sciendo QPI 2019, volume 1, issue 1, pp. 371-377

SELECTED PROBLEMS OF INDUSTRY DATABASES AND INFORMATION INFRASTRUCTURE SECURITY

doi: https://doi.org/10.2478/9783110680591-050
Date of submission of the article to the Editor: 01/04/2019
Date of acceptance of the article by the Editor: 28/05/2019

Dariusz Karpisz[1] – *orcid id: 0000-0003-0848-6124*
Anna Kiełbus[1] – *orcid id: 0000-0001-9642-6142*
Maryna Zembytska[2]
[1]Cracow University of Technology, Faculty of Mechanical Engineering, Jana Pawla II 37, Cracow, **Poland**
[2]Khmelnytsky National University, Instytutska 11, 29016 Khmelnitsky, **Ukraine**

Abstract: The paper presents selected security problems in ICT systems and OT used in industry. In the Industry 4.0 era, the knowledge and competence of the IT staff and the maintenance staff must be linked. Selected problems and their analysis and solutions form the semi-secure network and use of NoSQL databases as a database bridges are presented in the article for various branches of industry.
Keywords: industry databases, information infrastructure, security, industry 4.0

1. INTRODUCTION

Computer system security is a standard subject taken when building new or rebuilding existing infrastructure in IT scope. In Industry 3.0 era, where the basis it was increasing production automation, industrial networks in the OT (Operational Technologies) were separated from the administrative LAN (Local Area Network). Necessary ERP, CRM, CAD/CAM and Team Work systems did not have access to critical production infrastructure (Teumim, 2010). This everything has changed in the Industry 4.0 era, where well-known IT solutions have become a novelty in OT.

The transfer of standards, infrastructure and solutions form IT also entails the transfer of known and unknown hazards. Hacking the server can result in lost or steal of data. Attacking devices on the production line can lead to material losses or situations that threaten human life. Stopping the production line by hacking event itself is a problem with the lowest weight in relation to, for example, an explosion caused by the loss of control over the cooling system.

The scope of Industry 4.0 has not been defined yet. Nor is it not defined range of IT technologies to penetrate the OT. The effects of breakdown or other effects of hacking in the living production plant are much more considerable, therefore it is necessary to become aware of the risks of new IT technologies. One of such problems is access to servers on the OT side. It is known that Industry 4.0 will be based on the collection and analysis of data from PLC (Programmable Logic Controllers), IoT devices (Internet of

Things), engine controllers and even individual sensors with many different network interfaces (Gilchrist, 2016). Huge amounts of data are collected already, but most of them are unprocessed now. This situation will change in the coming years. Today, Big Data slogan is known for technologies for processing large amounts of data in IT. All of them are based first of all on the source and the data bank - the NoSQL database system or the classic relational SQL system. The article discusses the problem of separating the Demilitarized Zone (DMZ) (Webb, 2014) sub-network for OT and for servers that can have a connection to the OT, mainly databases servers. The problems of security for industrial automation and control systems are described in IEC 62443 standard (IEC, 2019).

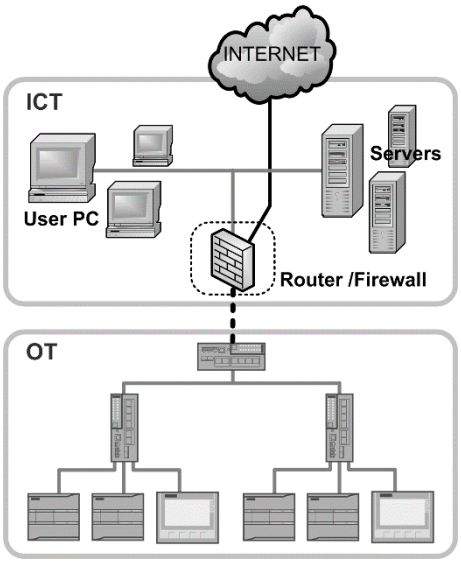

Fig. 1. Concept of standard factory network with separated ICT and OT zones

As a basis for further analysis, the most common network model for industry shown in Fig. 1 will be used. The production plant is divided, generally, into an administrative part with an internal LAN and a set of ICT (Information and Communication Technologies) systems, and a production part of the OT with an separated industrial network. The connection between both networks should be made at least through a firewall.

2. MATERIAL AND METHODS

The standard network division as shown in Figure 1 is insufficient in the Industry 4.0 era. A large data transfer from production lines to servers serviced on the IT side is expected. The connection of Internal LAN to the industrial network brings the risk of breaking the only one point of resistance and opening access to the whole OT infrastructure. It should be assumed that the most critical is connect: PLC controllers (as a data source) with the database server. Every potential hacking into the database server increase the risk of hacking into data sources. As shown in Fig. 2, it is also possible to transfer the database server directly to the OT area and completely separate the SCADA (Supervisory Control And Data Acquisition) production systems from the Internal LAN. This is not compatible with the Industry 4.0 concept.

Currently, it is recommended to isolate the DMZ zone for all elements that require special protection. Figure 2 shows DMZ1 for servers and DMZ2 for OT network parts. In the proposed structure of te network, the WAN router should be a separate hardware device from the firewall solution. It should be noted that there should be independent

IDS/IPS systems on the side of the Internal LAN, DMZ1 and DMZ2 networks blocking network traffic in case of threat detection. For the OT, disable network traffic at the output to other subnets should not be critical, because all OT devices (PLCs, drivers for engines, sensors) execute the programmed action and are usually only a source of data for supervisory systems, eg TPM or SCADA. As shown in fig. 2, the SCADA or TPM system can be located together with a database inside the OT in DMZ2, as one of the possible solutions.

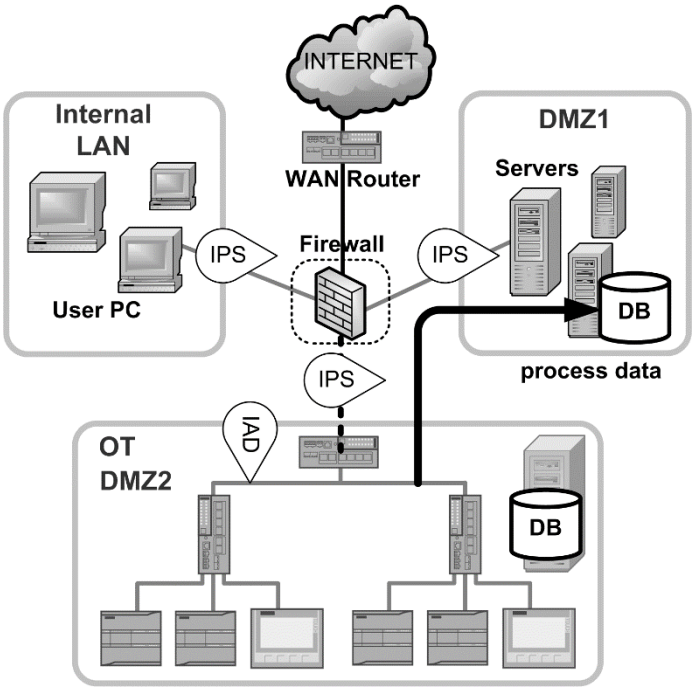

Fig. 2. Concept of factory network with separated secured DMZ zones

The concept of increasing safety by designing DMZ zones can be divided into 4 levels (Webb, 2014):

1. For Level 1 DMZ, all services requiring special security are collect to a separate zone that is accessed by a single firewall - one point of filtering network packages and security.
2. For Level 2 DMZ, a separate network segment or VLANs can be created for each service or set of identical services. Their solution provides one firewall, however, filtering and traffic rules are implemented for each DMZ separately.
3. Level 3 DMZ using multiple firewalls for each DMZ. This solution is most complicated by using Internal and External Firewall.
4. Level 4 DMZ is similar to Level 3, however it uses additional firewalls for connections between DMZs, as a double boundary design.

The next development of the concept of industrial networks protection is the partitioning of individual segments of the OT network into separately protected zones, as shown in Figure 3. This is compatible with Level 2/3 DMZ design concept (Webb, 2014).
In the OT ZONE 1 there is a database server and other services servers (SCADA). As a firewall, it uses the IPS protection system for the whole ZONE1. If is run an independent firewall on the database server that protects against dangers from inside the OT network, the level of security increases significantly (up to Level 3). Such double protection may be necessary when accessing a network of people from the

service team with their own programmer device or laptops. Service engineers may unknowingly distribute Malware or viruses over the network.
In the OT ZONE 2, an Open Controller (OC) PLC device was used instead of a standard server as is in ZONE 1. The OC controller is a combination of a classic PLC with an industrial computer under the control of the Linux or Windows operating system. The built in OC embedded-PC is completely independent of the PLC, therefore the failure, suspension or utilization of 100% of CPU performance does not affect to the PLC working. On embedded computer is possible to install database server with extremely fast access to data. This is not possible to classic connection via Ethernet network. Siemens Simatic ET 200SP Open Controller with preinstalled S7-1500 Software Controller was used as the basic solution. This solution allows to install on the embedded computer any software, such as database server, AI systems using neural networks or machine learning or compile dedicated software in selected programming language.

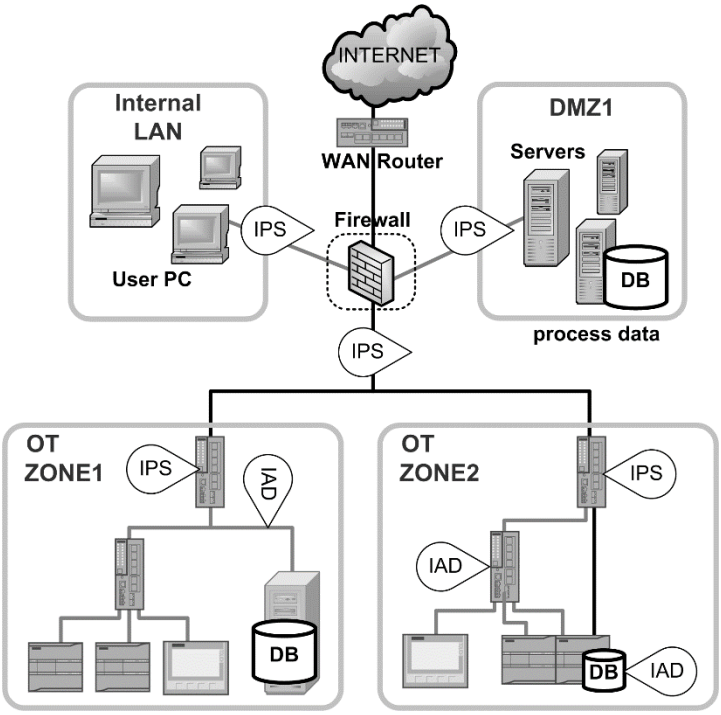

Fig. 3. Use of internal OT database (ZONE 1) or database implemented in Open Controller environment (ZONE 2)

Both ZONE1 and ZONE2 have additionally used IAD (Industrial Anomaly Detection) systems that can analyze devices and servers logs. This is an additional increase in the level of infrastructure and data security during its operation with the possibility of predicting failures.
To check the possibility of using data buffering on the OT side, a commuter connected to the Profinet network with the MongoDB database system was used. The concept of the test environment is shown in Fig. 4, where the number 1 indicates the standard data path with reading process data from the PLC and writing them to the database server in the DMZ1 zone for servers. The number 2 indicate reading data path with storing process data in NoSQL (MongoDB) data bank and next their transfer to the relational database (Oracle 12c). Process data are generated by the low-frequency analog signal generator plugged into the PLC controller input (Siemens S7-1200, CPU 1215C). Initial processing of the reading values is on the controller, and next by using the function to

share data with TCP/IP protocols it is sent to the program on the PC or server side. In both cases between the OT and DMZ1 zones, the network packets are analyses by the firewall and the IDS/IPS system (Snort).

3. RESULTS

As the database in DMZ1, new user schema in existing instance of database in Oracle 12c DBMS was used. On the database server under the control of the Linux operating system (CentOS), a firewall (iptables) and an IDS/IPS system (Snort) have been configured. As shown in Fig. 4, symbol "1" indicates the direct download of data from the PLC and their transfer to the database server in DMZ1. The PLC internal program uses the block TSEND_C to share data to external sources. An additional program prepared in C++ language was installed on the database server, which intercept data form PLC and forwarded to the database server.

Instead of the SQL server, in the ZONE 1 OT a computer was installed with NoSQL class MongoDB Community Server under the control of the Linux operating system (CentOS), a firewall (iptables) and an IDS/IPS system (Snort), as in DMZ1. In both cases, JSON (JavaScript Object Notation) was selected as the data storage format. In addition, the relational server saved data in relational tables in XML and standard data formats in specially designed databases (Karpisz, 2016; Karpisz, 2018). It should be noted that despite a significant difference in hardware performance, the buffer server in the OT provided twice as fast data access in direct user connect to DBMS. This is because MongoDB natively supports the JSON format and utilization of the server is low. Security mechanisms on the internal firewall and database server side have also been reduced what is not possible on the SQL server.

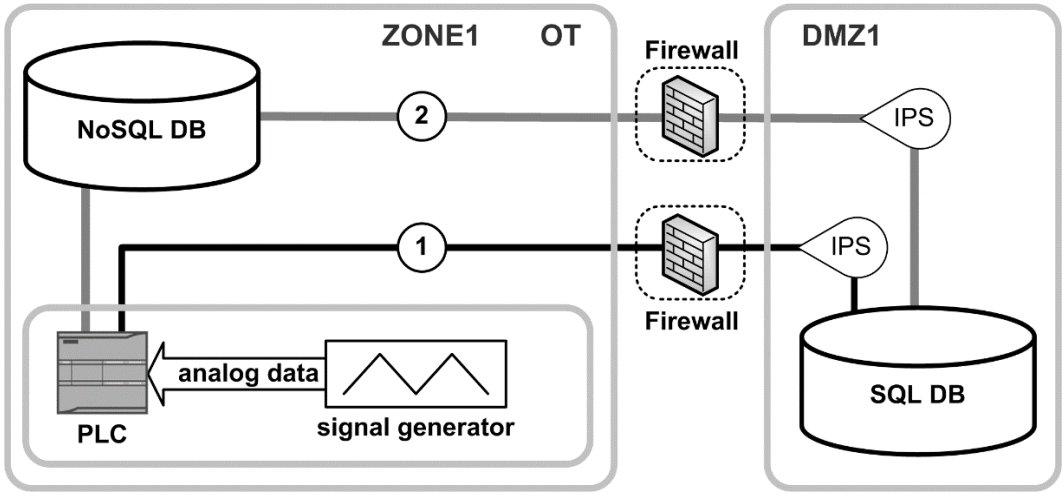

Fig. 4. Testing environment with NoSQL data store as a buffer for relational database

As shown in Fig. 4, symbol "2" indicates path to replicate data from NoSQL database to relational database in DMZ1. In this way, the application from the Internal LAN to read the data from the OT must go through the many firewalls and many IPS by which the hacking risk is significantly eliminated for the OT as Level 3 DMZ design.

4. CONCLUSIONS

The obtained results confirm the need to implement IT solutions on the OT side. This is especially important for the acquisition of data from fast-changing processes. The

classic RDBMS are too complex, and the individual elements of prevention and analysis systems in TCP/IP networks introduce delays in data storage. Therefore, the choice of simple NoSQL DBMS as data buffers seems to be right choice.

In the future there may be a problem with systems on the OT side that will implement the Industry 4.0/5.0 concept by using automation based on the analysis of data from devices from the same or other network segment. All hardware devices and software solutions such as IPS and IAD systems introduce delays and allow the possibility of interrupting data transmission which may stop the production process. It will also require to introduce RT/IRT high performance communication and also TSN (Time-Sensitive Networks) correlative with IPS, IAD protection systems. The Open Controller solution solves some of the problems by the ability to cache data in the same hardware platform where production control is realised, which is why they can be considered more forward-looking.

The authors plan further activities related to the use of the embedded PLC solutions like Open Controllers or PC based automation to integrate services on the OT side in order to share them for intelligent production systems.

Results presented in this paper may be interested to any researcher, because computer databases and computer networks exist in all laboratories. Securing results of industrial interest is particularly important, because they are exposed to espionage e.g. in machine building (Pietraszek et al., 2017; Pacana and Pacana, 2018; Ulewicz and Selejdak, 2018), heavy-duty machine production (Domagala et al., 2018a; Domagala et al., 2018b; Fabis-Domagala et al., 2018; Krawczyk et al., 2018), power plants (Dwornicka, 2014; Osocha, 2018), biotechnology (Skrzypczak-Pietraszek et al., 2018) and – last but not least – in materials science (Skulski et al., 2009; Gadek-Moszczak et al., 2015) being source of new materials (Strzelczak and Dudek, 2018) and related technologies (Pliszka et al., 2018; Radek et al., 2018). Constraints imposed by data security have to be considered in management of industry (Kozien, 2017) and academia (Kozien and Kozien, 2017a; Kozien and Kozien, 2017b).

REFERENCES

Domagala, M., Momeni, H., Domagala-Fabis, J., Filo, G., Krawczyk, M., 2018b. *Simulation of Cavitation Erosion in a Hydraulic Valve*. Materials Research Proceedings, 5, 1-6. DOI: 10.21741/9781945291814-1

Domagala, M., Momeni, H., Domagala-Fabis, J., Filo, G., Kwiatkowski, D., 2018b. *Simulation of Particle Erosion in a Hydraulic Valve*. Materials Research Proceedings, 5, 17-24. DOI: 10.21741/9781945291814-4

Dwornicka, R., 2014. *The Impact of the Power Plant Unit Start-Up Scheme on the Pollution Load*. Advanced Materials Research, 874, 63-69. DOI: 10.4028/www.scientific.net/AMR.874.63

Fabis-Domagala, J., Filo, G., Momeni, H., Domagala, M., 2018. *Instruments of identification of hydraulic components potential failures*. MATEC Web Conf., 183, art. 03008. DOI: 10.1051/matecconf/201818303008

Gadek-Moszczak, A., Pietraszek, J., Jasiewicz, B., Sikorska, S., Wojnar, L., 2015. *The bootstrap approach to the comparison of two methods applied to the evaluation of the growth index in the analysis of the digital x-ray image of a bone regenerate*. New Trends in Comput. Collective Intell., 572, 127-136. DOI: 10.1007/978-3-319-10774-5_12Comput. Collective Intell., 2015, vol. 572, pp.127-136.

Gilchrist, A., 2016. *Industry 4.0.* Apress, Berkeley, CA.

IEC 62443-4-2:2019, *Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components*, IEC.

Karpisz, D., 2016. *Design of manufacturing databases*, Technical Transactions, 113, 73-77. DOI: 10.4467/2353737XCT.16.123.5734

Karpisz, D., Kielbus, A., 2018. *Selected problems of designing modern industrial databases*. MATEC Web Conf., 183, art. 01017. DOI: 10.1051/matecconf/201818301017

Kozien, E., 2017. *Identification of stage phase growth in the checklist method using different statistical parameters*. 20th Int. Sci. Conf. Economic and Social Development, Prague, Varazdin, 538-545.

Kozien, E., Kozien, M.S., 2017a. *Academic governance as a determinant of efficient management of a university in Poland - legal and comparative perspective*. ESD 2017: Economic and Social Development Conf., Madrid, Varazdin, 38-47.

Kozien, E., Kozien, A., 2017b. *Commercialization of scientific research results and transfer knowledge and technologies to economy as determinants of development of universities and enterprises in Poland - legal and economic perspective*. 26th Int. Sci. Conf. Economic and Social Development, Zagreb, Varazdin, 326-335.

Krawczyk, J., Sobczyk, A., Stryczek, J., Walczak, P., 2018. *Tests of New Methods of Manufacturing Elements for Water Hydraulics*. Materials Research Proceedings, 5, 200-205. DOI: 10.21741/9781945291814-35

Osocha, P., 2018. *Calculation of Residual Life for P91 Material Based on Creep Rate and Time to Rupture*. Materials Research Proceedings, 5, 177-182. DOI: 10.21741/9781945291814-31

Pacana, J., Pacana, A., 2018. *Analysis of Possibilities of Using Polymeric Materials for Testing Prototypes of Harmonic Drive*. Materials Research Proceedings, 5, 61-66. DOI: 10.21741/9781945291814-11

Pietraszek, J., Szczotok, A., Radek, N., 2017. *The fixed-effects analysis of the relation between SDAS and carbides for the airfoil blade traces*. Arch. Metall. Mater., 62, 235-239. DOI: 10.1515/amm-2017-0035

Pliszka, I., Radek, N., Gadek-Moszczak, A., Fabian, P., Paraska, O., 2018. *Surface Improvement by WC-Cu Electro-Spark Coatings with Laser Modification*. Materials Research Proceedings, 5, 237-242. DOI: 10.21741/9781945291814-42

Radek, N., Pietraszek, J., Szczotok, A., 2018. *Microstructure and Tribological Properties of ESD Coatings after Laser Processing*. Materials Research Proceedings, 5, 206-209. DOI: DOI: 10.21741/9781945291814-36

Skrzypczak-Pietraszek, E., Reiss, K., Zmudzki, P., Pietraszek, J., 2018. *Enhanced accumulation of harpagide and 8-O-acetyl-harpagide in Melittis melissophyllum L. agitated shoot cultures analyzed by UPLC-MS/MS*. PLoS ONE 2018, 13, art. e0202556. DOI: 10.1371/journal.pone.020255610.1371/journal.pone.0202556

Skulski, R., Wawrzala, P., Korzekwa, J., Szymonik, M., 2009. *The electrical conductivity of PMN-PT ceramics*. Arch. Metall. Mater. 2009, 54, 935-941.

Strzelczak, K., Dudek, A., 2018. *Characteristics of Multimaterial Joints of Nickel-Based Superalloys*. Materials Research Proceedings, 5, 166-171. DOI: 10.21741/9781945291814-29

Teumim, D.J., 2010. *Industrial network security*. International Society of Automation.

Ulewicz, R., Selejdak, R., 2018. *Impact of Laser Machining on the Structure and Properties of Tool Steels*. Materials Research Proceeding, 5, 37-40. DOI: DOI: 10.21741/9781945291814-7

Webb, J., 2014. *Network Demilitarized Zone (DMZ)*. ICTN 6870.