Towards a unified approach to detection of faults and cyber-attacks in industrial installations

Jan Kościelny*, Michał Syfert*, Andrzej Ordys*, Paweł Wnuk*, Jakub Możaryn*, Bartłomiej Fajdek*, Vicenc Puig, Krzysztof Kukiełka***

Abstract: **This paper investigates enhancing the ability to detect cyber-attacks by using information and methods related to fault detection. An experimental stand, and an associated simulator have been constructed to enable tests of combined cyber attacks and faults in industrial processes, and, possibly, to distinguish between them. Some scenarios of cyber attacks have been presented, analysed theoretically and then tested on the simulator, demonstrating that detection of cyber attacks by this method is possible.**

I. INTRODUCTION

Cyber-physical systems has been recognized as one of the key research areas in the research programs of the European Union [EU, 2020] as well as by the US National Science Foundation [NSF, 2016]. This is an important area research that is likely to dominate the design of control systems in the coming years as it results from the rapid advances in computer science and communication and industrial networks. Such systems are one of the pillars of Industry 4.0 [Dastbaz, 2019], a concept describing changes in production, leading to the so-called 4th industrial revolution. However, many of the new technologies can also be a potential threat to existing and fully operational processes, so safety is one of the essential elements.

Safety can be considered both in the sense of detection of physical damage to individual components of a process, and protection against their effects, and protection against the effects of incorrect actions of operators or the control system itself. Another important aspect is "security" - understood as protection of the system against intentional hostile actions aimed at taking control over the system, along with the possibility of destructive influence on its operation. Regardless of the cause, the effect can be the same: disruption of the cyber-physical system, or even its temporary or permanent immobilization (destruction).

This article considers the analysis of selected aspects of cybersecurity of interconnected *Information Technologies* (IT) and *Operational Technologies* (OT). IT and OT systems are currently operating in parallel within the so-called IT-OT convergence [Kamal, 2016], which allows for efficient monitoring and regulation of industrial processes. The current development and implemented technologies have the potential to enable connectivity between each of the devices in the office and in the industrial production workshop, in order to increase the availability of OT components while collecting and analyzing data about them.

Since computing primarily involves the storage, retrieval, manipulation and transmission of digital information, data and its confidentiality are the main problem here. IT security is crucial in any organization to ensure proper data protection and control. Safety and availability of devices and processes dominate in OT. The key is to maintain the continuity of work, which requires maintaining stable values of parameters (e.g. temperature, pressure or speed), requiring meticulous control. In summary, IT prioritises data confidentiality, OT focuses directly on process and people security.

In recent years, there have been several sophisticated cyber attacks on OT networks, exploiting vulnerabilities and new attack vectors resulting from IT-OT convergence [Applegate, 2013, Lee, 2014, Lee, 2016, Sullivan, 2017]

Based on the description of the attacks, it seems justified to use both IT solutions and those based on OT techniques, especially methods of diagnostics of devices and processes, in order to protect against cyber threats.

This article is organized as follows. In Section 2 fault detection and classification of cyber-attacks are described. In Section 3, a case-study test-stand and simulator for testing the detection are presented. In Section, 4 a theoretical analysis of cyber-attacks scenarios is given. Section 5 presents the preliminary simulation results.

II. DETECTION OF FAULTS AND CYBER-ATTACKS

Both faults and cyber attacks, as long as they get through standard security layers, manifest themselves in various changes in the functioning of the control system and the process deviating from its normal state. The resulting changes are observed by the operator as a sequence of alarms informing about exceeding the alarm limits by individual process variables.

The works [Kościelny et al. 2018, 2020; Van Long Do, 2015] show that *Industrial Control Systems* (ICS) can detect cyber attacks using diagnostic methods based on quantitative and / or qualitative models. These methods use only working signals so as not to interfere with the process flow. The paper [Sanchez et al, 2018] shows a different approach to identifying cyber attacks in ICS systems. In this approach,

*Institute of Automatic Control and Robotics, Faculty of Mechatronics, Warsaw University of Technology, ul. Sw Andrzeja Boboli 8, 02-525 Warszawa; e-mail: Firstname.Secondname@pw.edu.pl, e.g. Michal.Syfert@pw.edu.pl).

Those authors acknowledge support from a grant „Priority research area" from Warsaw University of Technology

Andrzej Ordys also acknowledges support from the National Agency of Academic Exchange (NAWA), "Polish Returns", grant No: PPN/PPO/2018/1/00063/U/00001.

**Polytechnic University of Catalonia (e-mail:vicenc.puig@upc.edu)

additional test signals are injected into the system, in particular, a sinusoidal signal with a time-varying frequency (authentication signature). This signal is injected into the closed-loop system and it is checked whether the output signal is compatible with the signature or not. This solution is analogous to the approach used in the past in analogue systems.

To detect cyber attacks, methods based on classic *Fault Detection and Isolation* (FDI) approach, e.g. [Frank, 1990, Blanke et al, 2002, Isserman, 2005, Gheorghe et al, 2013, Baeten et al, 2016], can also be used. It is assumed that either process components, measuring devices and/or actuating devices [Li et al. 2019] are being damaged. Failures of control units are detected independently by the dedicated diagnostic systems of the digital structure of the control system. For this task, methods of diagnostics of computer systems are used, which operate on the basis of self-testing and mutual testing by processor units. This approach fails, however, for cyber attacks that can target control circuits, changing the way they operate without damaging the control units. Therefore, a diagnostic system that should recognize both damage and cyber attacks should monitor the correct functioning of the regulatory loops. For this purpose, qualitative models in the form of rules provided in [Kościelny et al., 2018] can be used. It should be noted, however, that when qualitative models are used, only the symptoms of damage/cyber attacks should be taken into account in diagnostic conclusions. The absence of a symptom does not guarantee that it is fully operational. Monitoring control loop performance approaches are also used to detect degradation in the functioning of control loops [Harris, 1989; Xia et al, 2006, Saha P et al., 2012].

While the use of models to detect either damage or cyber attacks is beyond doubt, the approaches used to isolate (locate) damage are not directly useful for distinguishing between damage and cyber attacks. The basis for locating faults is determining the relationship between faults and the values of diagnostic signals. This relationship is determined on the basis of modelling, taking into account the impact of damage, learning or, most often, expert knowledge. It takes various forms [Kościelny et al., 2016], e.g. binary or trivalent signatures, as well as rules corresponding to lines of a binary diagnostic matrix or a Fault Isolation System. In the case of cyber attacks, it is not possible to determine their relationship with the values of diagnostic signals, e.g. providing signatures. The method (scenario) of an attack depends on its target as well as the creativity and knowledge of the attacker.

Therefore, a research problem emerges: how to distinguish a cyberattack from a damage that may arise in the controlled process and in the control system itself? At present, this is an open problem and any proposed approaches may contribute to the final solutions. However, it seems that the basis for distinguishing these threats is an advanced fault diagnostics system, which should ensure full fault detection and a high level of their distinguishability. The basis for identifying cyber attacks can be any redundancy of information that allows to detect inconsistencies between the observed symptoms and signatures of the damage. Therefore, the hardware and analytical redundancy of measurements in the ICS itself, as well as the redundancy of partial models and detection algorithms, are useful for this. The results of the operation of diagnostic system should be compared with the operation of the alarm system. Moreover, it is advisable to use the measurements existing in the Safety Instrumented Systems (SIS). The measurements used by the diagnostic system are made with separate measuring devices than in the SIS system. However, the use of such redundancy, requires a one-way data transmission from SIS to ICS. Furthermore, copies of the control system configuration database can be used to identify some cyber attacks. This allows detecting database intrusions and hostile modifications to the parameters of control systems.

Hence a rational methodological approach is to search for an explanation of the emerging disturbances in ICS functioning, starting with the hypothesis of a fault, with associated methods of fault detection, and then, if there is no proper match, to put forward a cyberattack hypothesis and to attempt to justify it.

III. Description of the Experimental Set-up

A system of two coupled tanks has been identified previously as a suitable candidate to test the algorithms of cloud-based control on one hand and the cyber-security of industrial installations on the other hand [Costa et al. 2013, Sanchez et al, 2018]. Hence, such a system is also considered in this study. The instrumentation part of laboratory test stand is presented in Fig. 1.

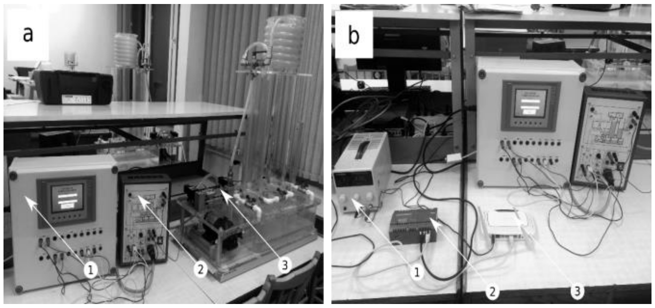

Fig. 1). Picture of the laboratory stand: a-1) control cabinet, a-2) control interface, a-3) test stand, b-1) power supply, b-2) SIMAATIC IOT2040 industrial gateway, b-3) router.

Components of the stand (Fig. 1) are: tanks Z_1 and Z_2, a pump P that is controlled by standard current signal that corresponds to a change of the pump capacity , LT_1 , LT_2 are pressure transducers for measuring a liquid level in each of tanks H_1, H_2). There are electro-mechanical cut-off valves V_1, V_2 , V_3, V_4 which are used to change the way that liquid flows.

There are also two cut-off electro-mechanical valves (VE_1 , VE_2), used to introduce disturbances into the process. By ZK_1 we denote leakage from the tank Z_1 (opening the valve VE_1), and by ZK_2 we denote leakage at pump outlet (opening the valve VE_2).

The control cabinet contains a Siemens SIMATIC S7-1200 controller. The device has Profinet/ Industrial Ethernet interfaces which are integrated with support for TCP / IP, ISO-on-TCP and S7 protocols. The controller can diagnose and monitor software through the Ethernet port and can communicate via RS-232, RS-485 and Modbus RTU protocols.

The environment also contains tools for creating new libraries of project objects (process variables, most frequently used functions - e.g. PID). A proven concept of OB organizational blocks, FC functions as well as FB function blocks and DB data blocks [Stenerson, 2015] is used.

The given test-stand allows for the design and evaluation of fault diagnosis and fault-tolerant control. Moreover, due to the controller having networking interface and the use of digital communication protocols also and cyber-security algorithms for cyber-physical systems can be tested. Due to its versatility and reconfigurability, the stand can be used to test various scenarios of possible cyber-attacks on industrial installations [Możaryn et al, 2020].

IV. Description of the Simulator of the Process

In parallel with the development of the experimental stand in the hardware version, its simulator in the software version has been created. The idea of developing a simulator is based on the following assumptions:

- as faithful as possible mapping of the operation of individual process components, including modelling the impact of classic faults in measuring channels, actuators and in technological components;
- modelling the communication links between the system components, according to the communication standards used,
- ensuring the possibility of replacing the simulator's subsystems with the corresponding physical subsystems and thus creating hybrid hardware and software solutions (hardware in the loop simulation),
- modelling of additional subsystems that will not necessarily be available in the hardware version, e.g. the security system,
- possibility to simulate selected failure scenarios.

The following main subsystems can be distinguished in the simulator:

- **Process.** A subsystem representing the physical components of the station together with measuring devices. The individual components, as far as it was possible, have been modelled on the basis of the description of physical phenomena. Physical parameters of equations, disturbances and additional factors, such as measurement noise, were selected on the basis of the analysis of real measurement signals and the behaviour of real components. A detailed diagram of this subsystem is shown in Fig. 5.
- **Control.** A subsystem representing the PLC controller, where the signals controlling the configuration are generated and the control system is implemented.
- **Operator interface.** The subsystem corresponding to the HMI / SCADA system on which the operator interface is implemented.

The vectors of set-point values and configuration options (SP + CFGs), control and configuration signals (CVs, CTRLs) and process variables (PVs) are transmitted/exchanged between subsystems.

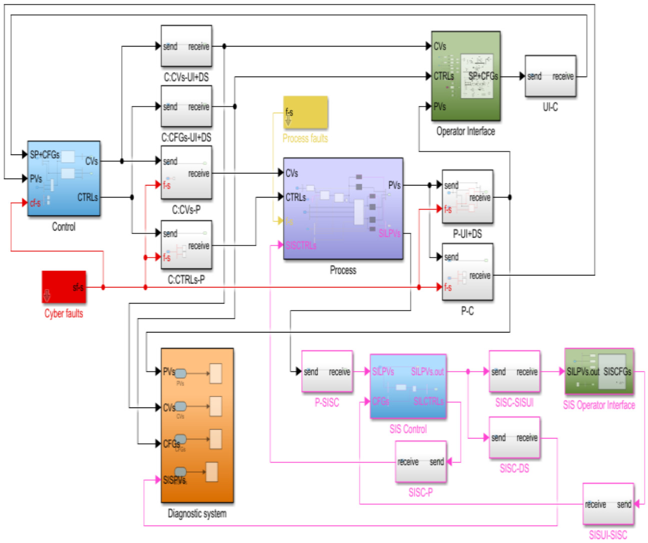

Fig. 2). Block diagram of the Coupled Tanks System simulator with additional elements - main subsystems.

Additional subsystems of the simulator are responsible for:

- representation of the safety system (SIS Control + SIS Operator Interface). The safety system uses a separate measurement system and has independent actuators assigned),
- implementation of the classical process diagnostics (Diagnostic system).

The individual subsystems are connected with blocks that represent communication links using specific communication standards. These blocks are the places of "disconnection" of the simulator, they enable the replacement of a given subsystem by its hardware version. This makes it possible to implement hardware-in-the-loop simulation.

An important feature of the simulator is that it enables modelling of failures in physical technological component as well as modelling of communication errors and modelling the operation of the control systems. For simulation purposes, a dedicated vector of process faults has been defined. This allows for various fault scenarios to be carried out. Faults from this group are the point of interest for classical algorithms of process diagnostics (Diagnostic system).

Regardless of the process failures, a number of additional failures related to the deliberate influence of external factors occurring during a cyberattack have been modelled, somewhat in parallel, in the simulator. For simulation purposes, a dedicated cyber faults vector has been defined for them. Maintaining independent modelling of process faults and ”cyber faults” allows for testing scenarios in which a cyber attack is simultaneously carried out and a process failure is present.

The separation of independent process and cyber fault inputs allows to plan very complex cyber attack scenarios. A specific cyber attack scenario will almost always consist of a specific sequence of one or more cyber faults, e.g. simultaneous modification of the control signal and the value of the process variable passed to the operator interface, so that the operator does not realize that some modifications are being made.

V. THEORETICAL ANALYSIS OF SOME SCENARIOS OF CYBER ATTACKS ON THE EXPERIMENTAL STAND

In this section, an analysis of three cases of cyber attacks on the test laboratory installation presented in Section 3 will be carried out, in terms of detection and the possibility of distinguishing a cyber attack from malfunction/fault of individual elements of the diagnosed object.

A. Description of cyber attacks

Assume that the experimental stand represents a system of buffer tanks with a toxic or flammable liquid (e.g. aviation fuel). The regulator (P or PI) stabilizes the level in tank 1. The cyberattack has been directed on the level control circuit in order to cause a failure, which will result in overfilling the tank and overflow of the medium, leading to environmental pollution or fire. We assume that, regardless of the diagnostic system, there is an alarm subsystem in the automation and process monitoring system that signals an alarm in the event of exceeding the permissible levels in the tanks: Hi-L1 and Hi-L2.

B. Description of the diagnostic system

The diagnostic system uses the knowledge of the four signals presented in Table 1. The list of possible failures is given in Table 2.

Models for fault detection were designed based on the set of available process variables. We assume that these models (neural/fuzzy) are representing the state without faults, determined on the basis of experimental data obtained from a wide range of signal variability. The set of models was developed in such a way as to obtain high discrimination of individual failures. For this purpose, it was also assumed that the assessment of residues would take into account their sign.The structures of the models for the generation of residues, the list of three-valued diagnostic signals and their sensitivity to residues are given in Table 3.

It is easy to check that the faults {f_1}, {f_2}, {f_3}, {f_6}, {f_7}, {f_8}, {f_9} are unconditionally distinguishable, the pair of faults {f_2, f_3} are unconditionally indistinguishable, and the pair of faults {f_4, f_5} are condition ally distinguishable [Kościelny et al. 2006; 2016].

TABLE 1. SET OF PROCESS VARIABLES

Description of variable	Symbol
Manipulated variable – signal of valve position V	CV_V
Measured variable – in-flow to tank T1	F_1
Measured variable – level of liquid in tank T1	L_1
Measured variable – level of liquid in tank T2	L_2

TABLE 2. SET OF FAULT CONDITIONS

f_k	Description of fault
f_1	Fault in measurement channel F_1
f_2	Fault in measurement channel L_1
f_3	Fault in measurement channel L_2
f_4	Fault in transmission of the manipulated variable CV_V
f_5	Fault of the pump P (change in pump flow)
f_6	Obstruction in the pipe between tanks T1 and T2
f_7	Obstruction in the pipe out of tank T2
f_8	A leak from tank T1
f_9	A leak from tank T2

In order to supervise the control circuit, a check is carried out using the qualitative model of the control loop in the form of rules:

a) If the controller operation is REVERSE and the control deviation is positive (PV> SP), the CV output signal decreases

b) If the controller operation is REVERSE and the control deviation is negative (PV <SP), the CV output signal increases

c) If (PV = SP), the CV output does not change.

These relationships are controlled in a sliding window. The detection of the non-compliance of the regulation system operation with the above rules leads to the hypothesis about possible damage f_2, f_4, f_5 or about a cyber attack.

The following two cyber attack scenarios are analysed below.

TABLE 3. SET OF RESIDUES.

R	S/F	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	V_j
$r_1 = F_1 - F_1^*(CV)$	s_1	+1 -1			+1 -1	-1					{0, +1, -1}
$r_2 = L_1 - L_1^*(F_1, L_2)$	s_2	+1 -1	+1 -1	+1 -1			+1		-1		{0, +1, -1}
$r_3 = L_2 - L_2^*(L_1)$	s_3		+1 -1	+1 -1			-1	+1		-1	{0, +1, -1}
$r_4 = L_1 - L_1^*(F_1)$	s_4	+1 -1	+1 -1				+1	+1	-1	-1	{0, +1, -1}
$r_5 = L_2 - L_2^*(F_1)$	s_5	+1 -1		+1 -1			-1	+1	-1	-1	{0, +1, -1}

Scenario 1. Falsifying the L_1 level value in the tank 1 by lowering its indication in order to obtain an increase in the level and ultimately overfilling the tank. The false PV value is entered both into the controller block $(PV = L_{1false})$, and also transferred to the visualization and other calculations.

Operation of the diagnostic system. The control loop test does not detect any fault/symptoms of attack. A false value of L_1 leads to the following values of diagnostic signals: $s_1 = 0$, $s_2 = -1$, $s_3 = +1$. Such values lead to a diagnosis DGN={f₂, f₃} indicating fault in the measurement channel L_1.

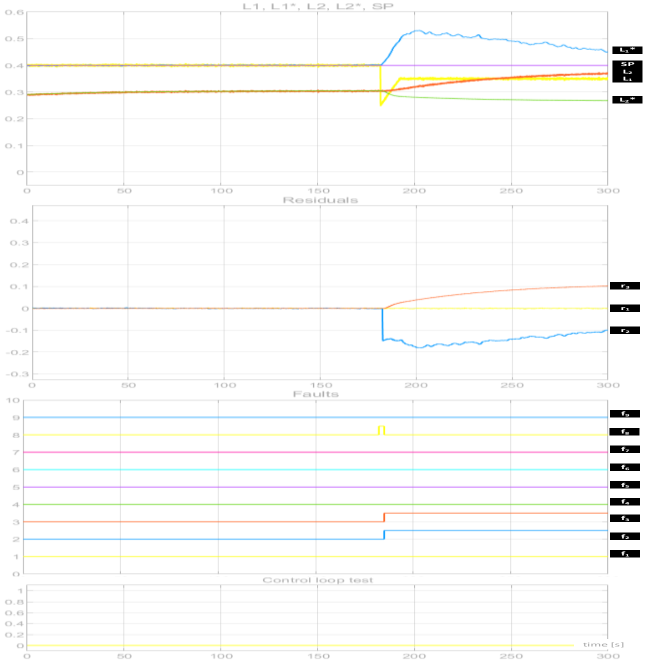

Fig. 6. Scenario 1 – process variables, residuals, classical diagnoses and control loop test result.

Conclusion: This cyber attack is indistinguishable from a fault to the measurement channel, because it consists in falsifying the value of this measurement.

Scenario 2. Falsifying the PV value in the control circuit by lowering the L_1 level in tank 1 so that PV is less than the set-point $(PV = L_{1false})$, in order to increase the level and ultimately overfill the tank. The false PV value is only forged in the controller block. Thus, the value of the L_1 variable is visualized correctly, and the true L_1 level measurement value is used in the calculation of the residuals and the control of the controller operation rules.

Operation of the diagnostic system. Because the attack causes reduction of PV seen by the controller, the controller responds by increasing the CV value (i.e. the flow-in). However, the diagnostic system uses the real value of PV, which is higher than the set point. Hence, the CV should decrease according to the qualitative model of the control loop (rule a – above) The control loop test detects the symptom, so a failure of f_2, f_4, f_5 or a cyberattack is possible. On the other hand, the diagnostic system, using the real value of the level in the residual calculations, does not detect any symptoms for residual r_3, therefore a no-fault diagnosis is generated.

Conclusion: By combining both pieces of information, we conclude that a cyber attack has occurred. Confirmation of the threat is signalled by the alarm system generating a Hi-L1 alarm when the limit is exceeded.

Based on the analysis of the above scenarios of cyber attacks, it can be concluded that the development of systems allowing to recognize not only faults, but also cyber attacks is a very difficult task. Such a system should make conclusions using the diagnostic system, results of control loop tests, detected alarms and redundant measurements from the SIS system.

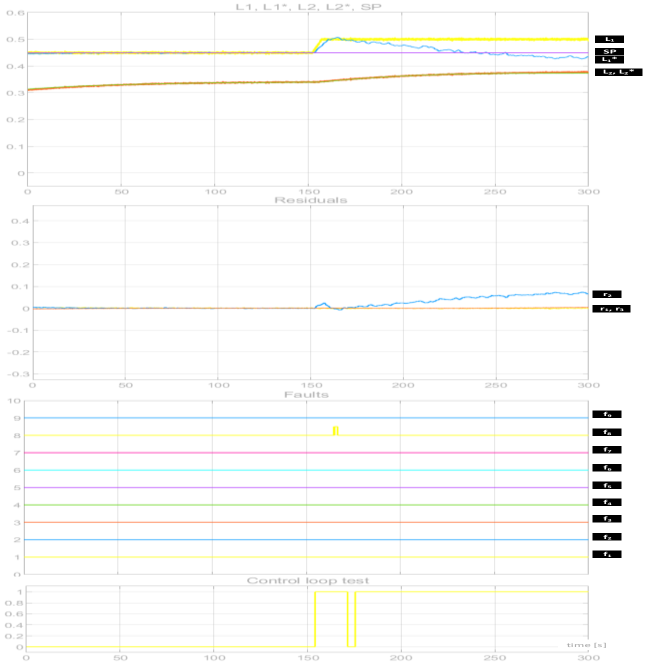

Fig. 7. Scenario 2 – process variables, residuals, classical diagnoses and control loop test result.

VI. Initial Results

This section shows the results of sample simulations conducted for the first two scenarios.

In scenario 1, shown in Fig. 6, the L_1 level reading of [m] was lowered by -0.15[m]. The upper waveform shows the lowered L_1 value, which the control system tries to bring to the set point SP = 0.45 [m]. After a while the tank T1 is overfilled at the level of 0.5 [m], the underestimated value remains at the level of 0.35 [m]. Below the reaction of the residues r_2 and r_3 is seen, according to the matrix presented in Table 3. The diagnostic system detects a few indistinguishable faults {f₂, f₃}, Control loop test does not detect any malfunction of the control system. Cyber attack is not detected.

In the scenario 2, shown in Fig. 7, a reduction of the L_1 level of -0.15 [m] was introduced only at the input to the controller. The upper plot shows that, as a result of the action of the controller, which tries to bring the reduced regulated value to the set value SP = 0.45 [m], the actual level value reaches its maximum value, i.e. the tank is overfilled. The reaction residuum r_2 is shown next. This residuum is responsive because the actual inflow value, F_1, does not agree with the level values L_1 and L_2 that were present in the training data collected during normal plant operation. It is also an example of a limited use of residuals based on models that are learned only using data from normal operation of the installation (without faults). According to the matrix in Table 3, the diagnostic system does not indicate any of the faults. However, the control loop test indicates the operation of the control system inconsistent with the situation observed by the operator. It is possible to indicate the possibility of a cyber attack.

VII. Conclusions

An experimental set-up and an associated simulation model have been presented, designed to test ability of detecting cyber-attacks with help of FDI system. Some initial test results – on simulation model have been presented. It can be concluded that the development of systems allowing to recognize not only faults, but also cyber attacks should make a link between the diagnostic system, results of control loop tests, detected alarms and redundant measurements from the SIS system.

REFERENCES

[1] Applegate, S. D. The dawn of Kinetic Cyber, 2013 5th International Conference on Cyber Conflict (CYCON), Tallinn, 2013, pp. 1-15.

[2] Baeten J.C.M., J. M. van de Morten-Fronczak, J. E. Rooda, Integration of Supervisory Control Synthesis into Model-based Systems Engineering. In G.M. Dimirovski (Editor), Complex Systems, Systems, Decision and Control 55. Springer Intl. Pub., Switzerland, pp. 38-58, 2016.

[3] Blanke M., M. Kinneart, J. Lonze, M. Staroswiecki, Diagnosis and Fault-tolerant Control. Springer, Berlin Heidelberg, 2002.

[4] Costa, B., Skrjanc, I., Blazic, S., Angelov, P., A Practical Implementation of SelfEvolving Cloud-Based Control of a Pilot Plant, 2013 IEEE International Conference on Cybernetics (CYBCO), 7-12 (2013).

[5] Dastbaz, M., Cochrane, P., Industry 4.0 and Engineering for a Sustainable Future, Springer International Publishing, Cham,

[6] EU:2020, Emerging Technologies in Electronic Components and Systems (ECS): Oportunities Ahead, EU Publications, 2020

[7] Frank P.M., Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy. Automatica, vol. 26, 3, 1990.

[8] Gheorghe A., A. Zolghadri, J. Cieslak, P. Goupil, R. Dayre, H. L. Berre, "Model-based approaches for fast robust fault detection in an aircraft control surface servo loop: From theory to flight tests." IEEE Control Systems Magazine, vol. 33, no. 3, pp. 20-30, 2013.

[9] Harris T.: Assessment of Control Loop Performance, The Canadian Journal of Chemical Engineering, Volume67, Issue5, 1989, Pages 856-861.

[10] Isserman R., Fault Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance. Springer, Berlin Heidelberg, 2005.

[11] Kamal, S. Z., Al Mubarak, S. M., Scodova, B. D., Naik, P., Flichy, P., & Coffin, G. (2016, September 6). IT and OT Convergence - Opportunities and Challenges. Society of Petroleum Engineers.

[12] Kościelny J.M., Bartyś M., Rzepiejewski P., Sá da Costa J. (2006). Actuator fault distinguishability study. Control Engineering Practice, 14, 645-652.

[13] Kościelny J.M., Rostek K, Syfert M., Sztyber A.: Fault isolability with different forms of faults-symptoms relation. International Journal of Applied Mathematics and Computer Science, 2016, Vol. 26, No. 4, 815-826.

[14] Kościelny J.M., Syfert M., Wnuk P.: The Idea of On-line Diagnostics as a Method of Cyberattack, in book: J.M. Kościelny et al. (eds.) Advanced Solutions in Diagnostics and Fault Tolerant Control, pp.449-457. Springer International Publishing AG 2018,

[15] Lee, R.M. M.J. Assante, T. Conway, German steel mill cyber attack, Ind. Control Syst. 30 (2014) 62.

[16] Lee, R.M., M.J. Assante, and T. Conway, Analysis of the Cyber Attack on the Ukrainian Power Grid, SANS Industrial Control Systems, 2016

[17] Li Q.-K., G. M. Dimirovski, J. Fu, J. Wang, "Switching strategy in tracking constant references for linear time-varying delay systems with actuator failures." International Journal of Control, vol. 92, is. 8, pp. 1870-1882,

[18] Możaryn J., Ordys A., Stec A., Bogusz K., Al-Jarrah O.Y. and Maple C. (2020) Design and Development of Industrial Cyber-Physical System Testbed. In: Bartoszewicz A., Kabziński J., Kacprzyk J. (eds) Advanced, Contemporary Control. Advances in Intelligent Systems and Computing, vol 1196. Springer, Cham.

[19] NSF:2016 https://www.nsf.gov/news/news_summ.jsp

[20] Saha P., Mukta C.B., Choudhury S., Performance Assessment of Control Loops International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064

[21] Sanchez H., Rotondo D., Escobet T., Puig V, Quevedo J: Frequency-based detection of replay attacks: application to a multiple tank system ?. IFAC-PapersOnLine, Volume 51, Issue 24, 2018, Pages 969-974

[22] Stenerson, J. and Deeg, D.: Siemens Step 7 (TIA Portal) Programming, a Practical Approach, CreateSpace IPP (2015).

[23] Sullivan J.E., D. Kamensky, How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid, The Electricity Journal, Volume 30, Issue 3, 2017, Pages 30-35,

[24] Van Long Do: Sequential Detection and Isolation of Cyber-physical Attacks on SCADA Systems, Thčse de doctorat de l'UNIVERSITE DE TECHNOLOGIE DE TROYES, 2015, 2015TROY0032.

[25] Wnuk P., Kościelny J.M., Syfert M., Ciepiela P. (2020). The Issue of Adaptation of Diagnostic System to Protect Industrial Control Systems Against Cyber Threads. In: Szewczyk R., Zieliński C., Kaliczyńska M. (eds) Automation 2019, Advances in Intelligent Systems and Computing, vol 920, pp 258-267. Springer, Cham.

[26] Xia, H., P. Majecki, A. Ordys, and M. Grimble, Performance assessment of MIMO systems based on I/O delay information, Journal of Process Control, Vol. 16, pp 373-383, 2006,