ISSUES OF CYBERSECURITY OF THE PRODUCTION SYSTEM

KARLA MARADOVA[1], PETR BLECHA[1], RADIM BLECHA[1], JANA ROZEHNALOVA[1], VOJTECH FRKAL[2]

[1]Brno University of Technology, Faculty of Mechanical Engineering, Institute of Production Machnes, Systems and Robotics, Brno, CZ

[2]TOSHULIN As, Wolkerova 845, Hulin 76824, Czech Republic

DOI: 10.17973/MMSJ.2022_12_2022151

Petr.Blecha@vutbr.cz

Cybersecurity of production systems is a very topical issue in response to the dangers associated with the very high number of cyber-attacks in Europe. The current digital transformation of the industry associated with the digitalisation of manufacturing brings both the positives associated with increased flexibility and productivity of production, and the negatives associated with the risk of data loss, data alteration or blocking of control systems. Cybersecurity issues are also reflected in the revision of EU harmonisation legislation governing the requirements for placing products on the market or in service. It appears that the issue of cyber security needs to be addressed comprehensively across the entire infrastructure of a manufacturing plant. The present paper focuses on the relationship between machinery security and OT/IT security and presents the results of a study aimed at identifying potential sources of threats in an integrated manufacturing system.

KEYWORDS

Cyber security, threat, integrated production system, prevention, cyber-attack, infrastructure

1 INTRODUCTION

The current digital transformation of the European industry is associated with innovating management systems, increasing the degree of automation of production lines, developing new sophisticated production machines, improving the reliability and accuracy of measurement of the final product and intermediate products, introducing predictive maintenance, and using artificial intelligence. This process is characterised by the implementation of a multitude number of measuring, sensing and evaluation units providing large amounts of data that need to be stored and secured. Therefore, it is essential that the appropriate security network solution meets the requirements of information security management system (ISMS).

At the same time, it is also necessary to think practically and design the technical solution efficiently, considering the financial possibilities of each individual company. The evolving Industry 4.0 has connected the IT (information) and OT (operational) infrastructures of enterprises. This phenomenon highlights specific characteristics and reveals possible risks associated with cyber security. Therefore, it is necessary to focus on the right infrastructure design for each integrated production system and to focus on its OT/IT security [Blecha 2008] [Pacaiova 2021].

2 LITERATURE REVIEW

Nowadays, workplace security is very complex, for example, various standards can be used (ISA/IEC 62443, ISO/IEC 2700x, NIST, etc.). Upcoming EU harmonisation legislation known as the "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on machinery products" will oblige manufacturers to address cyber security [EUR-LEX 2021]. However, the above safety standards are only informative and generally mention what needs to have been done or what should specify, but they do not say how to do it. The relationship between machine security and cyber security is addressed in the 2018 first edition of ISO/TR 22100-4. This standard describes the difference in the perception of security in relation to human and IT security.

Smart manufacturing leads to dynamic, real-time optimised, self-organising value chains. Therefore, a suitable regulatory framework and standardised interfaces and harmonised company processes are required.

The description of the network infrastructure needs to be further extended for smart manufacturing to allow sufficient privacy, automatic configuration, and ease of use. Therefore, it is essential to implement a rapidly available, reliable, and secure communication network.

The standard addresses aspects of machinery security that may be affected by IT-security attacks related to direct or remote access to the machinery control system and tampering by persons for the purpose of deliberate misuse. IT security attacks are increasingly a potential threat to the security of machinery. Although deliberate abuse falls outside the scope of ISO 12100:2010 and the (safety-related) risk assessment process required by the Machinery Directive 2006/42/EC, it is advisable for machinery manufacturers to consider such threats now [EUR-LEX 2006].

Current technology allows you to monitor and/or improve machine performance remotely by adjusting parameters without having to be on-site at the machine. This capability brings significant benefits, as machines can be maintained in operation without downtime and the associated costs of inefficient service calls.

However, the same ability to modify the parameters of the machine to increase performance allows persons with dishonest or criminal intent to make modifications that may endanger the machine operator and possibly other workers in addition to the production itself. For example, it is possible to adjust speed or power to unsafe levels, or to erase or falsify error codes or messages.

The European Commission is also looking at cybersecurity and its impact on safety and has produced a "Proposal for a Directive on measures to achieve a high common level of cybersecurity in the Union (NIS 2), which aims to help increase cybersecurity not only in EU countries [EUR-LEX 2020].

The European Data Protection Supervisor (EDPS) published his Opinion on the Cybersecurity Strategy and the NIS 2 Directive on 11 March 2021, in which he makes, inter alia, specific recommendations to ensure that the proposal correctly and effectively complements existing Union data protection legislation, in particular the General Data Protection Regulation and the e-Privacy Directive. He also asks for clarification of the different use of the term’s 'cybersecurity' and 'network and information systems security' throughout the text: to use the term 'cybersecurity' in general and the term 'network and information systems security' only for technical purposes where the context allows.

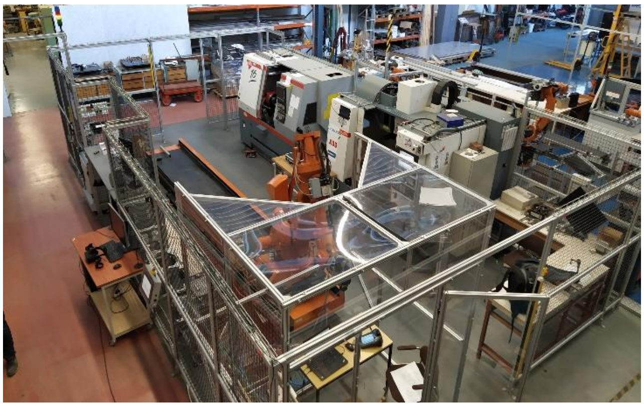


FIGURE 1. INTEGRATED PRODUCTION SYSTEM

A comprehensive methodology is not available today on how to appropriately implement cybersecurity for integrated manufacturing systems, although there are several sub-standards for automation, IT networks and, for example, the ISO 2700x series of standards for Information Technology - Security Techniques.

3 INTEGRATED PRODUCTION SYSTEM

3.1. The production system safety infrastructure

The experimental production system, on which we solved the problem in an area of cyber security, is composed of a Kovosvit MAS MCV 754 Quick machine controlled by a Siemens Sinumerik 840D, SPM6 and an ABB IRB 4400 robot with an IRC5 robotic controller. Firstly, it was necessary to determine which data (assets) needed to be protected for the safe control of this workstation, to identify the locations where communication with the machine takes place, to monitor all data flows to and from the machine, and to determine how to store and secure the data. The production system described is shown in Figure 1.

The relationship between machine safety and cyber security is further considered in the first edition of the 2018 ISO/TR 22100-4 standard [DIN 2020]. This standard describes the difference in the perception of security in relation to human and IT security, as we can see in Figure 2.

We need to identify relevant threats and then determine vulnerabilities, for example according to EN ISO/IEC 27005:2019 - Information technology - Security techniques - Risk management [ISO 2018].

We should understand that threats can be intentional, accidental, or environmental (natural) and result in damage or loss of an asset or service. The Internet network itself is not secure and we have to implement a multitude of security protocols and security features before connecting to it.

Types of damage can be:

- Physical damage – such as fire, water damage, destruction of equipment by accident;
- Information compromise – such as media or documents stolen, data from an untrusted source, manipulation of hardware or software, encryption of information by a virus;
- Technical failure – equipment failure or malfunction, information system overflow (e.g. Distributed Denial of Service (DDoS)), software malfunction;
- Unauthorised activities – data corruption or destruction, illegal data processing, unauthorised access to software and other devices;
- Human threats – we should focus special attention on these, unfortunately it is people who cause most of the threats for example hacker, cybercriminal, terrorist, industrial espionage (obtaining of competitive advantage) or dissatisfied ex-employee [ISO 2018].

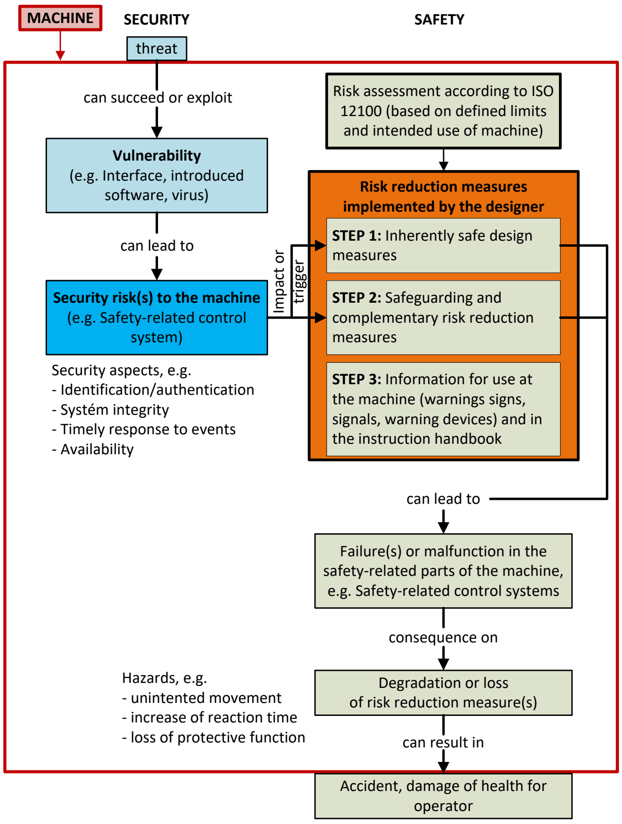

MACHINE
SECURITY
SAFETY
threat
can succeed or exploit
Vulnerability
(e.g. Interface, introduced software, virus)
can lead to
Security risk(s) to the machine
(e.g. Safety-related control system)
Security aspects, e.g.
- Identification/authentication
- Systém integrity
- Timely response to events
- Availability
Impact or trigger
Risk assessment according to ISO 12100 (based on defined limits and intended use of machine)
Risk reduction measures implemented by the designer
STEP 1: Inherently safe design measures
STEP 2: Safeguarding and complementary risk reduction measures
STEP 3: Information for use at the machine (warnings signs, signals, warning devices) and in the instruction handbook
can lead to
Failure(s) or malfunction in the safety-related parts of the machine, e.g. Safety-related control systems
consequence on
Hazards, e.g.
- unintented movement
- increase of reaction time
- loss of protective function
Degradation or loss of risk reduction measure(s)
can result in
Accident, damage of health for operator

FIGURE 2. RELATIONSIP BETWEEN SAFETY OF MACHINERY AND CYBERSECURITY (SOURCE: ISO/TR 22100-4:2018)

Vulnerabilities can be at the hardware, software, employees, organization, and especially enterprise network (OT/IT) level.

The area of network security is very extensive, and it is important to note that the appropriate communications infrastructure for the proposed production system should be designed first. A communication infrastructure is a set of technical means to ensure that individual communication systems and subsystems can communicate. Physically, this includes the cabling systems for the transmission of communications. This network is composed of cables, connectors, connection cables, switchboards, cable routes, but perhaps also premises for wireless networks.

All these elements together form a whole called a cabling system. Of course, the communication infrastructure also includes active elements (switches, routers, firewalls, etc.) that compose the so-called computer networks [Jordan 2013].

Another integral part is the design of the appropriate network typologies, the choice of software, and especially which network operating system we will use and the protocols that enable communication with each other. Computer networks are divided according to their ownership into public networks (Internet), private networks (home or corporate networks) and virtual private networks (VPNs). The VPN type should be preferred in companies, as computers are connected via a public network with secure access.

3.2. Analysis of cyber threats

Cyber-attacks are now focused on compromising corporate production activities and are directed by individuals or organised groups with different motivations. Cyber threats are mainly aimed at industrial control systems such as distributed control systems (DCS), programmable logic controllers (PLCs, PACs) and their networks, supervisory control, and data acquisition (SCADA) systems, human machine interface (HMI) systems and interfaces through various security gaps/holes based on poor architecture design, failure to take care of cyber security or simply obsolescence of components used in the system.

Types and description of cyber threats:

Malware – is malicious code (software) specifically designed to get into a computer without the knowledge of the owner of the device.

Computer worms – a program that can reproduce itself and spread, for example from one disk to another or via e-mail or other transmission mechanism.

Trojan a malicious part of software that is seemingly harmless. Users are usually tricked into downloading it via email.

Internet attacks – all techniques that involve redirecting a web browser to a malicious website through which malware can enter a computer.

Web (network) application attacks – introducing malicious code into unprotected servers and/or mobile applications.

Botnets – are one of the biggest internet threats today. They are a group of computers, also sometimes called zombies, under the control of so-called C&C (command and control) servers and our computer can turn into a zombie most often by getting infected with a virus. The most well-known botnet is the distribution of ransomware or spam. Botnets nowadays are not only created by individuals, but they are organized groups. They threaten all devices that have an Internet connection, which in Industry 4.0 data is transmitted over the IoT [Feily 2009].

Phishing – the most common threat, it involves sending out fraudulent emails that entices its recipient to visit a fake website or download an attachment that contains a virus. The goal is to get access to usernames, passwords, and codes to FOR EXAMPLE users' internet banking, companies etc. [Jansson 2013].

Control computer attack scenario

Computers can be attacked in many different methods. The most common type is by opening an attachment in an email, downloading freeware software, and distributing it via external memory (e.g., USB stick). Another method is exploiting a bug in a browser add-on (e.g., Adobe Flash). Another common method is when an internet mailbox convinces the user that they need an important update. If the device is compromised, a virus enters the system, which then attempts to smuggle the malware itself into the computer. The computer reports to the owner of the malware that it has been installed by someone and waits for instructions. The malware usually goes into a standby mode and tries not to attract unnecessary attention. Attacks are becoming increasingly sophisticated and are not only targeting manufacturing plants, but also the public sector such as banks, hospitals, government offices, ministries, etc.

Machines and devices can be infected with the virus, for example, from a usb flash drive when uploading a program or networking via the machine's LAN communication interface (in our case via a Sinumerick 840D sl PLC). Unfortunately, PLC devices do not normally have a firewall or antivirus software, so it is important to set up access points to the machine correctly.

In Figure 3 we can see the communication interface of the Sinumerick 840D sl (2x usb, 4x LAN).

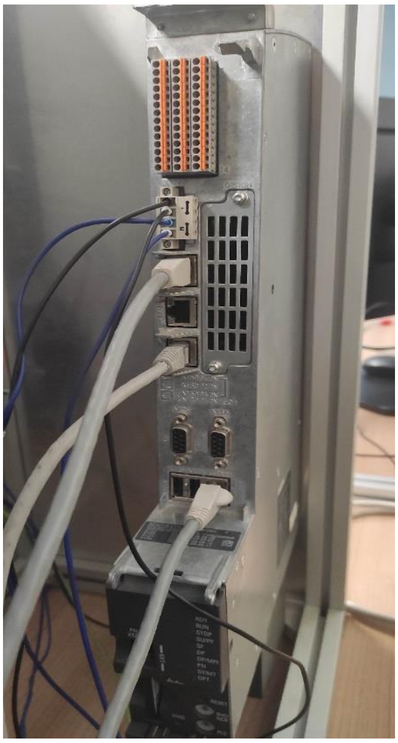


Figure 3. Sinumerick 840D sl (source own)

4 CASE STUDY

The aim of the experimental case study was to test the traffic on the research organization's network and the anomalies on the network caused, for example, by unwanted attacks from outside. A special Turris Omnia 2020 router was purchased from CZ.NIC, and we also received training from Phoenix Contact, a company that deals with automation and protective network elements for industry and lent us the MQuard RS4000 device, which is suitable for industrial use. The Turris Omnia 2020 router was configured at the same time as the HaaS honeypot application, which simulates an operating system and allows an attacker to log in via SSH or telnet and execute commands or download malware. Conventional routers do not have this technology, and the advantage for users is that commands are logged, and it can be used to analyse the behaviour of those seeking to penetrate corporate and end-user networks. In Figure 4 we can see the network elements we have used and in Figure 6 the network design using the security network elements.

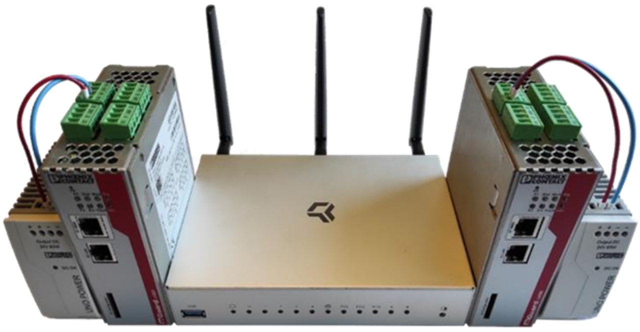
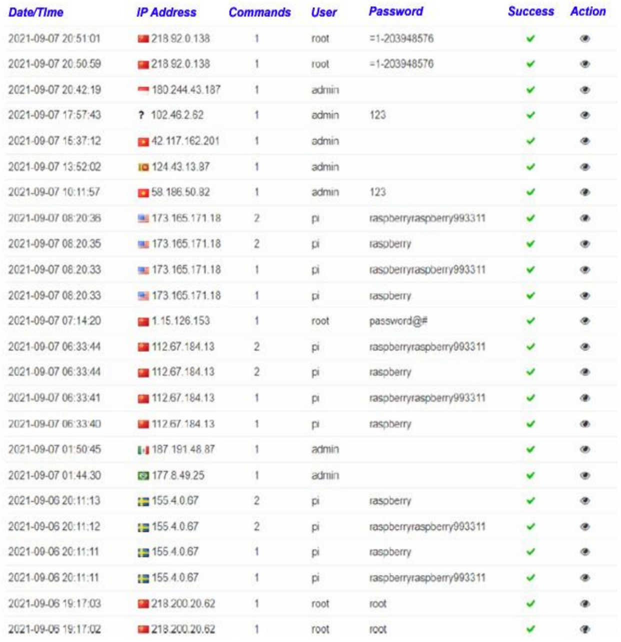


Figure 4. networking elements used in the study (in the middle Turris Omnia 2020, along edges 2 x MQuard RS4000)

During the 212 days of operation (16.6.2021 to 14.1.2022), 41203 SSH/telnet attacks from 93 countries of the world were intercepted and recorded on a public IP address. These attacks were subsequently processed and evaluated.

In the following Figure 5, IP addresses with the flag symbol of the country from where the attack was carried out, what password the attacker wanted to use, and many other details can be seen.



Date/Time	IP Address	Commands	User	Password	Success	Action
2021-09-07 20:51:01	218.92.0.138	1	root	=1-203948576	✓	👁
2021-09-07 20:50:59	218.92.0.138	1	root	=1-203948576	✓	👁
2021-09-07 20:42:19	180.244.43.187	1	admin		✓	👁
2021-09-07 17:57:43	? 102.46.2.62	1	admin	123	✓	👁
2021-09-07 15:37:12	42.117.162.201	1	admin		✓	👁
2021-09-07 13:52:02	124.43.13.87	1	admin		✓	👁
2021-09-07 10:11:57	58.186.50.82	1	admin	123	✓	👁
2021-09-07 08:20:36	173.165.171.18	2	pi	raspberryraspberry993311	✓	👁
2021-09-07 08:20:35	173.165.171.18	2	pi	raspberry	✓	👁
2021-09-07 08:20:33	173.165.171.18	1	pi	raspberryraspberry993311	✓	👁
2021-09-07 08:20:33	173.165.171.18	1	pi	raspberry	✓	👁
2021-09-07 07:14:20	1.15.126.153	1	root	password@#	✓	👁
2021-09-07 06:33:44	112.67.184.13	2	pi	raspberryraspberry993311	✓	👁
2021-09-07 06:33:44	112.67.184.13	2	pi	raspberry	✓	👁
2021-09-07 06:33:41	112.67.184.13	1	pi	raspberryraspberry993311	✓	👁
2021-09-07 06:33:40	112.67.184.13	1	pi	raspberry	✓	👁
2021-09-07 01:50:45	187.191.48.87	1	admin		✓	👁
2021-09-07 01:44:30	177.8.49.25	1	admin		✓	👁
2021-09-06 20:11:13	155.4.0.67	2	pi	raspberry	✓	👁
2021-09-06 20:11:12	155.4.0.67	2	pi	raspberryraspberry993311	✓	👁
2021-09-06 20:11:11	155.4.0.67	1	pi	raspberry	✓	👁
2021-09-06 20:11:11	155.4.0.67	1	pi	raspberryraspberry993311	✓	👁
2021-09-06 19:17:03	218.200.20.62	1	root	root	✓	👁
2021-09-06 19:17:02	218.200.20.62	1	root	root	✓	👁

FIGURE 5. RECORDING OF CAPTURED ATTACKS FROM HONEYPOT (OWN SOURCE)

The data from that period was converted into excel using a script created in Python and evaluated according to the frequency of attacks by the country from which the attack was directed Table 1 and according to the frequency of passwords Table 2, which attackers enter to penetrate the password of the network element (router Turris Omnia 2020).

Countries	Number of attacks	frequency in percentage
The United States of America	7081	17,19 %
China	5061	12,28 %
Germany	3320	8,06 %
France	2836	6,88 %
Sweden	2620	6,36 %
Poland	1961	4,76 %
Russia	1590	3,86 %
Earth failed to detect	1387	3,37 %
Ukraine	1323	3,21 %
Other countries	14024	34,03 %
Total	**41203**	**100 %**

TABLE 1. *THE FREQUENCY OVERVIEW OF THE MOST ATTACKS (OWN SOURCE)*

Username	number	frequency in percentage
root	22298	54,12 %
admin	5224	12,68 %
pi	2768	6,72 %
user	1581	3,84 %
ubuntu	880	2,14 %
debian	855	2,08 %
cirros	849	2,06 %
ubnt	673	1,63 %
test	452	1,10 %

TABLE 2. *THE FREQUENCY OVERVIEW OF THE MOST COMMON ATTACKS (OWN SOURCE)*

The management of network security is a fundamental value of any organisation. The router is a security component, as it separates our network (corporate network, research organization network, etc.) from the external Internet network and acts as a gateway for all connected devices to use the Internet. We used in the case study the Turris Omnia router. It can also serve as a monitoring device for preventive protection, as it allows us to monitor network traffic and record attempts to penetrate the security of a particular network. We have to realize that the router itself must also be configured securely. First, after the router is switched on, we need to set a new strong password for the device administrator. The basic admin/admin is commonly used by attackers. The password should not be simple or easy to guess, so the router we used has a 14-digit password. If the device has a Wi-Fi module, WPA2 security is also required with a strong enough password. Since WPA2 can be attacked by a dictionary attack (a technique in computer security and cryptanalysis that involves trying to guess the password by having the attacker try probable passwords from a prepared list), it is advisable to use a random sequence of at least 8 characters. Older security methods should not be used. Most endpoint devices are networked via switches and on LANs without the ability to be configured on individual VLANs. New routers and switches from various companies, for example Phoenix Contact, Cisco, Beckhoff, already have these configurable active elements in their portfolio, with the help of which it is possible to better segment the corporate network into individual subnets, which has an impact on the security of individual sections of the organization's infrastructure.

The design of a network with security active elements to enhance network security is illustrated in Figure 6.

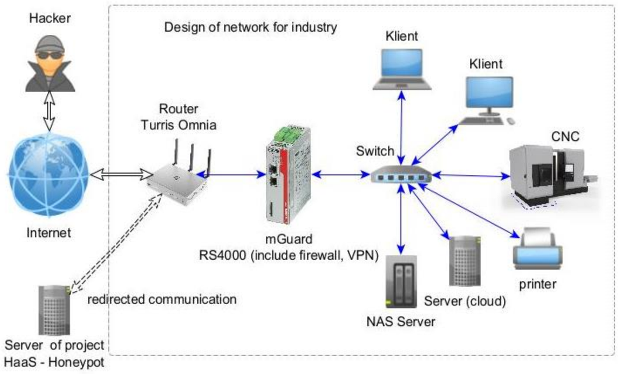


FIGURE 6. NETWORK DESIGN WITH SAFETY ACTIVE ELEMENTS (OWN SOURCE)

The experiment also showed the importance of implementing monitoring devices in the network design as a preventive measure [Zuzhen 2021]. In accordance with the international standard ISO/IEC 27039 Information technology - Security techniques - Selection, deployment, and operations of intrusion detection systems (IDPS), we chose the Honeypot tool. There are many other tools such as firewall, SIEM (Security information event management) and others [ISO 2015].

5 CONCLUSIONS

The aim of the presented paper and case study was to identify the threats that occur on the Internet and the need to reduce the associated risk through appropriate preventive measures. Considering the hundreds of attacks recorded in a single day, it seems necessary to monitor network traffic and design IT network infrastructure considering the identified and potential threats. Based on the results from the period, it can be seen, that the endpoints from which attacks are directed are in all countries. Although the study was conducted on a research organization's network, its application to industrial networks is possible. The recommendation is to assess all the risks of all the devices we connect to corporate networks. It is possible to reduce risks by proper network design, implementing network segmentation, controlling system accesses and multi-level security, for example, a combination of password and mobile authentication code. Given the rapid evolution of technology, both employees and professionals involved in both industrial automation and network security should be trained regularly.

Cooperation between management and all employees responsible for IT security is also very important. Finally, it is essential for manufacturing companies to cooperate with ISMS experts who can help with information security risk assessment and evaluation, not only because of the certification for information security management system according to ISO/IEC 27001:2014 [ISO 2014]. As can be seen in Figure 7 how a network could be segmented in an organization. This design is as an example. Segmenting the network into VLANs can help increase the security of the enterprise network, but it must be well configured, ports set up, communication tunnels by IT experts.

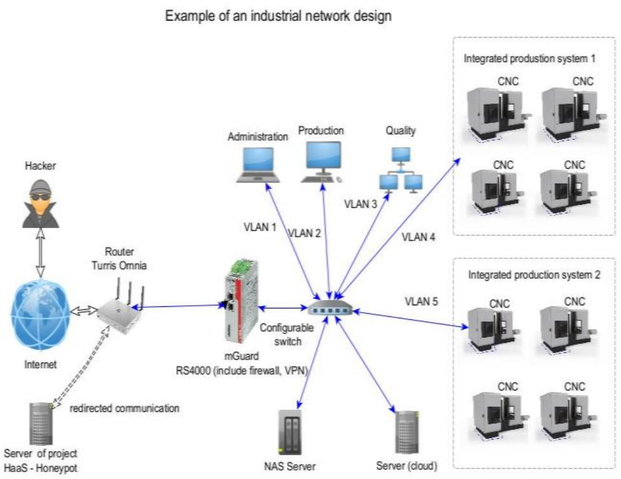


FIGURE 7. EXAMPLE OF AN INDUSTRIAL NETWORK DESIGN (OWN SOURCE)

ACKNOWLEDGMENTS

This paper has been supported by the project "Manufacturing engineering and precision engineering" funded as project No. CZ.02.1.01/0.0/0.0/16_026/0008404 by OP RDE (ERDF).

REFERENCES

Book:

[Jordan 2013] Jordan, V. and Ondrak, V. Infrastruktura komunikacnich system I. Brno: Akademicke nakladatelstvi Cerm, 2013. ISBN 0978-80-214-4839-1

Paper in a journal:

[Blecha 2008] Blecha, P., System methodology of risk assessment in machine tools. MM Science Journal, April 2008, Vol. 1, No. 1, pp 1-4, ISSN 1803-1269, DOI: https://doi.org./10.17973/MMSJ.2008_04_20080402

[Feily 2009] *M.* Feily, *A.* Shahrestani *and* S. Ramadass, *A* Survey of Botnet and Botnet Detection*,* 2009 Third International Conference on Emerging Security Information, Systems and Technologies*,* June 2009*,* pp. 268-273*,* ISBN 978-0-7695-03668-2 doi: 10.1109/SECURWARE.2009.48.

[Jansson 2013] Jansson, K. and Solms, R. Phishing for phishing awareness, Behaviour & Information Technology, 32:6, 584-593, DOI: 10.1080/0144929X.2011.632650

[Pacaiova 2021] Pacaiova H., et al. Methodology for Complex Efficiency Evaluation of Machinery Safety Measures in a Production Organization. Journal of Applied Sciences, January 2021, Vol. 11, No. 1, pp 453/1-453/16, ISSN 2076-3417, DOI: https://doi.org/10.3390/app11010453

[Zuzhen 2021] Zuzhen Ji, et al., Process Safety and Environmental Protection , April 2021, volume 148, pp 1279-1291, https://doi.org/10.1016/j.psep.2021.03.004

Technical reports or thesis:

[ISO 2010] ISO/IEC 12100:2010. Safety of machinery - General principles for design - Risk assessment and risk reduction,: ISO, Geneva, 2010.

[ISO 2013] ISO/IEC 27001:2013. Information technology - Security techniques – Information security management systems - Requirements,: ISO, Geneva, 2013.

[ISO 2015] ISO/IEC 27039:2015. Information technology - Security techniques – Selection, deployment and operations of intrusion detection systems (IDPS),: ISO, Geneva, 2018.

[ISO 2018] ISO/IEC 27005:2018. Information technology - Security techniques – Information security risk management,: ISO, Geneva, 2018.

[DIN 2020] DIN CEN ISO/TR 22100-4:2020. Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects (ISO/TR 22100-4:2018),: DIN, Berlin, 2018.

WWW page:

[EUR-LEX 2006] Directive 2006/42/EC of the European Parliament and the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast), OJ L 157, 9.6.2006, p. 24–86. Webpage created in 26/07/2019 [09.09.2020]. Available from <http://data.europa.eu/eli/dir/2006/42/oj>.

[EUR-LEX 2020] Directive of the European Parliament and of the Council of 16 December 2020 on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. Available from <https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF>

[EUR-LEX 2021] Proposal for a Regulation of the European Parliament and of the Council of 21 April 2021 on machinery products COM/2021/202 final. Available from <https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:52021PC0202>

CONTACTS:

Assoc. Prof. Ing. Petr Blecha, Ph.D.
Brno University of Technology
Faculty of Mechanical Engineering
Institute of Production Machines, Systems and Robotics
Technicka 2896/2, 616 69 Brno, Czech Republic e-mail:
Petr.Blecha@vutbr.cz, websites
https://www.vutbr.cz/en/people/petr-blecha-2489