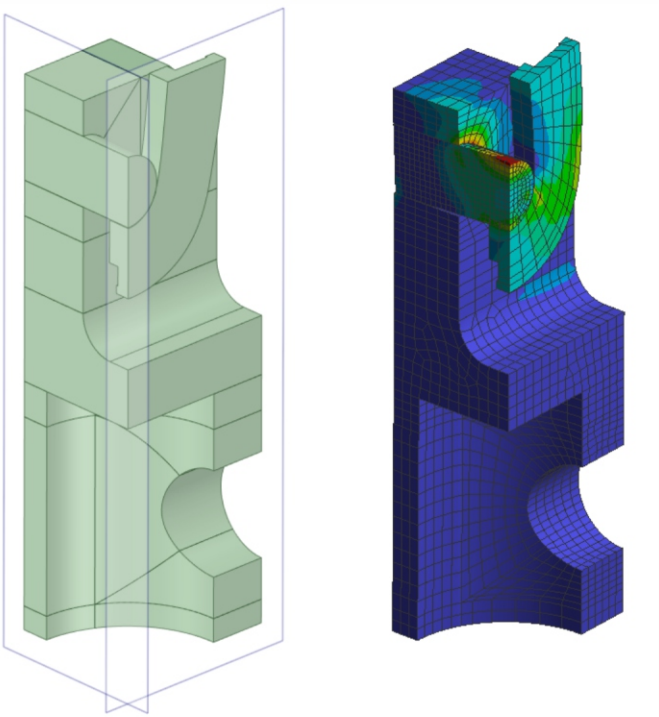
KATEDRA MECHANIKI
I INŻYNIERII OBLICZENIOWEJ
WYDZIAŁ MECHANICZNY TECHNOLOGICZNY POLITECHNIKA ŚLĄSKA

Studencka Konferencja Naukowa

METODY KOMPUTEROWE 2020



Gliwice 2020

Katedra Mechaniki i Inżynierii Obliczeniowej

Wydział Mechaniczny Technologiczny

Politechnika Śląska

Studencka Konferencja Naukowa

„METODY KOMPUTEROWE – 2020”

Gliwice, wrzesień 2020 r.

Katedra Mechaniki i Inżynierii Obliczeniowej
Wydział Mechaniczny Technologiczny
Politechnika Śląska
ul. Konarskiego 18A, 44-100 Gliwice
tel.: 32 237 12 04, fax: 32 237 12 82

Wydanie zeszytów naukowych zostało sfinansowane przez MESco Sp. z o. o. w Bytomiu.
Rysunek na okładce wykonała inż. Barbara Ciszyńska, Autorka artykułu na stronie 13.
ISBN 978-83-951185-1-7
Artykuły opublikowano na podstawie oryginałów dostarczonych przez Autorów.
Druk i oprawę wykonano w Wydawnictwie Politechniki Śląskiej.
Nakład 100 egz. Druk ukończono we wrześniu 2020 r.

Wstęp

Zeszyt naukowy zawiera 42 artykuły prezentowane na czternastej Studenckiej Konferencji Naukowej „Metody Komputerowe”, odbywającej się 24 września 2020 roku na Wydziale Mechanicznym Technologicznym Politechniki Śląskiej w Gliwicach. Konferencję zorganizowali studenci i pracownicy Katedry Mechaniki i Inżynierii Obliczeniowej Politechniki Śląskiej. Publikacje dotyczą zastosowania metod komputerowych w różnych dziedzinach techniki, takich jak:

- wspomaganie komputerowe prac inżynierskich,
- wytrzymałość materiałów,
- biomechanika,
- hydromechanika,
- termodynamika,
- robotyka,
- informatyka,
- optymalizacja,
- badania doświadczalne.

Dziękuję studentom za przygotowanie artykułów i prezentacji na konferencję, Komitetowi Naukowemu za troskę o poziom naukowy prac, Komitetowi Redakcyjnemu za przygotowanie zeszytu naukowego do druku i wersji elektronicznej materiałów konferencyjnych, a Komitetowi Organizacyjnemu za przygotowanie obrad konferencji.

Szczególne podziękowania za wsparcie finansowe organizacji konferencji składam przedstawicielom firmy MESco Sp. z o. o.

Duża liczba zgłoszonych artykułów świadczy o znacznej aktywności naukowej studentów i potrzebie organizacji tego rodzaju konferencji. Życzę studentom owocnych dyskusji w czasie konferencji. Mam nadzieję, że udział w niej będzie inspiracją do dalszych badań naukowych.

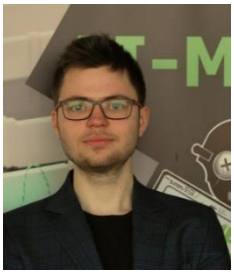
Opiekun Naukowy Studenckiego Koła Naukowego
„Metod Komputerowych”

Prof. dr hab. inż. Piotr Fedeliński

Gliwice, wrzesień 2020 r.

A CONCEPT OF ICS CYBERSECURITY BENCHMARK PROBLEM

WOJCIECH HAŃDEREK, Eng.
Automation and Robotics, semester III, graduate studies
MICHAŁ KOBIELSKI
Automation and Robotics, semester IV, undergraduate programme
PAWEŁ POLNIK
Automation and Robotics, semester VI, undergraduate programme
Supervisor: Piotr Przystałka, PhD, DSc, Eng., Prof. at SUT



Abstract. The main objective of the paper is to present hardware and software parts of the cybersecurity benchmark problem for industrial automation systems. A laboratory stand was elaborated to simulate cyber-attacks on industrial systems. The control system of the new stand was developed using all the possibilities of the Festo stand as well as SCADA system in the Siemens ET 200SP device. The application created using the Snap 7 library allows simulation of cyberattacks on industrial control systems.

KONCEPCJA PROBLEMU BENCHMARKOWEGO W ZAKRESIE CYBER BEZPIECZŃSTWA SYSTEMÓW ICS

Streszczenie. Głównym celem artykułu jest przedstawienie elementów sprzętowych i oprogramowania problemu testowego dotyczącego cyberbezpieczeństwa systemów automatyki. Opracowano stanowisko laboratoryjne do symulacji cyberataków na systemy przemysłowe. System sterowania nowego stanowiska został opracowany z wykorzystaniem wszystkich możliwości stanowiska Festo. Aplikacja utworzona przy użyciu biblioteki Snap 7 umożliwia symulację cyberataków na przemysłowe systemy sterowania.

1. Introduction

For the last few years, there were numerous incidents, outages, and other failures that have been detected and identified as the result of a cyberattack. These were mainly situations where fault was nearly impossible to detect. In March 2000 in Maroochy Shire Council, there were detected communication problems with wastewater pumping stations, alarms were not send to system, pumps did not work properly. As the result in the next three months, liters of effluent were released to local waterways. Attack was proceeded by Vitek Boden, who had taken control over 150 sewage pumping stations, using a personal computer and a radio transmitter. Finally, Mr. Boden was arrested, however after his operation, it was very difficult to restore initial state of waterways [1].

In 2008 in Baku-Tbilisi-Ceyhan, a cyberattack was initiated to control system pipeline with petroleum. Alarms were suppressed, and system operators were blind. In result, pipeline was ruptured and that caused an oil ignition and an explosion. Operator spokesperson denied that there was any tampering with computers or communication system. That shows danger of cyberattacks, which could be difficult to notice [2]. Apart from these attacks there are also experiments, that show how cyberattacks can be initiated, and how can we protect industrial control systems. In 2007, Aurora Project was started, which was an experiment by Idaho National Laboratories (INL). This project focused on behavior of controller during a cyberattack. The experiment, made by security researchers shown, the plant could be even destroyed. During this presentation breakers on a diesel generator were opened and closed out of synch, which caused an explosion. Aurora Project was reported in 2007 by CNN, showing the seriousness of security in ICS, mainly in power infrastructure [3]. There were also examples of very complex solutions of cyberattacks, like Stuxnet. Stuxnet is a worm which is a virus on Microsoft Windows system, searching in the local network connected Siemens ICS systems, like PLC controllers and HMI panels [4]. Before Stuxnet in 2008, there was another worm, which began to infecting U.S. military machines and carried into CENTCOM's classified network [5]. In 2012 in corporation Saudi Armco, a virus was implemented, which attacked control system [6]. In 2014, German article informed that an unnamed steel mill was attacked, and in result it was destroyed [7].

2. The laboratory stand and benchmark problem

The main goal of the article is to illustrate a concept of ICS cybersecurity benchmark problem corresponding to the project realized by a student research group called AI-METH. The project includes the design and implementation of a laboratory stand and software to simulate cyber-attacks on industrial control systems. It must be highlighted that the authors of this project do not attempt to find vulnerabilities in software and automation devices or neither do they attempt to find a way to compromise network protocol security. By cyber-attack simulation, we mean a case in which all security systems have already been cracked by a cybercriminal, as a result of which changes are made to the control system through the previously obtained access to the network and/or installed malware.

One of the fundamental elements of the benchmark problem is a laboratory stand made by Festo company for development control methods and process diagnostics. The stand is built of one pressure tank where a current pressure is controlled by a PID module, two tanks where medium levels are also controlled by a PID module, a solenoid valve, a pneumatic actuator responsible for openness level of the valve, a pump, a heater and a sensor system**.** All devices from SIEMENS were programmed in TIA Portal software - version 15.1. The whole laboratory stand used in this research is shown in Fig. 1.

Fig. 1. Laboratory station for cyberattack simulation
Rys. 1. Stanowisko do symulacji cyberataków na przemysłowe systemy sterowania

The next element of the laboratory station is WebSCADA visualization system. The authors use a new approach for visualization of industrial process. In contrast to basic SCADA system, the authors propose a real photo representation of the laboratory stand which can be applied to show all the changes in the process variables. In such approach it is very important to prepare a detailed graphics for WebSCADA visualization. We mainly use photo layers, on which we get an animation effect by applying layers. The structure of animation process is implemented in HTML 5, where semantic elements are necessary for correct visualization of the process. This part is implemented in CS3. The most important property is z-index, which allows us to set photo on a longitudinal axis Z. An element with greater stack order is always in front of an element with a lower stack order. Z-index property allows us to create three-dimensional animation effect in the case of two-dimensional photos. The main rules of the visualization system are included in PLC SIEMENS S7-300. Visualization data can be downloaded and transferred by the functions implemented in TypeScript with the use of webserver functionalities of the PLC. In this way it is possible to animate all changes of the process variables in real time, e.g. animation of the medium level in a tank, states of valves, values obtained from manometer sensors, temperature sensors, etc.

3. A case study

The proposed benchmark problem can be applied to collect data that represents the object acting in different states such as:

- F0 – faultless conditions;
- F1 – cyber-attack leading to the physical damage of the object. For example there can be a situation where a cybercriminal intends to physically damage the components of the installation responsible for cooling the nuclear power plant reactor to cause high material, environmental and human losses. The attack on the object can occur from anywhere in the world at any time. The cybercriminal would break all protections and would change the values of the parameters of PID controller implemented in the PLC responsible for controlling the pressure in the expansion tank. The result might be an unstable pressure control that could lead to the physical damage of one or more components of the installation which is necessary to supply the medium that was needed to cool the reactor. For example, the centrifugal pump might be damaged due to its overload or the tank being the pressure buffer in the system might be broken. As a result of the attack, the power plant might fail. And as a consequence, an ecological disaster covering significant territorial areas;
- F2 – cyber-attack leading to a change in the product formula. Imagine a situation where a cybercriminal intends to change the product formula to cause general anxiety in society. The cybercriminal breaks all firewalls and makes a slight change in the set point at some stage in the production of a popular medicament. A few processes in the pharmaceutical industry are very sensitive to even the smallest changes in parameters. Any deviations from the optimal values of technological parameters have a direct impact on the quality and quantity of the manufactured product. As a result of the attack the final product does not meet the formula requirements adopted by the process technologist. Changes are not detected in the quality control process and the medicament is placed on the market. After some time and in-depth research on the composition, a scandal breaks out because the medicament turns out to be ineffective;
- F3 – cyber-attack leading to dazzling operator. The last considered example of cyber-attack is action aimed at the so-called operator blinding. Blinding the operator involves making

changes in the control system and falsifying values in the process visualization system. Therefore, the personnel supervising the process (operator/ dispatcher/ technologist) observes the values of artificially generated process variables and has the impression that the process is running correctly. This action can lead to serious damage because the operator is not aware of what is really going on in the control process. As a rule, this type of attack occurs with other attacks and is designed to delay or prevent detection.

One of the examples of a cyber-attack is discussed below. A symptom of the one of designed cyberattacks simulated on the stand (F2) is the change in the set point value of the liquid level in the tank 102. In the SCADA system implemented on the ET 200SP the change is visible, the value 10 is displayed instead of 100, it is shown in Fig. 2. However, it is not possible for the operator to know the values of all process variables for a given documentation of the production process. To see a change in a parameter, the operator responsible for the process must check the documentation and compare all values of the process variables or ask a technologist for help. As a result of the simulated cyber-attack, the recipe is changed, and at a later stage the obtained product does not comply with the initial assumptions of the production process.

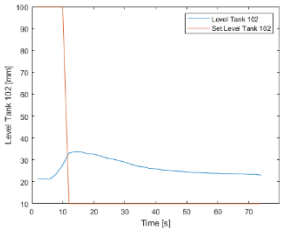


Fig. 2. Value of level in tank 102 – set and measured
Rys. 2. Wartość poziomu w zbiorniku 102 – zadana i mierzona

References

1. G. Hughes, The cyberspace invaders, The Age, June 22, 2003 paragraph 2 – 7 https://www.theage.com.au/national/the-cyberspace-invaders-20030622-gdvx44.html
2. Robert M. Lee, Michael J. Assante, Tim Conway, SENS ICS - ICS Defense Use Case (DUC) Dec 20, 2014, pages 1 – 2 https://ics.sans.org/media/Media-report-of-the-BTC-pipeline- Cyber-Attack.pdf
3. J. Meserve, CNN.com. Sources: Staged cyber-attack reveals vulnerability in power grid, http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack electricinfrastructure. September 26.2007 (cited: November 3.2010).
4. E. Chien, Symantec. Stuxnet: a breakthrough, http://www.symantec.com/connect/blogs/ stuxnet-breakthrough, November 2010 (cited: November 16.2010), Paragraph 1 - 5
5. Graham Messick CBS News, Cyber war: sabotaging the system, http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml, November 8, 2009 (cited: November 3.2010)
6. Nicole Perlroth - In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back, New York Times, Paragraph 1 – 3, https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html
7. Kim Zetter, A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever, January.08.2015 https://www.wired.com/2015/01/german-steel-mill-hackdestruction/