communication.

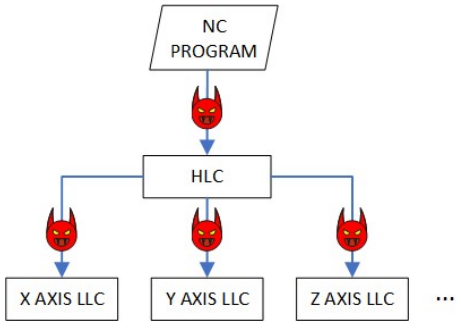

Fig. 5. Possible points of attack in distributed NCK.

Cybersecurity issues at the transfer of program to HLC are appropriately recognized and they were in the focus of a few research works. As a rule, in these investigations exteroceptive sensors were used to compare the commanded with the executed trajectory. For example, two approaches based on the analysis of multimedia signals for the detection of cyber-attacks in additive manufacturing are proposed in [25]. One method recognizes cyber-incident using spectral analysis of audio signal and the other carries out the comparison of the path reconstructed from video with the commanded path. As observed in this work, the method based on audio signal requires less expensive installation, but it is more sensitive to the background noise, thus making the method based on video stream preferable in long run. Cyber-attack detection in additive manufacturing based on vibration signal was also explored [26], where the features extracted using LSTM (long short-term memory recurrent neural networks) based autoencoder were employed.

Another research from [27] explored the implementation of machine learning, in particular the classification based on k-Nearest Neighbors (kNN), random forest and anomaly detection, for the detection of MITM attacks on communication of part programs in additive manufacturing and milling. For additive manufacturing image analysis of video stream and for milling analysis of audio signal is performed. In both use cases different machine learning methods have shown comparative results on selected cyber-attacks.

Research work presented in [28] considered the MITM attack that aimed at the change in the geometry of part obtained using CNC turning. In the proposed solution the attack is detected using control charts designed over the machining time of individual cutting cycles extracted from spindle power consumption.

The analyzed approaches represent pioneering research in cybersecurity for motion control and their effectiveness in the most perfidious attacks that aim exceedingly small, but effective changes in trajectory (e.g., resulting in violation of tolerances) is to be explored yet. Furthermore, these approaches can detect the changes in trajectory, but cannot localize their source. In addition, it is not clear where in the control system the methods would be employed and how the ground truth program would be securely presented to the method.

The second level of communication within distributed motion control - the communication between HLC and LLCs is more intensive and suitable for launching highly creative cyber-attacks. Namely, the execution of the commanded trajectory within desired tolerances requires the synchronization of individual axes motion and synchronous execution of LLCs' control algorithms. Even without attacks in distributed motion control this requirement represents a challenging task since LLCs are realized on different hardware components with potentially unsynchronized clock sources. Lack of clocks synchronization in LLCs leads to the unsynchronous actuation signals (motor pulse trains) and to the errors in the obtained trajectory as presented in Figure 6. For this reason, several methods for the synchronization of LLCs algorithms execution were developed [29, 30, 31].

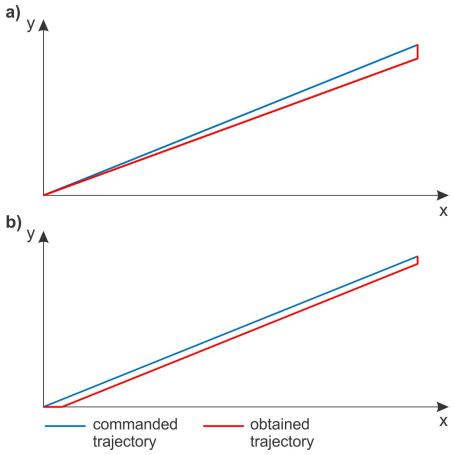

Fig. 6. Errors in trajectory introduced through the lack of synchronization between axes: a) y axis lags x axis for a fixed period; b) error in pulse width synchronization.

Thus, on the communication links between HLC and LLCs, in addition to deception attacks, DoS attacks if launched properly can lead to undesired consequences. Namely, short term DoS attack can remain unnoticed, but desynchronize axes or make their LLCs starve the tasks.

Although the distributed motion control at distribution point 4 for ADCAI and distribution point 5 for ADCBI is readily employed in industrial practice, the cybersecurity at this level of system integration did not draw the required research attention. One example of the investigations in this direction is the research from [32, 33] that proposed controller encryption for motion control systems.

V. Conclusion

This paper considered cybersecurity issues and challenges in motion control tasks within ICS. Firstly, we reviewed several

 ISBN 978-86-7466-970-9

attacks on ICS whose potential/real consequences have triggered faster developments in the field of ICS cybersecurity, and then we proposed the taxonomy of cyber-attacks on ICS. Our focus was directed to motion control as the key element of control systems in machines such as machine tools and industrial robots. Before consideration of security concerns, we explained how motion control tasks are distributed and what are possible distribution points according to the structure of NCK. Security issues were discussed in the context of two levels of communication, one between the system at the higher level of the automation pyramid and HLC, and the second between HLC and LLCs. The conducted analysis covered different types of attacks and points of attack. Obtained knowledge could hold significant value in the development of novel security mechanisms which represents the goal of our further research.

ACKNOWLEDGMENT

This research was supported by the Ministry of Science, Technological Development and Innovations of the Serbian Government under the contract No. 451-03-47/2023-01/200105.

REFERENCES

[1] H. Kagermann, W. Wahlster, J. Helbig, *Recommendations for implementing the strategic initiative INDUSTRIE 4.0*, Acatech, Berlin, 2013.

[2] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, "Guide to industrial control systems (ICS) security," NIST Special Publication, no. 800-82, rev. 2, 2015.

[3] Y. Koren, X. Gu, W. Guo, "Reconfigurable manufacturing systems: Principles, design, and future trends," *Front. Mech. Eng.,* vol. 13, pp. 121–136, 2018.

[4] V. Lesi, Z. Jakovljevic, M. Pajic, "Towards Plug-n-Play numerical control for Reconfigurable Manufacturing Systems," IEEE 21st International Conference on Emerging Technologies and Factory Automation, Berlin, Germany, pp. 1-8, 2016, doi: 10.1109/ETFA.2016.7733524.

[5] R. Fritz, P. Zhang, "Detection and Localization of Stealthy Cyber Attacks in Cyber-Physical Discrete Event Systems," *IEEE Trans. Automat. Contr.*, pp. 1-8, 2023, doi: 10.1109/TAC.2023.3253462.

[6] Z. Jakovljevic, V. Lesi. M. Pajic, "Attacks on Distributed Sequential Control in Manufacturing Automation," *IEEE Trans. Industr. Inform.*, vol. 17, no. 2, pp. 775-786, Feb. 2021.

[7] D. Nedeljkovic, Z. Jakovljevic, "CNN based method for the development of cyber-attacks detection algorithms in industrial control systems," *Comput. Secur.*, vol. 114, article 102585, 2022.

[8] D. Fährmann, N. Damer, F. Kirchbuchner, A. Kuijper, "Lightweight long short-term memory variational auto-encoder for multivariate time series anomaly detection in industrial control systems," *Sensors*, vol. 22, no. 8, article 2886, 2022.

[9] A. Nourian, S. Madnick, "A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 1, pp. 2–13, 2015.

[10] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, S. Sezer, "Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid," 4th International Symposium for ICS & SCADA Cyber Security Research, Belfast, UK, pp. 53–63, Aug. 2016.

[11] A. Cherepanov, R. Lipovsky, "Blackenergy–what we really know about the notorious cyber attacks," Virus Bull October 2016. [Online]. Available: https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cherepanov-Lipovsky.pdf, Accessed: 15-Apr-2023.

[12] J. Tidy, "Hacker tries to poison water supply of florida city," 2021. [Online]. Available: https://www.bbc.com/news/world-us-canada-55989843, Accessed: 15-Apr-2023.

[13] J. Tidy, "Colonial hack: How did cyber-attackers shut off pipeline?," 2021. [Online]. Available: https://www.bbc.com/news/technology-57063636, Accessed: 15-Apr-2023.

[14] M.A. Russon, "US fuel pipeline hackers 'didn't mean to create problems'," 2021. [Online]. Available: https://www.bbc.com/news/business-57050690, Accessed: 1-Apr-2023.

[15] D. Ding, Q.L. Han, Y. Xiang, X. Ge, X.M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 2018.

[16] G. Elbez, H.B. Keller, V. Hagenmeyer, "A new classification of attacks against the cyber-physical security of smart grids," Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, pp. 1–6, Aug. 2018.

[17] A.O. de Sá, L.F.R. da Costa Carmo, R.C. Machado, "Covert attacks in cyber-physical control systems," *IEEE Trans. Industr. Inform.*, vol. 13, no. 4, pp. 1641–1651, 2017.

[18] A. Teixeira, D. Perez, H. Sandberg, K.H. Johansson, "Attack models and scenarios for networked control systems," Proceedings of the 1st international conference on High Confidence Networked Systems, Beijing, China, pp. 55–64, Apr. 2012.

[19] Y. Xu, Y. Yang, T. Li, J. Ju, Q. Wang, "Review on cyber vulnerabilities of communication protocols in industrial control systems," Proceedings of 2017 IEEE Conference on Energy Internet and Energy System Integration, Beijing, China, pp. 1–6, Nov. 2017.

[20] OPC foundation, OPC UA Online Reference, OPC 10000-2: OPC Unified Architecture, Part 2: Security Model, Release 1.04, 2018-08-03. [Online]. Available: https://reference.opcfoundation.org, Accessed: 15-Apr-2023.

[21] S.H. Suh, S.K. Kang, D.H. Chung, I. Stroud, *Theory and Design of CNC Systems*, Springer-Verlag, London, 2008.

[22] V. Lesi, Z. Jakovljevic, M. Pajic, "IoT-Enabled Motion Control: Architectural Design Challenges and Solutions," *IEEE Trans. Industr. Inform.*, vol. 19, no. 3, pp. 2284-2294, 2023.

[23] K. Erwinski, M. Paprocki, L. M. Grzesiak, K. Karwowski, A. Wawrzak, "Application of ethernet powerlink for communication in a linux rtai open cnc system," *IEEE Trans. Ind. Electron.*, vol. 60, no.2, pp. 628–636, 2013.

[24] N. Zhou, D. Li, "Cyber–Physical Codesign of Field-Level Reconfigurations in Networked Motion Controllers," *IEEE ASME Trans. Mechatron.*, vol. 26, no. 4, pp. 2092-2103, 2021.

[25] W. Yang, J. Chen, C. Zhang, K. Paynabar, "Online detection of cyber-incidents in additive manufacturing systems via analyzing multimedia signals," *Qual. Reliab. Eng. Int.*, vol. 38, no. 3, pp. 1340-1356, 2022.

[26] Z. Shi, A.A. Mamun, C. Kan, W. Tian, C. Liu, "An LSTM-autoencoder based online side channel monitoring approach for cyber-physical attack detection in additive manufacturing," *J. Intell. Manuf.*, vol. 34, pp. 1815–1831, 2023.

[27] M. Wu, Z. Song, Y.B. Moon, "Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods," *J. Intell. Manuf.*, vol. 30, no. 3, pp. 1111-1123, 2019.

[28] M. H. Rahman, M. Shafae, "Physics-based detection of cyber-attacks in manufacturing systems: A machining case study," *J. Manuf. Syst.*, vol. 64, pp. 676-683, 2022.

[29] M. Paprocki, K. Erwiński, "Synchronization of Electrical Drives via EtherCAT Fieldbus Communication Modules," *Energies*, vol. 15, no. 2, article 604, 2022.

[30] V. Lesi, Z. Jakovljevic, M. Pajic, "Synchronization of Distributed Controllers in Cyber-Physical Systems," IEEE International Conference on Emerging Technologies and Factory Automation, Zaragoza, Spain, pp. 710–717, Sept. 2019.

[31] C. Dripke, D. Schoebel, A. Verl, "Distributed Interpolation: Synchronization of motion-controlled axes with coordination vector and decentralized segment controllers," IEEE 16th International Workshop on Advanced Motion Control, Kristiansand, Norway, pp. 141-146, Apr. 2020.

[32] K. Teranishi, K. Kogiso, J. Ueda, "Encrypted Feedback Linearization and Motion Control for Manipulator with Somewhat Homomorphic Encryption," 2020 International Conference on Advanced Intelligent Mechatronics, Boston, USA, pp. 613-618, July 2020.

[33] K. Teranishi, M. Kusaka, N. Shimada, J. Ueda, K. Kogiso, "Secure Observer-based Motion Control based on Controller Encryption," 2019 American Control Conf, Philadelphia, USA, pp. 2978-2983, July 2019.