*Paper*

# On Preventing and Detecting Cyber Attacks in Industrial Control System Networks

Adam Padée, Michał Wójcik, Arkadiusz Ćwiek, Konrad Klimaszewski, Przemysław Kopka,
Sylwester Kozioł, Krzysztof Kuźmicki, Rafał Możdżonek, Wojciech Wiślicki,
and Tomasz Włodarski

*National Centre for Nuclear Research, Otwock, Poland*

https://doi.org/10.26636/jtit.2019.131219

**Abstract—This paper outlines the problem of cybersecurity in OT (operations/operational technology) networks. It provides descriptions of the most common components of these systems, summarizes the threats and compares them with those present in the IT domain. A considerable section of the paper summarizes research conducted over the past decade, focusing on how common the problem is and in which countries it prevails. The article presents techniques most commonly used in the protection of these systems, with many examples from the nuclear industry given.**

***Keywords—attack preventing, cybersecurity, industrial control systems.***

## 1. Security of Industrial Control Systems

It is common belief that cybersecurity threats affect primarily typical IT systems, such as databases, web servers or corporate LANs, and that the main focus of cybercriminals is on confidential information stored in these systems. This image somewhat overshadows an equally important question of the security of Industrial Control Systems (ICS). The approach to the issue has begun to change recently, with the discovery of Stuxnet worm and with the subsequent publication of Blackout – a novel by Marc Elsberg. Cybersecurity of ICS has been gaining more and more public attention since that time. Despite such a recent growth in popularity, security issues related to ICS have a much longer history. It dates back to the year 1982, when CIA agents, in response to the large-scale efforts of the soviet National Security Committee (KGB) to bypass the embargo and steal Western technology, designed special software, installed it on programmable logic controllers through a chain of fictitious companies, and sold them to Russians. This has eventually led to a huge explosion of the Trans-Siberian gas pipeline, severely affecting the Soviet economy [1]. This historical example is interesting, because it shows that neither the Internet (which did not exist at that time in its current form), nor direct access to the facility being targeted are necessary to perform a successful attack.

Another interesting example is a local Polish case that is much more recent than the previous one, as it occurred in 2008 in Łódź. A fourteen-year-old boy modified an old TV remote and used it to arbitrarily change the settings of the city tram system switch points. Using this device, he caused several road accidents and tram collisions. As he testified later, he did it "just for fun", and he got the knowledge necessary to build the remote talking to old engineers at tram depots.

This example shows that no extensive resources are necessary to exploit an ICS, and that there are more ways to attack an ICS than just via a typical IT system or network [2]. This problem has been gaining in importance, as with advances in automation, more processes vital to the economy can be targeted by cybercriminals. It is also harder to protect them by physical isolation, because many of these systems require constant external control and updates from the outside.

Technically, there are two types of advanced, distributed ICSs: Supervisory Control And Data Acquisition (SCADA) and Distributed Control Systems (DCS). They share many common features, and the boundary between them is not sharp, but it is usually assumed that SCADA systems focus on data gathering, while their DCS counterparts – on

Table 1
ICS systems components

| Low level (field devices) | High level (central systems) |
|---|---|
| PLC – Programmable Logic Controller | HMI – Human-Machine Interface |
| RTU – Remote Terminal Unit | FEP – SCADA servers |
| IED – Intelligent Electronic Device | Front End Processors |
| | Historians (for storing logs, etc.) |

processes. This implies that DCSs are process state driven, and SCADAs are event driven. This makes DCSs harder to protect, because disturbing process continuity or integrity may lead to severe consequences. There are several components of these systems that have standard names which are abbreviated in the same way. The most popular of them are shown in Table 1.

SCADA and DCS systems may ultimately serve the same purpose, but while SCADA vendors concentrate on providing higher-level functions and human operator interaction, and assume that lower-level components can be provided by different vendors as long as they implement standard protocols, DCS solutions are generally sold as a whole, with low-level control elements included. DCS systems may use proprietary protocols for internal communication. They may be supplemented with some high-level application servers and SCADA components from other vendors, but the core of the system remains homogenous.

The ISO/IEC 27005 (Information Technology – Security Techniques – Information Security Risk Management) standard defines vulnerability as "a weakness of an asset or group of assets that can be exploited by one or more threats", where "assets" are defined as anything that has a non-zero value to the organization. This definition, contrary to more specific ones, e.g. those used by the Internet Engineering Task Force, is so general that it can be applied to ICS and IT systems alike. The main difference appears to be in the relative value of the assets (listed in Table 1). In IT systems, the threat hierarchy is described with the CIA acronym: confidentiality, integrity, availability. The order of the threats reflects their importance. Usually, the most severe consequences are associated with information leaks (which are, in most cases, irrecoverable), then with breaching the system's integrity (which can be restored using backups or through system reinstallation), and ultimately with rendering the system inaccessible, e.g. by means of a Distributed Denial of Service (DDoS) attack which often requires considerable resources and is effective only as long as the attack takes place. In ICS the threats are similar, but their hierarchy is reversed (AIC instead of CIA), because availability of the system has usually the biggest influence on safety, especially for DCS. The biggest risks are associated with rendering the system inoperable, because it means losing control over industrial processes and may lead to catastrophic consequences.

Unauthorized alteration of the system's state is the second item in the list. It may lead to severe implications as well, but if the system is still operational, more or less successful countermeasures may be immediately applied by the facility staff, thus minimizing the negative consequences. ICSs are also equipped with many independent safety devices and procedures, so it is hard for the attacker to turn them all off. This minimizes the impact of unauthorized alterations as long as the system remains operational as a whole. Information loss is by far the least important factor – information stored in ICSs comprises mainly monitoring data and logs. Someone may use this data to gather some knowledge about the system and launch a more successful attack in the future, but disclosure of this information does not pose any immediate risks to the process.

There is also a difference at the other end of the definition, concerning "weakness". In IT systems, especially in lower layers of the OSI model, we have just a few standardized and well described protocols, such as Ethernet, IP, TCP/UDP etc. In ICS, in turn, the situation is a bit more complicated, because many vendors of the components listed in Table 1 utilize their own, proprietary protocols which are not disclosed to the general public. This makes the security analysis of the system harder and means that many more unknown factors need to be dealt with. Another problem consists in inherent lack of security of some of the protocols used in ICSs, even those that are open standards with publicly available specifications. The very popular Modbus protocol may serve as a perfect example here. It originates from simple point-to-point serial connections, so it lacks any encryption and security mechanisms, but now is commonly used over Ethernet networks[1]. In this case, it is sufficient for the attacker to obtain physical access to any of the network components (cables, switches) to be able to control the entire system. There are also examples of ICS equipment where, although encryption is implemented, weak algorithms and/or self-signed certificates are used.

## 2. Statistics and Geographical Distribution of Potentially Insecure ICS

The reasons outlined in Section 1 create a strong belief that the best solution to ensure the security of ICS networks is to isolate them completely from the Internet and to maximally restrict access to them. This recipe is true and confirmed by a vast majority of ICS security specialists (cf. [4] as an example), but it is equally true that it often impairs the functionality and accessibility of specific solutions. ICSs seldom serve company clients directly via the Internet, so remote access to them may be very limited, but is often hard to eliminate completely due to such reasons as software upgrades, configuration changes and supervision over the system performed by engineering team members. For these reasons, the engineering side usually stands in opposition to security people. For the former of these two groups, restricting remote access to the system actually lowers the safety level of the industrial process, because it drastically increases their response time to any problems, especially outside normal working hours, and increases the amount of work needed to fix them. This is the reason why too strict a policy enforced by the security team may

[1] Since 2018, some security extensions to Modbus have been introduced, but most of the equipment present on the market does not support them yet [3].

Table 2
Number of indexed systems for each query, data taken from [8]

| Shodan query | Connections | Category | Note |
|---|---|---|---|
| Niagara+Web+Server | 2794 | HAN/BMS | Web server for EMS/BMS |
| TAC/Xenta | 1880 | BMS | Self certs for HTTPS |
| i.LON | 1342 | BMS | Primarily for energy |
| EnergyICT | 585 | RTU | Primarily energy |
| Powerlink | 257 | BMS/HAN | |
| /BroadWeb/ | 148 | HMI | Known vulnerabilities |
| EIG+Embedded+Web+Server | 104 | Embedded web server | |
| CIMPLICITY | 90 | HMI | Zero config web view |
| SoftPLC | 80 | PAC | Eastern Europe |
| HMS+AnyBus-S+WebServer | 40 | Embedded web server | |
| ioLogik | 36 | PLC | Small vendor |
| Allen-Bradley | 23 | PAC | |
| RTS+Scada | 15 | SCADA | Runs on FreeBSD |
| SIMATIC+NET | 13 | HMI | Affected by Stuxnet |
| Simatic+S7 | 13 | PLC | Affected by Stuxnet |
| Modbus+Bridge | 12 | Protocol bridge | IP to Modbus |
| ModbusGW | 11 | Protocol bridge | |
| Reliance+4+Control+Server | 10 | SCADA | |
| Simatic+HMI | 9 | HMI | Affected by Stuxnet |
| Cimetrics+Eplus+Web+Server | 6 | Embedded web server | |
| A850+Telemetry+Gateway | 3 | Telemetry | |
| ABB+Webmodule | 3 | Embedded web server | |
| CitectSCADA | 3 | PCS | |
| Modicon+M340+CPU | 3 | Protocol Bridge | |
| webSCADA-Modbus | 3 | HAN | |
| RTU560 | 2 | RTU | Web interface |
| WAGO | 2 | Telemetry | |
| eiPortal | 1 | Historian | |
| NovaTech+HTTPD | 1 | Embedded web server | Substation automation |
| **Total** | **7489** | | |

be in fact counterproductive, because then the engineering people may set up their own backdoors to the system, remaining outside any control or supervision of the security people.

These may take the form of unauthorized VPN tunnels, sometimes disguised in some other protocols to avoid detection and closure by the security team, or even worse, GSM modems connected directly to the industrial systems, completely bypassing all levels of security within the corporate network. This is not a purely theoretical threat, as poorly secured VPN tunnels were used as an attack vector in the recent successful attack on the Ukrainian power grid that took place on December 23, 2015 [5]. As far as GSM modems or other communication devices that completely expose the industrial system components via the Internet are concerned, they are, quite incredibly, much more common than one could expect.

Cryptographic tools, mainly encryption of web traffic, are nowadays rarely used in ICS (both DCS and SCADA), but are seriously considered as a future standard [6]. Management of cryptographic keys and optimization of resources are subjects of extensive discussions. In 2009, John Matherly created Shodan – search engine indexing services exposed to the Internet [7]. Two years later, E. P. Leverett, a student at Cambridge University, wrote a set of queries for Shodan that are based on signatures of the most popular ICS components. Although the list includes some popular BMS vendors as well, it is partly justified, because BMS often control factory premises and have access to deeper parts of ICS networks. A detailed description of the tests may be found in [8].

A look at the geographical distribution of these systems is interesting as well, because it is common belief that the problem of ICS security exists only in developed countries.

Table 2 shows that the problem exists all over the world, on all continents. Indeed, most of the indexed systems are located in developed countries with large numbers of industrial users, such as the United States of America, Sweden, the Netherlands or Canada. However, there are interesting exceptions, e.g. a relatively low number of connections in China, despite their big industry, rapid economic growth and large number of users. But this may be attributed rather to a relatively low number of IP numbers assigned to China, so the scale of the problem is probably the same as in other industrially developed countries, just hidden in private subnets used by Internet operators or in the IPv6 address space. Nevertheless, exposing ICS components even in a private network of a large Internet operator is only a little less dangerous than doing it openly on the Internet. It is of particular interest for the authors of this paper that a relatively high number of exposed systems exist in Poland, despite the fact that most operators have not been assigning, for a few years now, public IP addresses to their users by default. It is a feature that has to be paid for extra. This increases the probability that these exposures are intentional rather than accidental.

Table 3
Number of indexed systems per country, data taken from [6]

| Country | Count | Country | Count |
|---|---|---|---|
| United States | 3920 | Greece | 10 |
| Sweden | 442 | Israel | 10 |
| Netherlands | 370 | Luxembourg | 9 |
| Canada | 365 | South Africa | 9 |
| Finland | 301 | Philippines | 8 |
| Norway | 271 | Thailand | 7 |
| Denmark | 194 | Turkey | 7 |
| Poland | 191 | Mexico | 7 |
| United Kingdom | 122 | Malaysia | 6 |
| Portugal | 93 | Singapore | 5 |
| Germany | 92 | Panama | 4 |
| Czech Republic | 90 | Puerto Rico | 4 |
| Spain | 86 | Hong Kong | 3 |
| Australia | 81 | Serbia | 3 |
| Ireland | 76 | New Zealand | 3 |
| Taiwan | 66 | Argentina | 2 |
| Japan | 59 | Chile | 2 |
| Italy | 57 | Croatia | 2 |
| France | 53 | Iceland | 2 |
| Slovenia | 50 | Indonesia | 2 |
| Korea, Republic of | 41 | Dutch Antilles | 2 |
| Belgium | 39 | Albania | 1 |
| Russian Federation | 37 | Armenia | 1 |
| Switzerland | 34 | Bermuda | 1 |
| No country information available | 31 | Faroe Islands | 1 |
| China | 29 | Guernsey | 1 |
| Brazil | 27 | Iran, Islamic Republic of | 1 |
| Cyprus | 23 | Jersey | 1 |
| Estonia | 20 | Kazakhstan | 1 |
| Austria | 17 | Vietnam | 1 |
| Slovakia | 16 | Macedonia | 1 |
| Hungary | 14 | Namibia | 1 |
| India | 14 | Trinidad and Tobago | 1 |
| Romania | 13 | Latvia | 1 |
| Ukraine | 12 | Kuwait | 1 |
| Lithuania | 12 | Malta | 1 |
| Bulgaria | 10 | **Total** | 7489 |

The results published by Leverett stirred up a vivid discussion about cybersecurity in modern industry and inspired many other researchers to follow with similar tests. Especially interesting is work [9] by Roland C. Bodenheim, because he repeated exactly the same queries as Leverett two years later, in 2013. Although one may expect that the number will drop because of increasing awareness of the problem, the actual result is reverse. The total number of connections raised from 7489 in 2011 to 57409 in 2013. It is more than 7500% increase in just two years. Following huge media interest in the results of the searches, authors of Shodan limited the access to the search engine, so it is harder to find data from the next years, but extrapolating the growth from 2011–2013, there is no reason to believe that the trend is no longer present.

## 3. Protection of ICS Against the Attacks

Absolute safety against cybercrime is a goal that is impossible to attain. Even if we imagine we have perfectly designed system running bug-free code, there is always some space for human error. There are several ways to lower the probability of successful break-in and minimize the impact if such event occurs. They are in principle similar to those used in IT systems, but not all techniques used for IT can be applied also to ICS. For example, penetration or red team tests are generally avoided, as they may impair the industrial process and lead to irrecoverable damage. They may be tried in simulated environments mimicking parts of the real system, but this severely limits usefulness of these methods. Also whitebox tests are often hard to conduct, because, as stated in Section 1, many components utilize proprietary hardware architectures with closed-source software. Security of the system begins with proper design. It is especially important with ICS, where large parts of the system (e.g. aforementioned Modbus network) lack any security mechanisms at all.

There are many publications covering different aspects of ICS security, but it is hard to find a general and up-to-date guidebook thoroughly covering all the aspects, from technical designs, through staff employment to operational procedures. There is one special branch of the industry though, where such guidebooks exist and are constantly updated and improved. It is the nuclear energy industry. They are necessary because of potentially catastrophic consequences of a security breach there. The standards are created and maintained by the International Atomic Energy Agency (IAEA). Their quality is proven in practice, because up to now there were only several publicly known, successful cyber break-ins to nuclear facilities [10]. And the only one that really inflicted some damage to the industrial process was with Stuxnet worm in 2010 on Iranian military factories for uranium enrichment. These factories were outside IAEA control then and were using illegally acquired ICS components (because of embargo). Other attempts, like the one in 2014 in South Korea, did not affect anything besides office computers of the company staff, not reaching any of the critical systems. The reason for this is that there are strict design requirements, described in [11], and compliance with them is later checked at the licensing stage.

One of the most important general design rules, formulated in [11], is defense-in-depth – there have to be as many independent levels of protection as possible, and a single point of failure which exposes vital parts of the system disqualifies the design. Such a point of failure does not have to have the form of a physical entity. For example, it may be the same model of firewall used to separate different network levels. If a remotely exploitable vulnerability is found in its software, access to all network levels may be obtained. The defense-in-depth rule is well known in the IT security world, but is rarely strictly obeyed. In the nuclear sector, it is been applied to the construction of reactors almost since the beginning of their commercial use, so naturally it is also strictly required in the field of cybersecurity. Security checks of industrial facilities must deal with the problem outlined at the beginning of this chapter. Therefore, a strong emphasis is placed on security assessments considered to be the most effective way of preventing break-ins. There are many good general guides on how to perform a cybersecurity assessment of an ICS, so the process will not be described in detail here. [12] may be a good starting point. But in this aspect, the nuclear industry also has its own procedures that are worth mentioning. In the book [13], there is a detailed guide on how to perform a security assessment of the entire facility, including such aspects as physical access and human resource policies. Apart from the questions devoted directly to the protection of radioactive materials, this publication may serve as a good basis for performing cybersecurity assessments in any advanced industrial facility.

## 4. Software

Because of very limited access of ICS systems to the Internet, no automatic software updates may be performed. Moreover, such an approach is discouraged in the case of production systems. Availability and security of industrial processes come first, so if the software patch fixing some less important security issues contains a bug or a change in the functionality, the entire process is jeopardized. Therefore, complicated procedures regarding the installation of new software versions are usually in place at industrial facilities, including thorough tests performed in simulated environments, and possibly even with some quarantine periods. On the other hand, updates are necessary, especially when a severe security flaw or a functionality problem is detected. Propagation of information about the vulnerabilities and updates constitutes another problem. Unlike in IT systems, where information about vulnerabilities found in most of the popular operating systems and applications is available at a single location, e.g. NVD (National Vulnerability Database), it is much harder to identify such a service for ICS. Most big vendors publish their own security bulletins in different formats and with different access rules. There are several national CERTs aggregating such information and republishing it, but the range of covered vendors may vary. The most complete and verbose are the services maintained by the American ICS-CERT [14]. There is a certain problem with them though – preparation of such data takes time, so alerts and advisories are often published by ICS CERT with a delay of several days compared to the original publication by the vendor of the affected system. System administrators interested in getting the information immediately are still forced to check security bulletins of the vendors of all the components used in the system. This does not guarantee anything, though. Many PLCs are now built using standardized x86 or ARM architectures, so they often share many operating system components with IT systems. When analyzing publications in NVD and security bulletins of the ICS component vendors, it may be noticed that bug reports (and software patches) in the latter case may appear even a year after their initial publication in NVD. This means that very dangerous periods are experienced when unpatched ICS components can be attacked by relying on general purpose IT exploits. This constitutes another reason for keeping ICS networks as isolated from the Internet as possible.

The last aspect requiring consideration is personnel training. All the people in the organization should know and understand the security policy, including engineering team and even office staff which has nothing to do with plant operations. Recent successful break-in examples, like the one in Ukraine [5], show that the first stage of the attack usually consists in spear phishing targeted at several people within the organization. Getting inside the internal network, even via office computers, gives the attacker numerous opportunities to spread the infection further. This is where the defense-in-depth paradigm shows its usefulness, because the aforementioned attack in Korea in 2014 ended within the office network – the attackers were not able to breach deeper levels of security. The results gathered by Leverett, Bondenheim and others, as cited in Section 2, show indirectly the danger of too tight security policies. Even if the policy is known by the engineering team, when it feels it hinders their work, they will look for a way to go around it. This may result in fully exposed systems using unauthorized modems, etc. That is why it is equally important to ensure that the technical people responsible for plant operations have real influence on security policies. This cannot work one way, because an enforced policy written without taking into account any feedback will be generally contested.

## 5. Detection of Successful Attacks

Advanced persistent threat (APT) attacks are extremely hard to prevent and detect, as they use some sophisticated social engineering techniques often paired with 0-day vulnerabilities and structural weaknesses of the organization. Traditional means of detection, like antivirus software, are not sufficient to stop this kind of attackers. That is why specialized Security Operations Centers (SOCs) have been becoming ever more popular recently. The idea of SOC is to proactively analyze network traffic and logs in order to detect any suspicious behaviors.

A detailed setup falls outside of the scope of this article, but there are many commercial products helping in performing task, or even companies that may provide a complete SOC as an outsourced service. It is worth mentioning though that it is possible to set up a functional SOC using open source tools, such as Elasticsearch + Logstash + Kibana (ELK), Bro network monitor, topped off by the Malware Information Sharing Platform (MISP). Especially the last of these tools is very useful, because it is constantly fed with information by a very large community of users, so indicators of compromise (IOCs) are quickly recognized. Such a setup is being successfully used at the European Organization for Nuclear Research (CERN) and other institutes federated in the Worldwide LHC Computing Grid (WLCG), including the National Centre for Nuclear Research in Poland [15].

Detection of backdoors using modems and other means of independent, unauthorized communication outside of the facility is another topic that is not necessarily covered even by a well setup SOC. The risk of installation of such devices can be minimized with proper policies (e.g. forbidding bringing any USB devices or mobile phones into the critical areas of the facility). It cannot be eliminated entirely though, without very expensive and troublesome means of security. Monitoring of Shodan results in search for company's specific equipment by the security team is not an effective means of protection. Shodan indexes new systems in approx. 19 days [9], and, as stated earlier, does not cover private networks of Internet operators. It is also not easy to use Shodan for malicious purposes, because of strict limits on the number of results in the free, anonymous version. For this reason, cybercriminals use their own botnets to do the same work, and their indexing schemes may be different. The use of radio-frequency (RF) shielding or signal jammers may be an effective way of ensuring protection of critical assets, but effective shielding is very expensive and jammers are usually forbidden by law. It is possible, though, to monitor RF signals in the area and even identify active client stations, in a search for unauthorized ones. The required hardware is expensive and difficult to come by, but good results can be achieved even with software defined radio. Example of such an application may be found [16].

## 6. Conclusions

This article presents the scale of the problem of insecure ICS systems. The data summarized in the paper and available in cited publications shows an alarming trend in the security of ICS/OT networks. Strong evidence exists that the number of ICS installations without proper isolation of components from the Internet is growing, despite the increasing level of awareness of the problem among ICS vendors and despite constant presence of this topic in the media. This can be partially attributed to the threat hierarchy outlined in the introduction to this article. When availability of the process is treated as the most important asset, cybersecurity issues are often overlooked, because their direct impact on availability is delayed in time.

The paper outlines several good practices on how to improve cybersecurity of ICS/OT networks, with references to more detailed sources of information, e.g. the process of establishing a simple SOC using open source tools to facilitate the detection of attacks. It also mentions the problem of locating unauthorized RF devices and ways to detect them. The article shows how standards set for the nuclear industry may be used to protect critical assets in other domains where ICS are used, with references to detailed guidelines included. These simple countermeasures may increase the security of the systems at a relatively low implementation cost. More in-depth methods, such as introduction of cryptographic measures to ICS (e.g. with new versions of the Modbus protocol [3]) are deliberately skipped in this paper because they often require serious changes of the architecture of the system and its components.

## Acknowledgments

Work done as part of the CYBERSECIDENT/369195/I/NCBR/2017 project supported by the National Centre of Research and Development in the frame of CyberSecIdent Programme.

## References

[1] T. C. Reed, *At the Abyss: An Insider's History of the Cold War*. Presidio Press, 2004 (ISBN 0891418210).

[2] T. Jablonski and M. Jach, "Jak 14-latek spowodowal katastrofę", 2008 [Online]. Available: http://lodz.naszemiasto.pl/archiwum/jak-14-latek-spowodowal-katastrofe,1602388,art,t,id,tm.html [in Polish]

[3] "MODBUS/TCP Security Protocol Specification" [Online]. Available: http://modbus.org/docs/MB-TCP-Security-v21_2018-07-24.pdf

[4] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to industrial control systems (ICS) security", NIST Special Publication 800-82 Revision 2, 2015 (doi: 10.6028/NIST.SP.800-82r2).

[5] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid", E-ISAC publication, March 18, 2016 [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[6] D. Fauri *et al.*, "Encryption in ICS networks: A blessing or a curse?", in *Proc. IEEE Int. Conf. on Smart Grid Commun. SmartGridComm 2017*, Dresden, Germany, 2017 (doi: 10.1109/SmartGridComm.2017.8340732).

[7] Shodan search engine home page [Online]. Available: https://www.shodan.io/

[8] E. P. Leverett, "Quantitatively assessing and visualising industrial system attack surfaces", Master Thesis, University of Cambridge, 2011 [Online]. Available: https://www.cl.cam.ac.uk/∼fms27/papers/2011-Leverett-industrial.pdf

[9] R. C. Bodenheim, "Impact of the Shodan computer search engine on Internet-facing industrial control system devices", Master Thesis, Air Force Institute of Technology, Ohio, USA, 2014 [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a601219.pdf

[10] P. Hitchin, "Cyber attacks on the nuclear industry", Nuclear Engineering International, 15 September 2015 [Online]. Available: https://www.neimagazine.com/features/featurecyber-attacks-on-the-nuclear-industry-4671329/

[11] "Computer Security at Nuclear Facilities", IAEA Nuclear Security Series No. 17 [Online]. Available: https://www-pub.iaea.org/mtcd/publications/pdf/pub1527_web.pdf

[12] "Cyber security assessments of industrial control systems. A good practice guide", Centre for the Protection Of National Infrastructure, U.S. Department of Homeland Security, Apr. 2011 [Online]. Available: https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/CPNI-Guia-SCI.pdf

[13] *Conducting Computer Security Assessments at Nuclear Facilities*, IAEA, Vienna 2016 (ISBN: 978-92-0-104616-1).

[14] ICS-CERT Alerts home page [Online]. Available: https://ics-cert.us-cert.gov/alerts?page=1

[15] D. Crooks *et al.*, "Operational security, threat intelligence & distributed computing: the WLCG Security Operations Center Working Group", in *Proc. of 23rd Int. Conf. on Comput. in High Energy and Nuclear Phys. CHEP 2018*, Sofia, Bulgaria, 2018.

[16] R. Feroze, "Passive GSM sniffing with Software Defined Radio", 02/06/2017 [Online]. Available: https://payatu.com/passive-gsm-sniffing-software-defined-radio/

**Adam Padée** received his M.Sc. in 2003 and his Ph.D. degree in 2013, both from the Faculty of Electronics and Information Technology of the Warsaw University of Technology, Poland. He participated in many European and national projects focused on supercomputing and distributed computing. Since 2009 he has been working for the National Centre for Nuclear Research (NCNR). He was one of the founders of Świerk Computing Centre. Currently he is the Head of Division of Computing Technologies and Deputy Director of Department of Complex Systems at NCNR. His scientific interests are focused mainly on high performance computing and infrastructure, evolutionary computation, IT and OT security.

E-mail: adam.padee@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

**Michał Wójcik** received his B.Sc. and M.Sc. degrees in Computer Science from Warsaw School of Information Technology, Poland in 2013 and 2018, respectively. His main areas of interest are computer networks and, in particular, network security, as well as information security management systems according to ISO 27001.

E-mail: michal.wojcik@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

**Arkadiusz Ćwiek** graduated from the University of Warsaw, M.Sc. in Physics, in 2011, in Biophysics and Didactics in mathematics and physics. From 2012 to 2018 leader of IT in the "Pi of the Sky" robotic telescopes project in which he worked with the best Polish research institutions, i.e. the National Centre for Nuclear Research, the Faculty of Physics of the University of Warsaw and the Centre for Theoretical Physics of the PAS. Responsible for development and maintenance of the telescope data acquisition and control systems, several facility instruments, and a suite of tools used for the preparation, planning and execution of observations. He was also responsible for research, design, specification and implementation of solutions. He also managed computer systems of the project spanning located on 2 continents. He also supported Creotech Instruments in some projects correlated with outer space observation. Since 2018 he works at Świerk Computing Centre. Currently he developing solutions using neural networks applied to computer network security and computer vision.

E-mail: arkadiusz.cwiek@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

**Konrad Klimaszewski** received his M.Sc. in Physics from the Warsaw University of Technology, Poland, and the Ph.D. degree in Physics from the Soltan Institute for Nuclear Studies, Poland, in 2004 and 2010, respectively. From 2015 he has been the Head of Information Technology Services

Laboratory at the National Centre for Nuclear Research, Poland. His scientific interests are focused mainly on high energy particle physics and nuclear medicine as well as high performance computing, could computing security and machine learning.
https://orcid.org/0000-0003-0741-5922
E-mail: konrad.klimaszewski@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

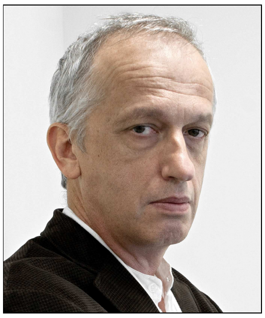
**Przemysław Kopka** is a last-year student at the Warsaw University of Technology at the Faculty of Physics. He has been with the National Centre for Nuclear Research as Python developer since 2018. He holds an B.Sc. in Mathematics and Physics from Warsaw University. His research areas focus on data processing and image reconstruction.
E-mail: przemyslaw.kopka@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

**Sylwester Kozioł** received his M.Sc. degree in Automation and Electrical Metrology, with distinction, from the Warsaw University of Technology, Poland, in 1979. Currently, he is a Major Technical Infrastructure Specialist at National Centre for Nuclear Research Świerk, Poland.

E-mail: sylwester.koziol@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

**Krzysztof Kuźmicki** received engineer's education at Warsaw School of Computer Science with an excellent degree in the major Managing Information Resources. Currently, he is a Technical Infrastructure Specialist at National Centre for Nuclear Research Świerk, Poland.
E-mail: krzysztof.kuzmicki@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

**Rafał Możdżonek** received his B.Sc. in Computational Physics and M.Sc. in Nuclear Physics from Warsaw University of Technology in 2011 and 2013, respectively. Currently he is a senior programmer at Laboratory for Information Technologies, Department of Complex Systems, National Centre for Nuclear Research. His main fields of interest include programming, numerical methods and data analysis.
E-mail: rafal.mozdzonek@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland



**Wojciech Wiślicki** graduated from Department of Physics of the University of Warsaw in 1982, received Ph.D. in Physics from A. Soltan Institute for Nuclear Studies in 1986, since 2007 and is a Professor Ordinarius at National Centre for Nuclear Research in Warsaw, Poland. Currently he is a Director of Department of Complex Systems and Computing Centre at this institute, also leads scientific groups participating in LHCb experiment at Large Hadron Collider at European Centre for Nuclear Research and KLOE at Frascati National Laboratory. His areas of scientific activity cover experimental high-energy physics and high-performance computing. He is an author of about 600 papers in various areas of physics and scientific computing, member of many committees, editorial boards and scientific bodies.
https://orcid.org/0000-0001-5765-6308
E-mail: wojciech.wislicki@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland

**Tomasz Włodarski** received his M.Sc. degree in Optoelectronics from Gdańsk University of Technology, Poland, in 2006. His main fields of interest include high performance computing clusters, network security and protocols, cloud computing and virtualization.

E-mail: tomasz.wlodarski@ncbj.gov.pl
National Centre for Nuclear Research
Andrzeja Sołtana 7
05-400 Otwock, Poland