Article

Stealthy Cyberattacks Detection Based on Control Performance Assessment Methods for the Air Conditioning Industrial Installation

Jakub Mozaryn [1]*, Michał Fratczak [2], Krzysztof Stebel[2], Tomasz Klopot [2], Witold Nocon[2], Andrzej Ordys[1], and Stepan Ozana[3]

[1] Institute of Automatic Control and Robotics, Faculty of Mechatronics, Warsaw University of Technology; jakub.mozaryn@pw.edu.pl
[2] Department of Automatic Control and Robotics, Faculty of Automatic Control, Electronics and Computer Science, Silesian University of Technology, 44-100 Gliwice, Poland; michal.fratczak@polsl.pl
[3] Department of Cybernetics and Biomedical Engineering, Faculty of Electrical Engineering and Computer Science, VSB-Technical University of Ostrava, 17. listopadu 2172/15, 708 00 Ostrava-Poruba, Czech Republic; stepan.ozana@vsb.cz
* Correspondence: jakub.mozaryn@pw.edu.pl

Abstract: The paper aims to study the workflow of the detection center of stealthy attacks on industrial installations that generate increase in energy consumption while avoiding triggering fault detection and damaging the installation. Such long-lasting attacks on industrial facilities make production more expensive and less competitive. We present the concept of the remote detection system of cyberattacks directed at maliciously changing the controlled variable in an industrial process air conditioning system. The monitored signals are gathered at the PLC-controlled installation and sent to the remote detection system, where the discrepancies of signals are analyzed based on the Control Performance Assessment indices. The results of performed tests prove the legitimacy of the adopted approach.

Keywords: cyberattack, control variable, feedback system, cyberattack detection, process air conditioning station.

1. Introduction

On December 23, 2015, the power grid of Ukraine was hacked, resulting in power outages for roughly 230,000 consumers in Ukraine for 1-6 hours. Around 0.015% of daily electricity consumption in Ukraine was not supplied (up to 73 MWh of electricity) [1]. The attack was distributed in an email via an infected Word document or PowerPoint attachment. Then BlackEnergy 3 malware remotely compromised the information systems of three energy distribution companies in Ukraine and temporarily disrupted consumer electricity supply [2].

TXOne Networks, the OT zero trust and Industrial IoT (I-IoT) security company has published a 2021 cybersecurity report [3] which focuses on the vulnerabilities that can affect Industrial Control Systems (ICS). According to the report, the number of advisories dramatically increased in 2021, when there were 389 advisories published, compared with 249 a year earlier. The growing number of cyberattacks aiming at disrupting critical infrastructure (CI) clearly shows that hackers seek new attack vectors for their potentially dangerous activities.

The CI is the set of systems and their related objects, consisting of buildings, devices, installations, and services, essential to the security of the state and its citizens and ensuring the efficient functioning of public administration, institutions and entrepreneurs [4]. CI consists of the following systems: (a) supply of energy and fuels, (b) communica-

 doi:10.20944/preprints202212.0259.v1

tions, (c) ICT (Information and Communication Technologies) networks, (d) financial, (e) food supply, (e) water supply, (f) health protection, (g) transport, (h) rescue, (i) public administration, (j) production, (k) storage, warehousing and usage of chemical and radioactive substances, including pipelines of hazardous substances. CI plays a key role in the state's functioning and citizens' lives. Because of events caused by forces of nature or human activities, CI may be destroyed or damaged, and its operation may be disrupted, which may endanger the life and property of citizens. Such events negatively affect the economic development of the country. Therefore, protecting CI is the priority of every state. The essence of tasks related to CI comes down not only to ensuring its protection against threats but also to ensure that potential damage and disruptions in its functioning are as short as possible, easy to remove and do not cause additional losses for citizens and the economy. Protection of CI is all activities aimed at ensuring the functionality, continuity of operations and integrity of CI to prevent threats, risks or vulnerabilities, limit and neutralise their effects, and restore this infrastructure quickly in the event of failures, attacks and other events interfering with its proper functioning. In many states, cooperation with private enterprises is important because, in many cases, a substantial part of the CI of key importance for state security is privately owned.

In modern industrial companies, there exist overlapping technologies, ie. Information Technologies (IT) regarding information, its flow, and administration and Operating Technologies (OT) regarding the operation of physical processes and the machines (e.g. controllers, actuators, sensors) used to implement them. Such synergy is called IT/OT convergence, and the two-way flow of information between these technologies brings the production process closer to the business world. For example, a visible trend has been observed in the monitoring and control of industrial plants based on the Industrial Internet of Things (I-IoT) devices and Computing Cloud (e.g. Control as a Service - CaaS) [5]. Despite significant improvements in cost, flexibility, and maintenance, it also introduces new problems that need to be addressed on the OT level, such as cybersecurity. Conventional ICSs are traditionally equipped with signal-induced fault detectors searching for anomalies in control and sensor signals concerning the behaviour of the ICS. They consist of estimating the state of the system and comparing the estimated states with the states measured by the sensors (i.e. residuals). Many works exist on defining faulty states based on the computed residuals (e.g.Chi-Square or CUSUM).

Until recently, the issues of detecting anomalies were carried out independently as Intrusion Detection Systems (IDS) in case of cyberattacks (security) or Advanced Diagnostic Systems (ADS) in case of technical faults (safety). However, cyber-attacks in the ICS can currently be seen as an anomaly generator [6]. Considering the industrial process specificity, process model and controller performance, the ADS should be equipped with the methods to detect and distinguish cyberattacks and process faults in OT infrastructure, thus working in parallel and exchanging information with IDS [7].

The three main cyberattack types on ICS can be distinguished:

- **Integrity attacks** that aim to degrade the control performance of the ICS (e.g. False Data Injection Attacks (FDIA), Man-In-The-Middle (MITM) attacks).
- **Availability attacks** that aim to disrupt the operations of some control equipment (e.g. DoS attacks),
- **Confidentiality attacks** that aim to collect information from the ICS (e.g. eavesdropping attacks).

Such attacks can be **stealthy attacks (covert attacks)** that generate anomalies while keeping fault detectors below their detection threshold and damaging or intruding into the system in the long term (e.g. Stuxnet) or **non-stealthy attacks** that are often quick-in-time attacks with huge impact.

Covert attacks refer to scenarios where an attacker has access to sensor measurements and system controllers and also possesses sufficient knowledge of system operations [8], [9], [10], [11]. Some attacks aim at understanding the control architecture (e.g. control law implemented in controllers, the response of supervisions, fault detection

 doi:10.20944/preprints202212.0259.v1

threshold) or knowing the field equipment (e.g. sensors, actuators) to launch further integrity or availability attacks [12].

There are distinguished three main areas of possible cyberattacks on the ICS with a set of attack vectors each [13, 14]:

- **Cyberattacks on software**, e.g. Buffer Overflow, SQL injection, Cross Site Scripting (XSS).
- **Cyberattacks on hardware**, i.e., accessing the physical location of the ICS in an unauthorised way to damage and modify the operational procedure of the system, e.g. make changes on certain threshold values.
- **Cyberattacks on communication**, i.e., exploiting the communication channel and protocol vulnerabilities, exploiting unnecessary ports and services.

In small and medium enterprises, SCADA (Supervisory Control And Data Acquisition) systems are vital to the ICS. The common practices of the SCADA system designers and operators with low-security levels cause them to be extremely vulnerable to various OT cyberattacks [15][16]. The broadly discussed and analysed virus Stuxnet is a typical example of a long-term covert attack damaging the system. It was revealed after it had caused over 1000 failures of the uranium enrichment centrifuges [17]. Another example is Triton malware targeting the SCADA / ICS system of the Saudi Arabian petrol company Petro Rabigh which went unnoticed for three years before being detected [18, 19]. Such covert cyberattacks are considered the most challenging to detect. There are two popular approaches for detecting covert attacks. The first one is based on the correlation among the sensor measurements assuming that the measures follow a known correlation structure. When part of the sensor measurements is manipulated, the original correlation structure does not hold, which is reflected in the residuals [11]. The second one is based on analysing the dynamics of the system. The attacker is assumed to have imperfect knowledge of the system dynamics. Thus, malicious manipulations of some sensor measurements and their control actions will not necessarily conform to the expectations of the operator and can, therefore, be detected by monitoring the residuals [20][21][22].

In the paper, we propose to use the Control Performance Assessment (CPA), used to measure the quality of a control system, for cyberattack detection [23][24]. The CPA bases on the study of the chosen indexes [25], based on the control system signals, can be grouped into the following classes (a) Step Response Indexes, (b) Data-Based Integral Measures, (c) Statistical Measures, (d) Model-based Measures, (e) Frequency Based Measures. The assessment requires methodologies and indexes (Key Performance Indicators) that enable measuring the system's quality and undertaking necessary improvement steps. CPA methods also allow benchmarking of different systems to prioritise maintenance actions. Furthermore, some of the measures may show a reason for the inappropriate operation, useful in detecting the deterioration of the system work. In the article, we discuss the use of data-based statistical measures, allowing the detection of possible anomalies in the system, and searching for the deterioration and possible statistically important changes within measured signals.

2. Motivation

Umsonst and Sandberg [26] presented an experimental evaluation of sensor attacks and defence mechanisms in feedback systems. Such attacks assume that the attacker can stealthily manipulate sensor readings in the control system, thus making the control system oblivious to the fact that the desired set points of process variables are not achieved. On the one hand, this will immediately affect the product quality, resulting in high costs of wasted raw materials and energy. In some cases, quality control in the plant should be able to relatively quickly detect the problem with deteriorating quality, and a proper investigation should lead to uncovering the stealthy sensor reading problem.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 December 2022 doi:10.20944/preprints202212.0259.v1

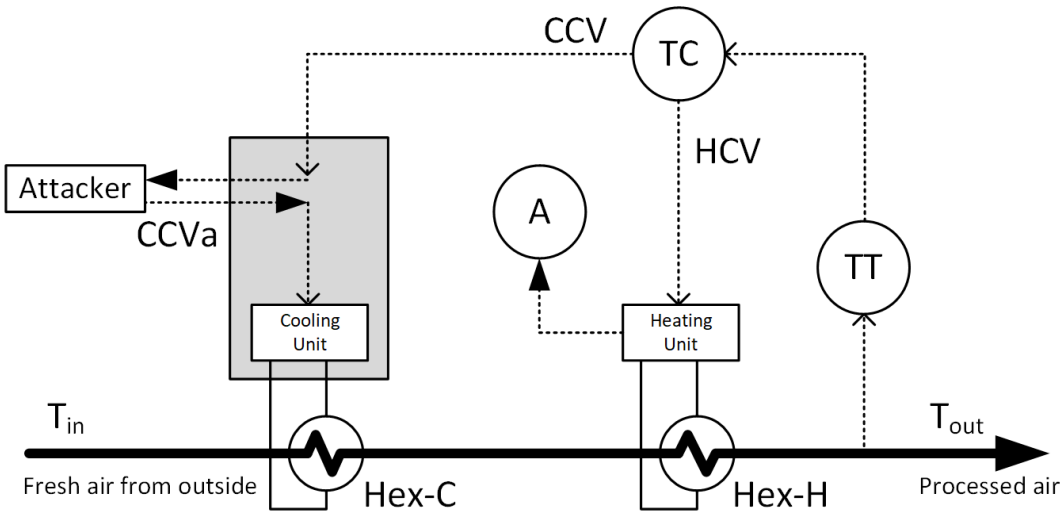
In this article, we evaluate the problem of stealthy manipulation of a selected control variable, especially in a feedback system requiring two independent control variables having opposite effects on the process variable. For example, when temperature control requires both heating and cooling, the attacker may try to change the operating regime of the cooling process, thus forcing the heating part of the system to increase energy usage to compensate for the temperature drop caused by the attack-related cooling. In such a case, the feedback control system will correctly maintain the controlled temperature according to the desired setpoint, thus preventing product quality deterioration. This will obviously prevent costs associated with raw materials wasting but will increase the cost of consumed energy and will only be possible to detect using continuous or periodical inspection of control system.

Therefore in this paper, we demonstrate a cyber-attack directed at maliciously manipulating a controlled variable (CV) in a feedback system and propose methods to detect such attacks. The process under consideration requires both cooling and heating to keep the desired temperature od process air. It is assumed that the heater's energy consumption (for example, the electric current) is monitored and it is very often fulfilled in practice, e.g. for diagnostics purposes. . However, because the cooler in the system is assumed to operate independently and, in many cases, requires energy consumption for the preparation of the cooling agent in advance, a straightforward identification of concurrent cooler and heater operation is not sufficient for detecting malicious manipulation of the cooler.

3. Models and methods

3.1. Feedback system under attack

The feedback system under consideration is an air conditioning unit, in which fresh air of inlet temperature Tin = 20°C passes through both a cooling unit and a heating unit (Fig. 1). Such approaches are used, for example, in air conditioning systems for paint shops. A process variable (PV) in this feedback system is the measured temperature Tout of the conditioned air.. A split range control algorithm uses two different control variables: a cooling unit controlled by the cooling control variable (CCV) when PV exceeds the set point (SP) or the heating unit controlled by the heating control variable (HCV) when SP exceeds PV. The heating unit is supplied with hot water at 90°C, and the temperature is controlled by a changing its flow of 0-20 L/min.The cooling unit is supplied by a glycol at 1°C, and temperature is controlled by a manipulating its flow of 0-20 L/min. It is assumed that the feedback system is properly tuned and inadvertent fast switching between the cooler and the heater are avoided.



 doi:10.20944/preprints202212.0259.v1

Figure 1. Feedback control of the air conditioning unit.

The assumed mode of cyber attack is through the cooling unit. If the attacker gets access to the internal data processing of the cooling system, the CCV value can be read and changed by the attacker to a new cooling control variable (CCVa). Moreover, it is assumed that our control system can't monitor the inner variables of the cooling unit, and the malicious manipulation of the cooling unit will not be directly detected. This assumption seems justified since many cooling units are sold as single and closed systems, with only a limited number of process variables exposed to the plantwide control system. Therefore, the attacker can force the cooling unit to operate and decrease the air temperature, even if cooling is not required. The feedback control system will react accordingly by increasing the power consumed by the heating unit, and the temperature of the process (albo conditioned) air will be maintained. However, the operating costs of the air conditioning unit will be significantly increased. Because the inner parameters of the cooling unit are not monitored, such a situation may last for prolonged periods. Heating unit's power consumption is measuredusing electric current measurement. For instance, thyristor power controllers often enable easy reading of output power.

Therefore, the following assumptions are made in the presented demonstration of cyber-attack detection. The measured variables are the temperature of the fresh air Tin, the temperature of the processed air Tout with its set point SP, and power consumption based on the electrical current measurement A.. The unknown or unmeasurable parameters are the power consumption of the cooling unit and the cooling control variable CCVa, manipulated by cyber-attack. Additionally, it is impossible to prevent the cooler from working simultaneously as the heating unit and vice versa since the closed cooling unit needs to prepare ice water in advance.

In this article we assume only a limited scope of cyber-attack. First, it is assumed that the setpoint temperature SP is greater or equal to Tout. Hence only the heater unit is being used by the split range controller. Secondly, it is assumed that the attacker maliciously manipulates the cooling controlled variable by increasing it and cooling the fresh air, thus forcing the controller to increase power consumption.

3.2 Proposed attack detection approach

In our research, we use the standard control performance assessment method based on Minimum-Variance (MV) benchmark to reveal the possible cyber threats. The proposed MV benchmark (as a reference performance bound) can be estimated from data monitored online (e.g. process value, control value). The only assumption is that the system delay estimate is known.

In CPA, the reference best feedback control used to benchmark is the Minimum-Variance Control (MVC, i.e. optimal H2 control) [26]. MVC produces the smallest possible closed-loop output variance, and it is worse for any other linear controllers. The MVC-based assessment compares the actual system-output variance σ_y^2 to the output variance σ_{MV}^2 as obtained using an MVC applied to an estimated time-series model from measured output data. The so-called Harris index (HI) is defined as [27]

$$\eta_{\mathrm{MV}} = \frac{\sigma_{\mathrm{MV}}^2}{\sigma_y^2} \tag{1}$$

Harris index is calculated from the measured data and is given in the interval [0,1], where a value close to 1 indicates best possible control concerning the theoretically achieved

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 December 2022 doi:10.20944/preprints202212.0259.v1

output variance, while 0 means the worst performance, including unstable control. Harris index is typically calculated for the process value, however, it can be used as the measure to assess any signal variance, and in our case can be adopted to the course of the control signal, allowing for the detection of potential anomalies (changes in variance) caused, among others, by cyberattacks. There are two advantages to using η_{MV} over σ_y^2: (a) it is independent of the underlying disturbances, and (b) η_{MV} is bounded between 0 and 1, thus we can set the threshold value that will indicate the deterioration of the signal, which can be due to the possible cyber-attack.

We calculate the Harris index as follows [28]

$$\widehat{\eta_{\mathrm{MV}}} = \frac{(n-b-m+1)\widehat{\sigma_{\mathrm{MV}}^2}}{\underline{\tilde{u}}^T\underline{\tilde{u}} + \bar{u}^2} \tag{2}$$

where n is the sample length, b is the estimated delay, m is a model rank.

The estimate of the residual mean square error is given by

$$\widehat{\sigma_{\mathrm{MV}}^2} = \frac{(\underline{\tilde{u}} - \tilde{X}\underline{\hat{\alpha}})^T(\underline{\tilde{u}} - \tilde{X}\underline{\hat{\alpha}})}{(n-b-2m+1)} \tag{3}$$

To calculate the estimate $\widehat{\sigma_{\mathrm{MV}}^2}$ we solve the set of linear equations

$$(\tilde{X}^T\tilde{X})\underline{\hat{\alpha}} = \tilde{X}^T\underline{\tilde{u}} \tag{4}$$

where

$$\underline{\tilde{u}} = \begin{bmatrix} \tilde{u}_n \\ \tilde{u}_{n-1} \\ \vdots \\ \tilde{u}_{b+m} \end{bmatrix}, \tilde{X} = \begin{bmatrix} \tilde{u}_{n-b} & \tilde{u}_{n-b-1} & \dots & \tilde{u}_{n-b-m+1} \\ \tilde{u}_{n-b-1} & \tilde{u}_{n-b-2} & \dots & \tilde{u}_{n-b-m} \\ \vdots & \vdots & \vdots & \vdots \\ \tilde{u}_m & \tilde{u}_{m-1} & \dots & \tilde{u}_1 \end{bmatrix}, \underline{\alpha} = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_m \end{bmatrix} \tag{5}$$

and

$$\tilde{u}_n = u_n - \bar{u} \tag{6}$$

is the corrected deviation of the control value u_n from its mean value $\bar{u}$.

.

3.3 System architecture

Fig. 2 presents the experimental set-up used in the presented research. The proposed architecture generally assumes that identifying cyber attacks is outsourced and performed by a remotely connected data centre,as outsourcing practice is becoming common nowadays. The presented cyberattack detection methods could be also realised using locally implemented systems, for example, edge computing [30]. Such an approach, however, needs more scalability and closer integration of the attack detection system with the hardware infrastructue of the control system. Therefore it was decided to prepare a distributed system, which fullfills the industrial requirements, considering security of the data.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 December 2022 doi:10.20944/preprints202212.0259.v1

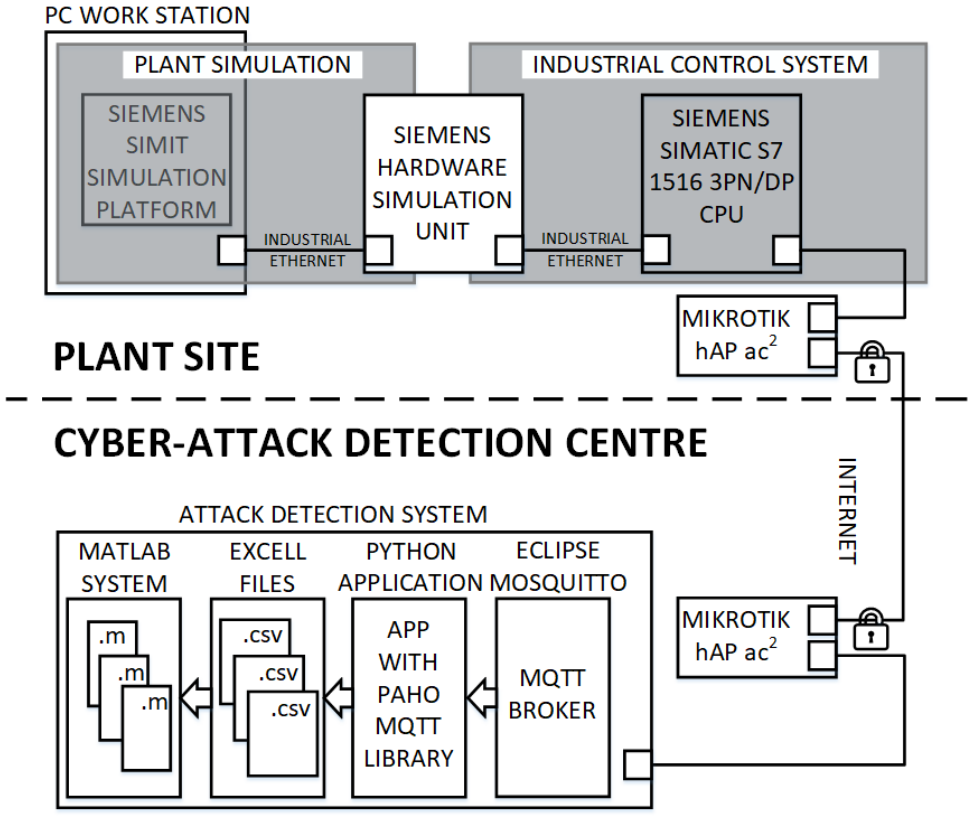


Figure 2. Distributed laboratory setup based on outsourcing idea

The system consists of a plant site and a cyber attack detection centre. The two parts communicate using a secure, tunnelled connection based on the Mikrotik hAP ac2 device. Physically, the plant site was located at the Silesian University of Technology in Gliwice, Poland, and the cyber attack detection centre was at the Warsaw University of Technology in Warsaw, Poland.

The plant site consists of a PC workstation, on which the air conditioning system (Fig. 1) is simulated. The simulation is implemented in the Siemens Simit Simulation Platform (Fig. 3), which is commonly used in industrial practice for the virtual commissioning of control systems[31,32]. This module simulates a ProfiNet process interface based on industrial Ethernet and serves as a connection between the control system and process simulation. The industrial control system was implemented using Siemens Simatic S7-1516-3 PN/DP PLC. This PLC implements the control algorithm and provides the capability of using the MQTT protocol, which enables safe communication with the distant cyber-attack detection centre.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 December 2022 doi:10.20944/preprints202212.0259.v1

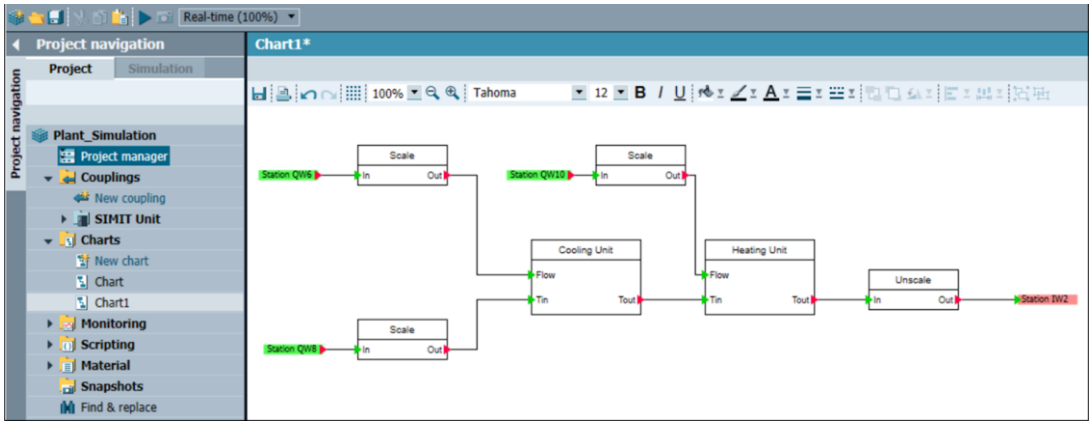


Figure 3. Simulation of the air conditioning unit in Siemens SIMIT.

The distant cyber-attack detection centre is based on a set of applications, including a data acquisition module that retrieves all necessary data from the plant side PLC using the MQTT protocol. Eclipse Mosquitto is used as the MQTT broker and mediates communication by both clients. From the client's point of view, communication is done only with the broker, and direct communication between clients is not possible. This principle facilitates the scalability of the MQTT network and enables easy expansion of the data set exchanged between clients. Additionally, all data is encrypted using TLS and user authentication based on login, and a password is provided. Data acquisition and storage are implemented in Python, acts as a MQTT client and uses the paho.mqtt.python library. Data is stored using csv files that are, in turn, imported into MATLAB for cyber-attack detection analysis.

4. Experimental results

The proposed cyber-attack detection method has been verified for periodic signals maliciously added to the control variable of cooling unit. Two different attacks were analysed: a triangular and sinusoidal signal (Fig. 4 and Fig. 5) added to the cooling control signal. The amplitude and frequency of the attack signal have been chosen so that the influence of the attack signal on process temperature is well within the noise range of the signal and is not clearly visible. Therefore, although process operators pay close attention to process variables (temperature in this case), such an attack would not have been easily detected. Potentially, this attack may be seen by observing the control signal of the heating unit; therefore Harris index is computed, which detects changes in the analysed signal variance. Harris index was calculated for N=1000 samples of the measured heating control signal, for a model of rank m = 30 and for a time delay tau = 1 sample with a moving window of n = 200 samples.

Fig. 6 presents results for a triangle attack signal being added as the CCVa signal, particularly the effect on the measured heating unit current HU [%]. Fig. 7 presents results for adding a sinusoidal attack signal as the CCVa signal. As can be seen, HU [%] is a good basis for detecting the attack. Since the variance of the HU signal increases, the Harris index decreases and can be thresholded to generate the attack detection signal. The threshold was selected as 0.2 based on historical data in this case. A slight delay in the detection signal concerning the actual attack is visible.

 doi:10.20944/preprints202212.0259.v1

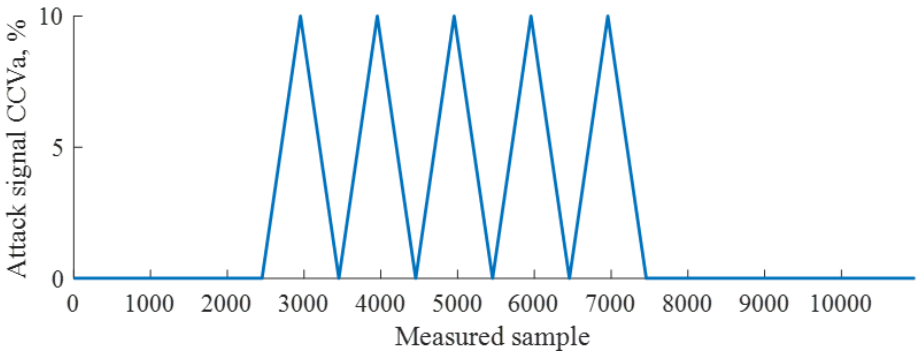


Figure 4. Triangle attack signal.

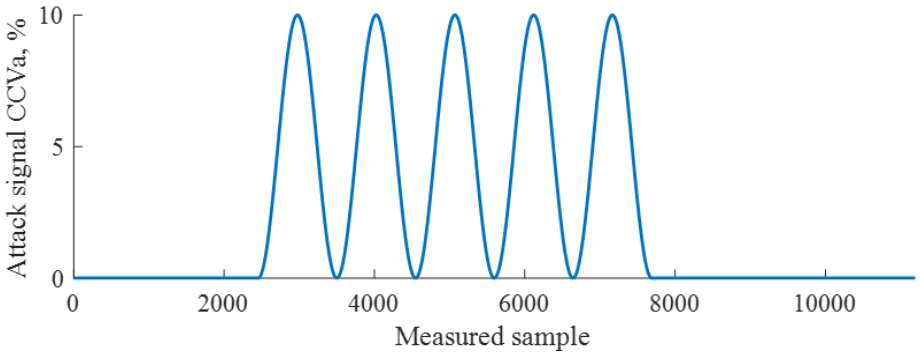


Figure 5. Triangle attack signal.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 December 2022 doi:10.20944/preprints202212.0259.v1

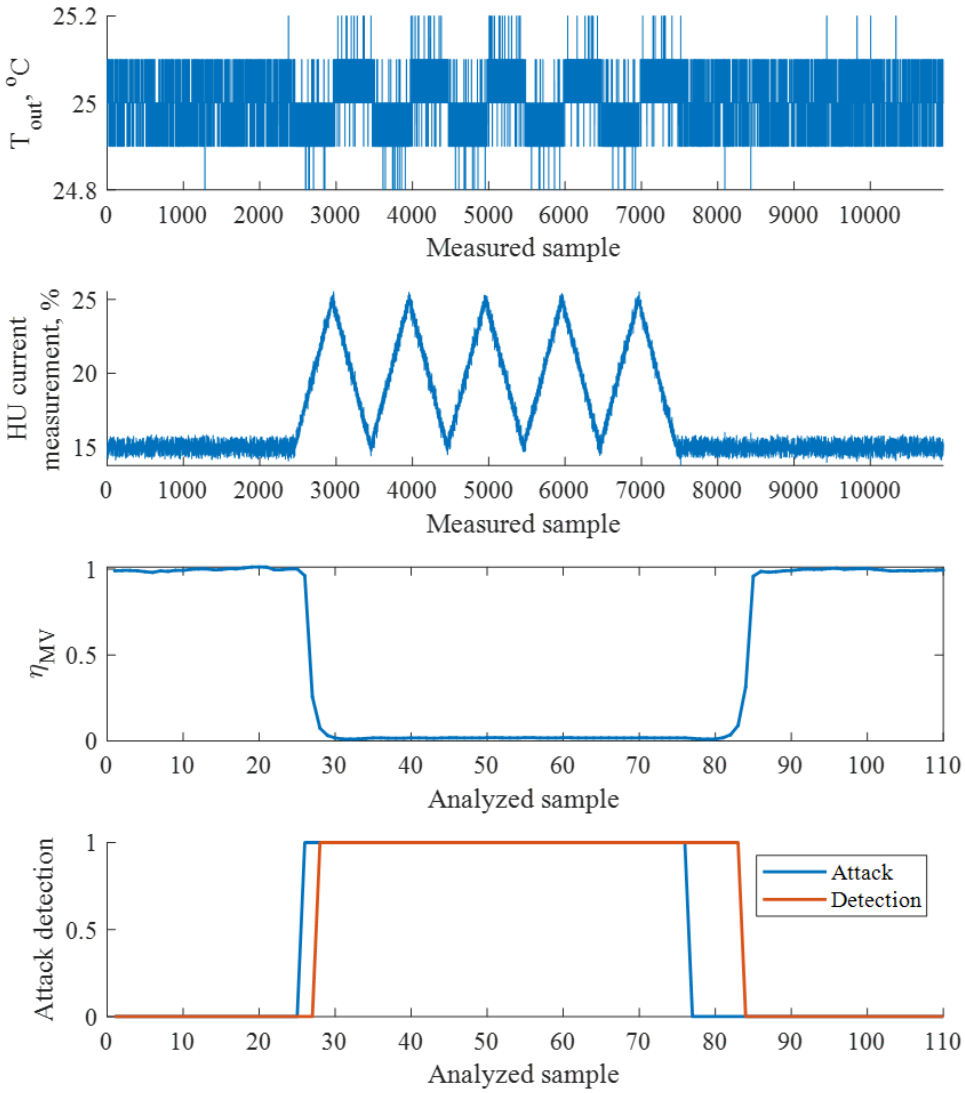


Figure 6. Effect of the triangular attack signal on process control.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 December 2022 doi:10.20944/preprints202212.0259.v1

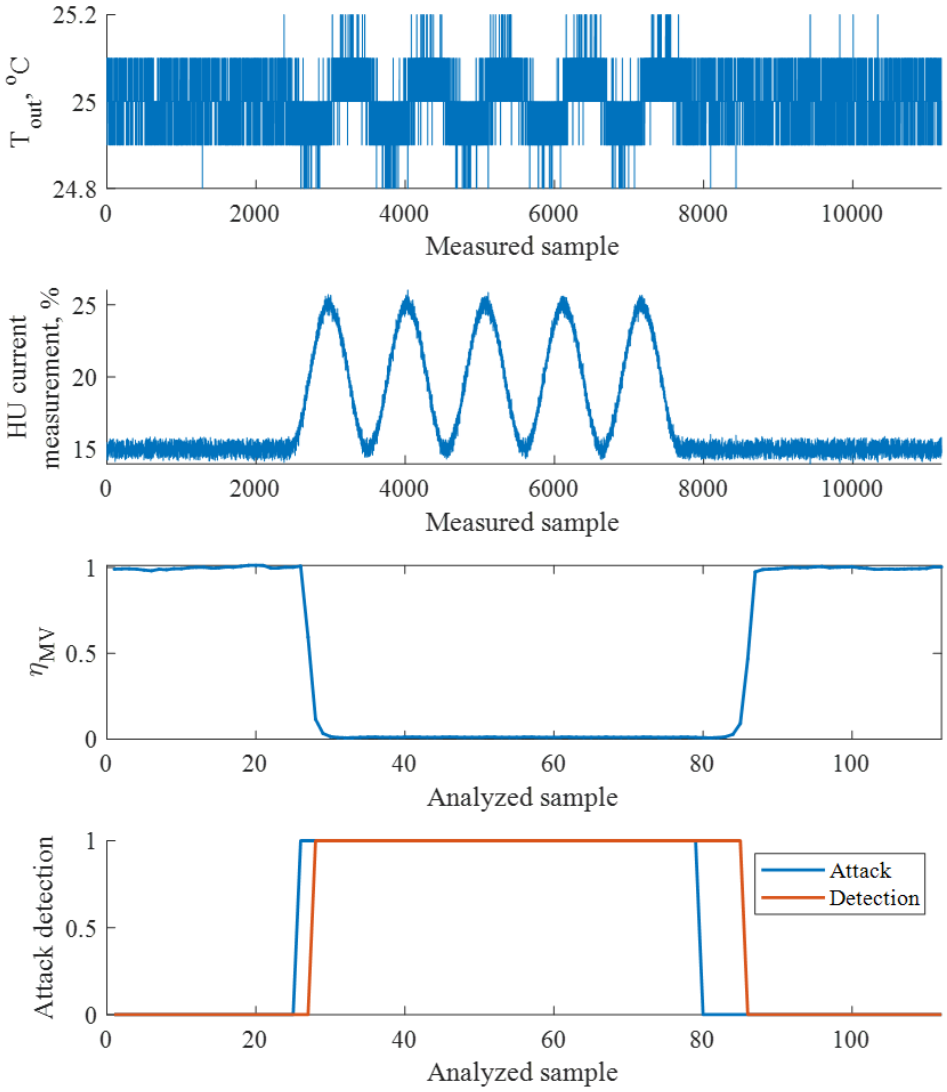
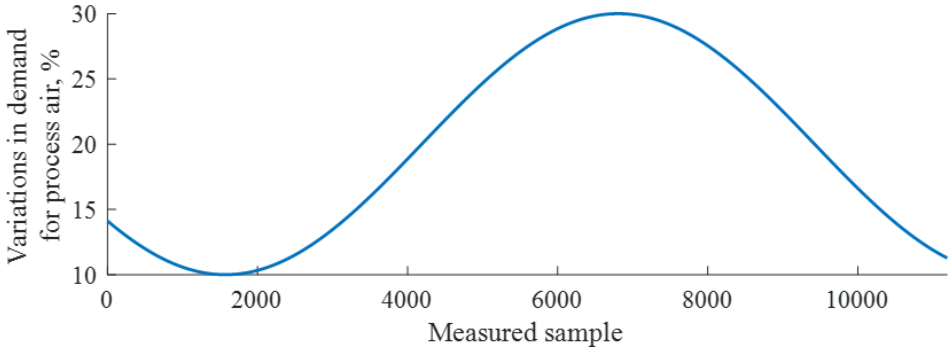


Figure 7. Effect of the sinusoidal attack signal on process control.

Results presented in Fig. 6 and 7 have been generated assuming that no natural disturbances caused by the process itself are present (for example, varying demand for processed air) or from varying parameters of fresh air from the outside. (for example, varying temperature and/or humidity). Fig. 8 presents a natural disturbance added into the process, representing changes in air demand for the air conditioning system. Figs. 9 and 10 present results for an additional sinusoidal process disturbance having a lower frequency concerning the attack signal itself.



 doi:10.20944/preprints202212.0259.v1

Figure 8. Changes in process air demand that represent natural disturbances in the process.

In this case, the variance of the HU signal is considerably larger, even when no attack is currently active, leading to increased changes in the Harris index. Based on historical data, a different threshold value has been selected as 0.1, and the attack is assumed active if HI is lower than 0.1.

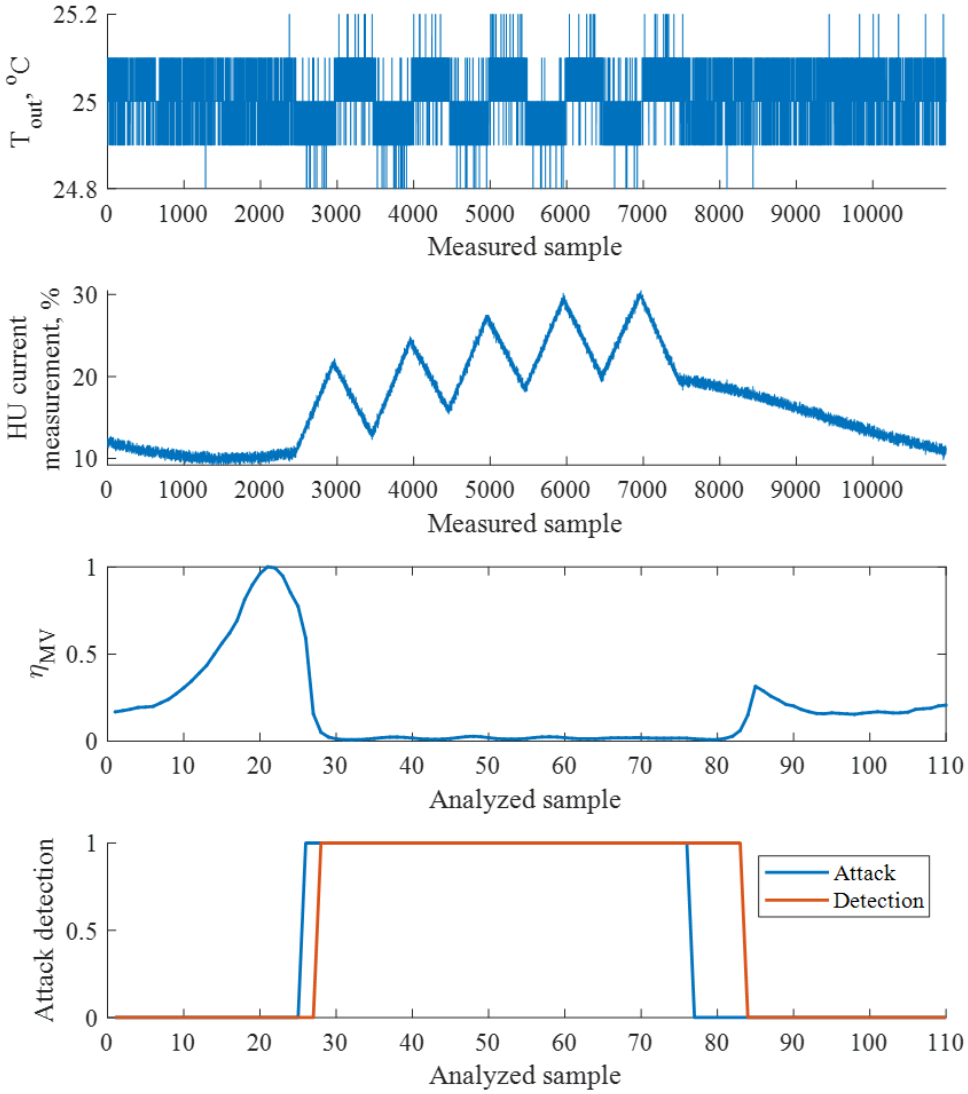


Figure 9. Triangular attack signal on top of a low-frequency natural sinusoidal disturbance.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 December 2022 doi:10.20944/preprints202212.0259.v1

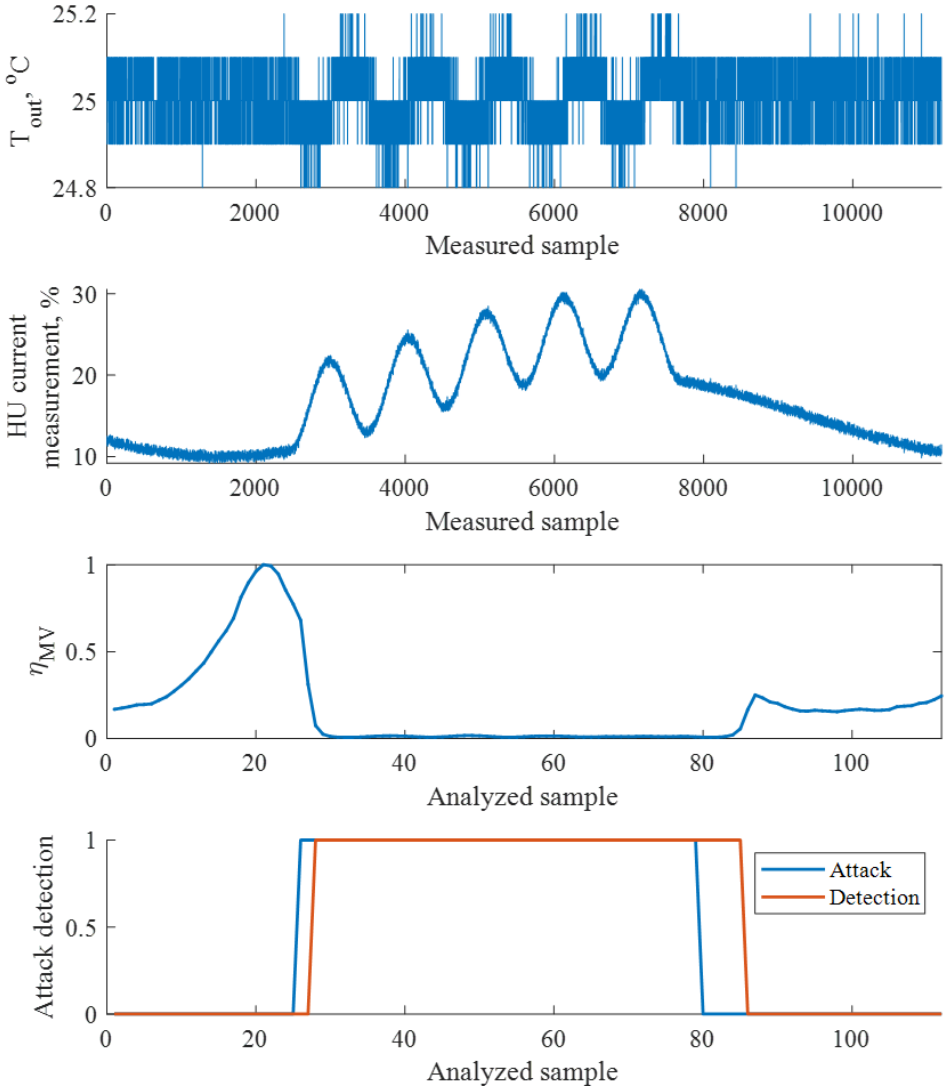


Figure 10. Sinusoidal attack signal on top of a low-frequency natural sinusoidal disturbance.

5. Conclusions

The method of stealthy attacks detection on the industrial installation based on the data-driven statistical control performance measure was presented. As an example, we used the simulation of the air conditioning installation where we evaluate the problem of stealthy manipulation of a selected control variable, especially in a feedback system requiring two independent control variables having opposite effects on the process variable. The proposed monitoring system has been implemented on the two industrial-type workstations and PLC controllers (one for the process workstation and the second for the anomaly detection centre), connected remotely using secure tunnelling communication.

The presented results suggest that the Harris index may be potentially used to detect periodic attack signals being added into one of the control variables. In reality process operators rarely focus on the control signal regularly; therefore, such a tool would support the operator and technology crews in detecting process cyber attacks. Obviously, control signal variance may change due to other reasons, for example, because of control units wearing out. The increased variance, however, unequivocally points to the problem

with the control performance. Precise detection of a cyber attack requires additional analysis of the situation, for example, by observation of network traffic [33].

Regarding the Harris index as a potential measure for cyberattack detection, we should emphasise that it requires proper tuning of the parameters, i.e. sample length, estimated delay, and model rank. Moreover, further experimental research should be performed to choose the detector thresholds for different types of attacks.

Author Contributions: Conceptualization, J.M., T.K., A.O.; methodology, J.M., M.F. and K.S.; software, J.M., M.F. and K.S.; validation, J.M., K.S., T.K. and SO; formal analysis, W.N.; investigation, J.M., M.F. and W.N.; resources, T.K., M.F.; data curation, K.S.; writing—original draft preparation, J.M., W.N., T.K.; writing—review and editing, W.N., T.K., S.O.; visualization, W.N. and K.S.; supervision, A.O.; project administration, A.O.; funding acquisition, A.O. and T.K. All authors have read and agreed to the published version of the manuscript

Funding: Andrew Ordys ands Jakub Możaryn acknowledge support from the National Agency of Academic Exchange (NAWA), "Polish Returns," grant No: PPN/PPO/2018/1/00063/U/00001; and from the POB Research Centre Cybersecurity and Data Science of Warsaw University of Technology within the Excellence Initiative Program - Research University (ID-UB). This work was financed in part by the grant from Silesian University of Technology - subsidy for maintaining and developing the research potential in 2022 The APC was co-funded by the Warsaw University of Technology and the Silesian University of Technology.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest

References

1. Gilbert, D. (2014). Black energy cyber attacks against Ukrainian government linked to Russia. *International Business Times. http://www. ibtimes. co. uk/blackenergy-cyber-attacks-against-ukrainian-government-linked-russia-1467401. Zugegriffen*, *4*.
2. Paganini, P. (2017). Black-Energy Used as a Cyber Weapon Against Ukrainian Critical Infrastructure. *Infosec Institute*.
3. TXOne, (2022). 2021 Cybersecurity Report, *https://www.txone.com/security-reports/2021-cybersecurity-report/*.
4. Hokstad, P., Utne, I. B., & Vatn, J. (2012). *Risk and interdependencies in critical infrastructures*. Springer, London.
5. Możaryn, J., et al. (2020). Design and development of industrial cyber-physical system testbed. In *Advanced, Contemporary Control* (pp. 725-735). Springer, Cham.
6. Kościelny, J., et al. (2021). Towards a unified approach to detection of faults and cyber-attacks in industrial installations. In *2021 European Control Conference (ECC)* (pp. 1839-1844). IEEE.
7. Syfert, M., Ordys, A., Kościelny, J. M., Wnuk, P., Możaryn, J., & Kukiełka, K. (2022). Integrated Approach to Diagnostics of Failures and Cyber-Attacks in Industrial Control Systems. *Energies*, *15*(17), 6212.
8. F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems", IEEE transactions on automatic control, vol. 58, no. 11, pp. 2715–2729, 2013
9. A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems", in 49th IEEE Conference on Decision and Control (CDC). Atlanta, GA. DEC 15-17, 2010, 2010, pp. 5991–5998.
10. A. O. de Sa, L. F. R. da Costa Carmo, and R. C. Machado, "Covert attacks in cyber-physical control systems", IEEE Transactions on Industrial Informatics, vol. 13, no. 4, pp. 1641–1651, 2017.
11. D. Van Long, L. Fillatre, and I. Nikoforov, "Sequential monitoring of SCADA systems against cyber/physical attacks", IFAC-PapersOnLine, vol. 48, no. 21, pp. 746-753, 2015.
12. Syfert, M., et al. (2023). Simulation Model and Scenarios for Testing Detectability of Cyberattacks in Industrial Control Systems. In *International Conference on Diagnostics of Processes and Systems* (pp. 73-84). Springer, Cham.
13. R. S. Smith, "A decoupled feedback structure for covertly appropriating networked control systems", IFAC Proceedings Volumes, vol. 44, no. 1, pp. 90–95, 2011.
14. Zhu, Bonnie, Anthony Joseph, and Shankar Sastry. "A taxonomy of cyber attacks on SCADA systems." *2011 International conference on internet of things and 4th international conference on cyber, physical and social computing*. IEEE, 2011.
15. Irmak, Erdal, and İsmail Erkek. "An overview of cyber-attack vectors on SCADA systems." *2018 6th international symposium on digital forensic and security (ISDFS)*. IEEE, 2018.
16. Buchanan, Scott Steele. "Cyber-Attacks to Industrial Control Systems since Stuxnet: A Systematic Review." (2022).
17. Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2022). SCADA Vulnerabilities and Attacks: A Review of the State-of-the-Art and Open Issues. Computers & Security, 103028.

18. Albright, D., Brannan, P., & Walrond, C. (2010). *Did Stuxnet take out 1,000 centrifuges at the Natanz enrichment plant?*. Institute for Science and International Security.
19. Myung, J. W., & Hong, S. (2019). ICS malware Triton attack and countermeasures. *International Journal of Emerging Multidisciplinary Research*, *3*(2), 13-17.
20. Di Pinto, A., Dragoni, Y., & Carcano, A. (2018, August). TRITON: The first ICS cyber attack on safety instrument systems. In *Proc. Black Hat USA* (Vol. 2018, pp. 1-26).
21. Schellenberger, C., & Zhang, P. (2017, December). Detection of covert attacks on cyber-physical systems by extending the system dynamics with an auxiliary system. In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)* (pp. 1374-1379). IEEE.
22. Hoehn, A., & Zhang, P. (2016, July). Detection of covert attacks and zero dynamics attacks in cyber-physical systems. In 2016 American Control Conference (ACC) (pp. 302-307). IEEE.
23. Li, D., Paynabar, K., & Gebraeel, N. (2021). A degradation-based detection framework against covert cyberattacks on SCADA systems. IISE Transactions, 53(7), 812-829.
24. Jelali, M. (2012). Control performance management in industrial automation: assessment, diagnosis and improvement of control loop performance, Springer, https://doi.org/10.1007/978-1-4471-4546-2.
25. Domański, P. D. (2020). Control Performance Assessment: Theoretical Analyses and Industrial Practice (Vol. 245). Cham: Springer.
26. Umsonst, D.; Sandberg, H. Experimental evaluation of sensor attacks and defense mechanisms in feedback systems, Control Engineering Practice 124 (2022) 105178.
27. Astrom, K. J. (1971). Introduction to Stochastic Control Theory. Elsevier.
28. Harris, T. J. (1989). Assessment of control loop performance. The Canadian Journal of Chemical Engineering, 67(5), 856-861.
29. Desborough, L., & Harris, T. (1992). Performance assessment measures for univariate feedback control. The Canadian Journal of Chemical Engineering, 70(6), 1186-1197.
30. Georgakopoulos, D., Jayaraman, P. P., Fazia, M., Villari, M., & Ranjan, R. (2016). Internet of Things and edge cloud computing roadmap for manufacturing. IEEE Cloud Computing, 3(4), 66-73.
31. Bysko S., et al. PID controller tuning by virtual commissioning - a step to Industry 4.0, Journal of Physics - Conference Series, 2022, vol. 2198,
32. Fratczak M., et al., Component-based simulation tool for virtual commissioning of control systems for heat exchange and distribution processes, Automation 2020: towards industry of the future : Proceedings of Automation 2020, Warsaw, Poland, March 18-20, 2020.
33. Nazir, S., Patel, S., & Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security*, *70*, 436-454.