



# SCADvanceXP—an intelligent Polish system for threat detection and monitoring of industrial networks


Mateusz Grzegorz Twardawa<sup>1</sup>, Marek Smolik<sup>2</sup>, Franciszek Rakowski<sup>3</sup>,  
Jakub Kwiatkowski<sup>4</sup>, Norbert Meyer<sup>5</sup>

<sup>1</sup>[mtwardawa@man.poznan.pl](mailto:mtwardawa@man.poznan.pl)

<sup>1</sup>  <https://orcid.org/0000-0003-0661-0128>

<sup>3</sup>  <https://orcid.org/0000-0001-6133-8900>

<sup>4</sup>  <https://orcid.org/0000-0001-7000-3862>

<sup>5</sup>  <https://orcid.org/0000-0003-4020-5329>

<sup>1,4</sup>ICT Security Department, Poznań Supercomputing and Networking Center (PSNC), affiliated to the Institute of Bioorganic Chemistry of the Polish Academy of Sciences, Jana Pawła II10, 61-139, Poznań, Poland; Institute of Computing Science, Poznań University of Technology, Piotrowo 2, 60-965, Poznań, Poland

<sup>2</sup>CTO, ICsec S.A., Wichrowa 1A, 60-449, Poznań, Poland

<sup>3</sup>R&D Department, ICsec S.A., Wichrowa 1A, 60-449, Poznań, Poland

<sup>5</sup>Data Processing Technologies Division, Poznań Supercomputing and Networking Center (PSNC), affiliated to the Institute of Bioorganic Chemistry of the Polish Academy of Sciences, Z. Noskowskiego 12/14, 61-704, Poznań, Poland

## Abstract

*SCADvanceXP is an industrial network intrusion detection system that scans and monitors data exchange between engineering stations, field divides, controllers, supervisory control and data acquisition (SCADA), and other elements of the operational technology network in detail. SCADvanceXP has the potential to detect advanced attacks on industrial infrastructures with the use of rule-based, signature-based, and behavioural detection methods, which are supported by sophisticated machine and deep learning models. As a system developed in Poland, it addresses the needs of industry in that region of Europe. The goal of this work was to assess SCADvanceXP's potential to detect common industrial threats. In order to check SCADvanceXP's potential, an effort was undertaken to evaluate its functionality on major industrial threats. For that purpose, twelve malware strains interfering with industrial systems were described. Later, the SCADvanceXP functionality was overlapped on malware behavioural and detection markers, pointing out exact mechanisms in SCADvanceXP that would detect analysed threats. The results show that SCADvanceXP is able to detect a wide range of attacks on industrial networks. SCADvanceXP's rich functionality is able to provide a high standard of security. However, if a threat is affecting systems not directly connected with industrial networks, SCADvanceXP will not be able to detect it. SCADvanceXP only monitors industrial systems; hence, corporate networks must be protected by a different solution to provide the required level of*

security. Nonetheless, SCADvanceXP is dedicated to operating within industrial networks and does not have access to regular IT networks. It can be concluded that SCADvanceXP is a specialist tool providing desired security for industrial networks.

## Keywords

malware, anomaly detection, cybersecurity, intrusion detection systems, industrial networks

### Article info

Received: 14 September 2023  
Revised: 11 December 2023  
Accepted: 27 December 2023  
Available online: 3 March 2024

Citation: Twardawa, M.G., Smolik, M., Rakowski, F., Kwiatkowski, J. Meyer, N. (2024) 'SCADvanceXP – An intelligent Polish system for threat detection and monitoring of industrial networks', *Security and Defence Quarterly*, 48(4), doi: [10.35467/sdq/177655](https://doi.org/10.35467/sdq/177655).

## Introduction

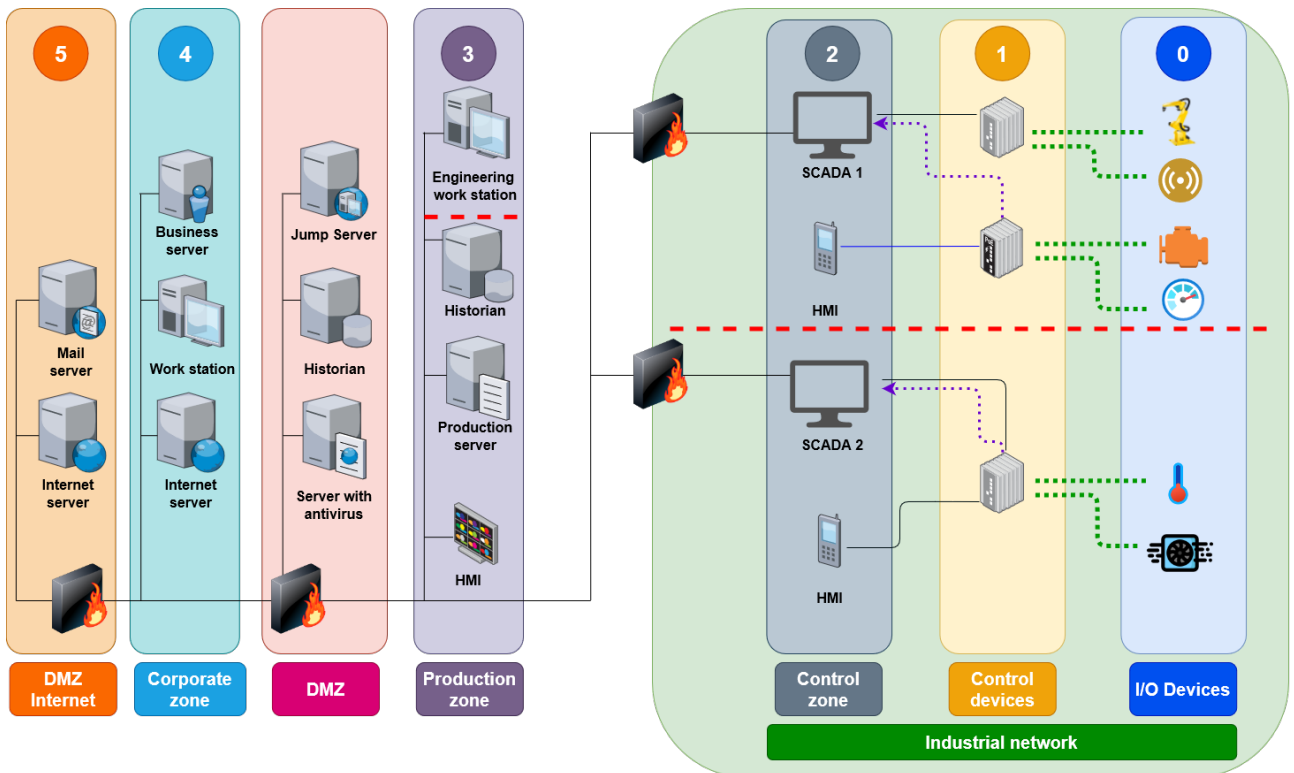
According to the in-depth principle of defence, ensuring IT enterprise-level protection is not enough if an industrial operational technology (OT) network remains without security supervision. Constant asset monitoring, vulnerability checking, and traffic analysis are essential to detect industrial network intrusions and weak spots. For this reason, SCADvanceXP was developed. SCADvanceXP is an advanced and dedicated system for intrusion detection in diverse industrial network environments. It encompasses many complementary functions, including traffic monitoring, deep packet inspection, independent process value monitoring, tools for asset management in an industrial network, a vulnerability scanner, and many other things. SCADvanceXP's intrusion detection methods incorporate advanced and tested machine-learning (ML) models that are able to provide robust and mature network monitoring mechanisms.

In this work, analysis was focused on overlapping SCADvanceXP functionality on the detection capacity of the most advanced current threats. For this purpose, twelve commonly occurring malware strains affecting (directly or indirectly) industrial systems were selected and SCADvanceXP's detection mechanisms were analysed for them.

## Industrial network security in a nutshell

Efficient and reliable communication between devices is essential for modern industrial process automation. Thanks to fast data exchange between elements of the industrial network like programmable logic controllers (PLCs) and terminal devices (e.g. valves, sensors, and mechanical arms), it is possible to continuously control even deeply complex processes. Industrial systems incorporate many dispersed elements that have to be orchestrated, monitored, and protected. The whole system is usually encapsulated under an integrated network called the industrial control system (ICS). A popular example of such system is Supervisory Control and Data Acquisition (SCADA). Figure 1 is a diagram of an internal network and shows the structure of zones typically defined for industrial networks, highlighting their overall location and difference from other networks (the Purdue model [Williams, 1994]). Almost all industrial systems demand speed, precision, and coordination to operate reliably and provide the required level of automation.

Figure 1. An internal network divided into two distinct parts, that is, corporate and industrial. The visuals highlight the differences between an industrial OT network and a more regular IT network on specific network levels marked with a number. Level 5 consists of servers and other equipment that have contact with the external network (the Internet), and this fragment should be treated as a demilitarised zone (DMZ). A typical corporate network is considered as 4th level. Office computers and equipment are meant to be localised in this network segment. Level 3 is called the production zone; it stores and processes crucial data that should be protected. Therefore, it might be necessary to distinguish additional DMZ between production and corporate zones. Levels 2, 1, and 0 represent the industrial network that should be desirably disconnected from any other network, although this is not always possible or convenient. Level 2 contains human machine interfaces, monitors, and SCADA operational centres, providing necessary orchestration and supervision over industrial processes. Level 1 is meant for controllers that oversee and send direct commands to sensors and other acting devices located on Level 0 that execute and maintain industrial processes.



There are three main industrial communication architectures that will be briefly described, that is, the RS-485 (Soltero *et al.*, 2002, pp. 3–12), the Controller Area Network (CAN) (De Andrade *et al.*, 2018), and the Ethernet (Spurgeon, 2000, pp. 23–38). Each of these interfaces was developed assuming different limitations and was meant to operate under well-defined but distinct conditions. RS-485 provides serial, fast, and robust communication over a fieldbus, allowing devices to communicate even at longer distances (Soltero *et al.*, 2002, pp. 3–12). Popular protocols operating in RS-485 include MODBUS remote terminal unit (RTU) (Modbus Organization Inc., 2012) and PROFIBUS DP (Mitchell, 2003, pp. 1–20). In contrast to RS-485, CAN was designed to work over short distances, and was developed especially for vehicles (cars, trains, planes, etc.). There is one protocol designed for this interface called CANopen (CAN in Automation [CiA], 2011). The Ethernet (IEEE 802.3) is the most common interface. The Ethernet allows large amounts of data to be transferred in a relatively short time. Although there are many regular protocols operating on the Ethernet within industrial networks, the basis for the communication relies on dedicated ones, for instance, MODBUS TCP/IP, DNP3, PROFINET IO, and EtherCAT (Lin and Pearson, 2018).

Industrial systems are common and extremely important for everyday life. Examples of industrial networks can be found in critical infrastructure, including power, water, or sewage treatment plants and across many factories. Moreover, industrial communication is essential for building management systems and modern vehicles. Work interruptions

within industrial networks may have a wide range of consequences. In some scenarios, outcomes can have some impact on infrastructure functioning, such as wasting an employee's time. However, the real attack scenarios (as any other causes of major failures) can have extreme consequences, including long-lasting blackouts, infrastructure collapse, and loss of life ([Hemsley and Fisher, 2018](#)). Table 1 shows selected and well-known examples of attacks on industrial networks.

Although attacks on an industrial network may cause enormous damage, these networks are often much less protected than corporate ones. The reasons behind this unintuitive situation are complicated and require some historical context to be understood.

Before the Internet became widespread, the security setup of industrial infrastructures was based on two falsely assumed premises. The first assumption was that physical access protection is one of the most important lines of defence from external threats. As might be historically true for manual elements of industrial infrastructure (e.g. hand valves and manual switches) and fully isolated networks, modern infrastructure security cannot be limited to physical access control. Moreover, industrial networks are no longer fully isolated ([Knapp and Langill, 2015](#), pp. 41–57). For example, engineering stations have access to both internal corporate network and industrial one. Computers with such configuration might be protected but, in principle, are capable of connecting (e.g. via proxy) to the Internet. Even if the network does not have any external connections, it must still be updated. Therefore, hackers may infect industrial machines using corrupted removal drives or compromised vendors. It is hard not to mention concerns about using new Internet of things (IoT) devices within the industrial networks that may be connected to the Internet and, at the same time, supervise the industrial process ([Jayalaxmi et al., 2021](#)). The second false assumption was that industrial systems are difficult to comprehend, since information about them is very hard to obtain (security by obscurity; [Alcaraz et al., 2012](#), pp. 120–149). This is no longer true, since it is possible to download for free, buy from legitimate vendors, or obtain from illegal sources industrial documentation and the specifications of almost any used industrial technology. Being in possession of large financial assets or sponsored by government, groups of hackers may even build entire industrial test laboratories. The number of industrial cybersecurity incidents was hard to notice in the last century. For example, the Repository of Industrial Security Incidents ([RISI, 2015](#)) includes only thirty-two attacks or occurrences of sabotage in automated industrial systems for the whole 20th century. This resulted in a false perception of threats, bad security practices, lack of attention, and investment in industrial control systems protection ([Knapp and Langill, 2015](#), pp. 41–57).

There are other reasons behind security holes in industrial control systems. Industrial networks often have to optimise speed and efficiency of communication by design, leaving limited options for security solutions ([Pei et al., 2018](#)). For example, it is common to switch off encryption and additional confirmations, since such options slow down response time. Moreover, older devices have limited or obsolete security functions. Some devices may not allow the creation of strong passwords, since they do not possess the required memory capacity to store enough information ([Knapp and Langill, 2015](#), pp. 41–57).

Usage of technical standards is unavoidable in industrial systems. They are used to facilitate integration, enforce compatibility, and quality of equipment as well as unification of communication technology offered by multiple vendors. It is not uncommon for standards to have some minor misfits with the exact needs of specific industrial infrastructure. This can make custom standard extensions seem viable, but also lead to security issues as

Table 1. Examples of successful attacks on industrial infrastructure.

Incident name	Short description	Consequences	Attack type (threat type)
PLC password change ( <a href="#">Canada, 1988</a> )	Frustrated employee of Allen-Bradley DH+ changed PLC password in different department. This situation led to loss of maintenance access ( <a href="#">Byres et al., 2002</a> ).	Time spent on restoring previous configuration and minor pause in industrial operations ( <a href="#">Byres et al., 2002</a> ).	Sabotage (insider)
Maroochy Water Incidents ( <a href="#">Australia, 2000</a> )	Ex-worker used stolen equipment (wireless radio, SCADA controller and control software) to control unprotected pumping station ( <a href="#">Slay and Miller, 2008</a> , pp. 73–82).	Contamination of river and coastal waters with more than 1,200 m <sup>3</sup> of untreated sewage that resulted in environmental harm, killing local marine life ( <a href="#">Slay and Miller, 2008</a> , pp. 73–82).	Sabotage (insider)
Tram accidents in Łódź ( <a href="#">Poland, 2008</a> )	Teenager constructed a device for remote control of tram line junctions ( <a href="#">Policja.pl, 2008</a> ).	Four trams were derailed and ten people were injured ( <a href="#">Policja.pl, 2008</a> ).	Sabotage (external)
Nuclear programme sabotage* ( <a href="#">Iran, 2010</a> )	Advanced malware (Stuxnet) infecting computers and PLCs developed to sabotage Iranian nuclear programme ( <a href="#">Langner, 2013</a> ).	Destruction of 20% of Iranian nuclear centrifuges ( <a href="#">Langner, 2013</a> ).	Sabotage (external)
German steel mill ( <a href="#">Germany, 2014</a> )	Perpetrators used social engineering to obtain access to internal network and later leveraged the access to industrial network. The attack made it impossible to shut down the furnace ( <a href="#">Lee et al., 2014</a> ).	Whole industrial infrastructure at steel mill suffered major damage ( <a href="#">Lee et al., 2014</a> ).	Sabotage (external)
Ukrainian power grid* ( <a href="#">Ukraine, 2015</a> )	Multistage attack on three power stations executed by Sandworm team. The attackers got access to network by spear phishing, and learned industrial processes and software. During the attack, power was remotely shut down, telephone lines suffered a DDoS attack, and data was destroyed ( <a href="#">Lee et al., 2016</a> ).	Blackout for up to 6 h, ~230,000 affected consumers ( <a href="#">Lee et al., 2016</a> ).	Cyberwar (external)
Colonial Pipeline ( <a href="#">USA, 2021</a> )	Using stolen passwords found on Darknet, perpetrators got access to internal network and downloaded 100 GB of sensitive data. One day later, adversaries deployed ransomware targeting company financial IT system used for billing customers ( <a href="#">Josephs, 2021</a> ).	The company paid a ransom (\$4.4 million) and halted pipeline operation as a precaution. Pipeline recovered after 5 days. Attack resulted in buying panic, altered flight schedules, gas and jet fuel shortages across five states, and even declaration of emergency ( <a href="#">Eaton and Volz, 2021</a> ).	Cybercrime (external)
Viasat satellite network* ( <a href="#">Ukraine, 2022</a> )	KA-SAT satellite network was attacked on the day of Russian invasion. Initial access to internal network was gained through exploitation of VPN misconfiguration. Attackers executed legitimate commands that overwrote crucial data in modem memory and made them unable to reconnect with the network ( <a href="#">Viasat Inc., 2022</a> ).	More than 10,000 modems in Ukraine were disconnected from satellite network. Since KA-SAT is used in the European Union (EU; mainly in Germany), collateral damage was done to 5,800 wind turbines that could not operate temporarily due to lack of network connection ( <a href="#">Burgess, 2022</a> ).	Cyberwar (external)

Note: \*Incidents sponsored or executed by a foreign country's forces.

a consequence. Furthermore, implementation of industrial standards can be flawed and adopt protective solutions poorly or insufficiently. If a standard is oblivious to certain existing threats, it may lead to much more dangerous situations in which standard vulnerabilities are exploited (Hajda *et al.*, 2021).

The high cost of halting industrial processes is a serious issue. Unscheduled operational pauses are able to seriously affect industrial safety. In fact, there are critical infrastructures that cannot be easily stopped from operating, and maintenance breaks must be carefully planned to preserve work continuity. This situation makes software and equipment security updates problematic, since planning and coordination are needed (Kumar *et al.*, 2022). Due to such constraints, security updates tend to be neglected or postponed. Furthermore, expensive investments in industrial machines and devices often assume long exploitation time (e.g. 20 years for controllers; Byres, 2013). On the one hand, industrial devices are able to operate for a considerable number of years, but on the other, progress in technology is so fast that new devices become obsolete within years. Many industries are not able to afford to replace all vulnerable devices and must rely on them, trying to strengthen the security in other places. This creates a dangerous situation in which there are many devices that are potential targets for hackers within the industrial network and none of them can be replaced for financial reasons (Byres, 2013).

Security incidents in industrial networks may affect vital processes and infrastructure, which may lead to severe consequences. Therefore, it is important to prevent unwanted events and counteract them, if possible. The majority of problems and blind spots in security within industrial infrastructure can be eliminated by careful management and deploying recommended security policies (Taherdoost, 2022).

## **SCADvanceXP—An innovative system specifically for industrial network protection**

SCADvanceXP is a new real-time intrusion detection system developed in Poland to ensure the safety of industrial networks (ICsec S.A., n.d.). The system was designed to fit a wide range of industrial designs, including many different networks operating in energy, manufacturing, production, or water treatment as long as there is an industrial control system to protect. The core role of SCADvanceXP is to monitor industrial network traffic and detect undesired or unusual events. There are many methods for anomaly detection embedded within SCADvanceXP analytics, including event processing, rule and signature detectors, statistical and machine-learning models, and physical process monitoring. As a fully functional and mature system, it can adapt to specific industrial network infrastructures in order to strengthen the ability to detect unwanted events. SCADvanceXP's main goal is to detect cyber threats (including Zero-Day threats) before they cause irreversible damage.

The origins of the SCADvanceXP system come from the research project SCADvance (SCADA Advance) (Dobski *et al.*, 2018). The aim of the SCADvance R&D project was to develop methods and solutions increasing the security of industrial networks, especially for companies in the electric power industry. The R&D project was conducted by ALMA S.A. (a beneficiary of the co-financed EU programme) and several renowned partners, including the Poznan Supercomputing and Networking Centre and Poznan University of Technology. The R&D project ended with a fully functional prototype (VI TRL level). Based on the promising results of the R&D project, the ICsec S.A. company designed the market-ready product, marketed it, and further developed and supported it afterwards.

ICsec S.A. conducted two R&D projects co-financed from EU funds within Smart Growth Operational Programme 2014–2020 that were aimed at further development of SCADvanceXP functionalities. First one, the SMUAP project (pl.: System monitoringu urządzeń automatyki przemysłowej - Industrial Automation Equipment Monitoring System) was focused on AI/ML module development, vulnerability checking, universal network sniffer (hardware and software). The second project - IDS Utilities (Development of the IDS system for OT in terms of the requirements of the public utility sector) was focused on managing the security of third-party communication protocols, which are used in SCADA drivers and programs. The project was especially focused on tracking physical values through Deep Packet Inspection (DPI) sent by industrial protocols and the use of the SBOM (software bill of materials) standard to extend the vulnerability checker module. The IDS Utilities project also introduced proxy servers as part of SCADvanceXP system that allow for distributed computing on selected parts of the network.

SCADvanceXP processes raw traffic collected by X1 probes installed in an industrial network. Probes were carefully designed to efficiently and reliably transfer data over the Ethernet (SPAN port and pass through), RS232/422/485 and CAN interfaces. These devices are also able to calculate fundamental traffic statistics based on embedded software. The important security feature of probes is a galvanic separation of sniffing listening that in practice makes bidirectional transmission impossible as well as any electromagnetic interference between the IT and OT sides related to the device. Therefore, the SCADvanceXP system is fully passive and unable to interfere with industrial processes and communication within the existing infrastructure of the OT network. In addition to that, thanks to its ability to work in a “transparent” or “SPAN port” mode, it is possible to install the X1 probe in all of the most complex configurations of industrial network topologies.

Time is the most important asset in industrial process automation, since rapid reaction to sudden changes may prevent irreversible losses and system failures. SCADvanceXP addresses this requirement by putting all the effort in making continuous monitoring and analysis as fast as possible and it qualifies as a real-time system. SCADvanceXP has many innovative functionalities that include asset management and inventory monitoring, industrial traffic analysis, and anomaly detection with a focus on cyber threats, vulnerability scanning, physical process monitoring, and incident management. To provide more details, each enumerated functionality is briefly described below.

Inventory awareness is essential for efficient network protection. The SCADvanceXP system detects devices connected to the protected network based on the observed traffic and creates a map of connections between devices in the network. Hence, any changes in communication architecture or device inventory can be easily spotted. With an automatically created OT network topological map, a user may study details about devices and data exchange to safely correct the configuration of industrial devices and ensure a network's operational integrity. To give more concrete examples, the SCADvanceXP system reacts if a new device appears in the network, an existing device vanishes, or in the case of packet exchange between devices that should not communicate. However, the SCADvanceXP system was designed to be passive; therefore, it cannot exclude or block devices within an industrial network.

SCADvanceXP is focused simultaneously on many details and dimensions of industrial communication. The key advantage of this system is its analytical engine. The analytical capabilities of SCADvanceXP are supported by multiple mechanisms, including rule-based methods, signature-based methods, and *Artificial Intelligence* (AI)/ML methods for anomaly-based detection.

SCADvanceXP uses complex mechanisms to adapt and adjust anomaly detection models. There are three major types of AI-based anomaly detection techniques operating in the system: statistical modelling, prognostic machine-learning, and deep neural networks. These techniques are complementary to each other, and furthermore, the system does have methods to integrate all the results and present coherent information. The system has automated mechanisms based on advanced optimisation to increase anomaly detection efficiency for users with limited hardware resources.

Along with machine-learning models, SCADvanceXP employs standard and well-established methods for threat detection, namely rule and signature matching. Such methods are obligatory and allow known dangers to be detected. It is possible to define threats and search for malicious activity traces that have been found and defined in other industrial networks. These methods may also be used to notify the user of suspicious packets (e.g. execution of rare commands on industrial devices) or simply any event of interest, not necessarily related to security issues. As can be seen, SCADvanceXP has enormous potential in event and anomaly detection, since it is able to encompass information about patterns of communication and learn details about network behaviour.

The SCADvanceXP system is integrated with Common Vulnerabilities and Exposures (CVE Program, n.d.) and Common Platform Enumeration (CPE) databases; therefore, it is able to detect known vulnerabilities. Thanks to this functionality, it is possible to prevent security incidents by making necessary security updates and hardening or replacing all outdated devices that could easily become a target for hackers. This feature is very important, since incident prevention is much less costly than restoring damaged infrastructure.

Another feature of SCADvanceXP is its ability to monitor physical process values. This trait is unique, since only the SCADA system and industrial devices are able to send and read requests. However, based on industrial standards, the SCADvanceXP system is able to decode user-defined variables with a dedicated module. Since the behaviour of industrial variables can be monitored, changes and unwanted variable values can be quickly reported to the users. Thanks to the fact that SCADvanceXP operates passively, it cannot interfere with industrial processes. Moreover, detection of SCADA failures is also possible. It is worth mentioning that many attacks on industrial networks are stealthy, meaning they use many means to hide their traces from SCADA systems, for example, by deploying replay attacks, disabling alerts, or misconfiguring SCADA to deceive an operator (Kleinmann *et al.*, 2018, pp. 93–109; Krotofil *et al.*, 2015, pp. 133–144; Liu *et al.*, 2011).

In addition to process value monitoring, SCADvanceXP is capable of deep packet inspection. Thanks to deep learning models, the system can learn packet features to detect distortions, unusual transmission patterns, or message content changes without the necessity of decoding message payload.

SCADvanceXP is not only capable of security incident detection but can also help coping with it. First of all, SCADvanceXP possesses forensic tools to help study timeline of events related to the incident. Moreover, SCADvanceXP is able to present network elements involved in attack and point to associated anomalies. All of this information may help in managing the incident, showing all exploited system elements that need to be handled as well as elements within the network that may not operate correctly.



## Assessment of SCADvanceXP threat detection capability potential

Industrial networks are exposed to many dangerous threats. It is difficult to assess how currently known threats may be detected by any system. The following analysis is based on assumptions and available knowledge. The goal of this analysis was to evaluate detection potential for twelve commonly occurring malware strains and variants. Since well-documented malware samples are taken into evaluation, it is possible to connect SCADvanceXP detection potential with infection indicators of malware samples.

The malware picked for the analysis is summarised briefly in Table 2. All analysed samples were described in more detail, pointing to specific markers of malicious activity that could be potentially detected by the current version of the SCADvanceXP system. In order to provide more concrete and specific analysis, Industroyer malware was chosen as

Table 2. Malicious software that are known to interfere with industrial control systems reported in Central and Eastern Europe.

Malware strain	Short description	Attacked countries	SCADvanceXP detection potential
BlackEnergy	Malicious software toolkit known from Russian conflicts. Originally DDoS tool, upgraded over time to inflict damage and spy (Khan <i>et al.</i> , 2016, pp. 1–11).	Ukraine and Georgia	Yes
GreyEnergy	Successor of BlackEnergy malware with ability to exploit more backdoors (Di Pinto [Nozomi Networks], 2019).	Poland and Ukraine	Yes
Industroyer	Malware dedicated to inflict damage in industrial systems, especially electrical substations (Kapellmann-Zafra <i>et al.</i> , 2022).	Ukraine	Yes
PipeDream	Sophisticated malware toolkit able to attack various industrial infrastructures (HeadMind Partners, 2022).	Unknown (Ukraine?)	Yes
Conflicker	Worm that was responsible for shutting down a German nuclear power plant in 2016 (Trend Micro Inc., 2016).	Germany, Global	Non-applicable
NotPetya	Wiper created to destroy IT infrastructure in Ukraine (Greenberg, 2018).	Ukraine, Poland, and Europe	Non-applicable
Conti	Ransomware attacking different targets around the world (Cimpanu, 2020).	Ukraine, EU, and USA	Non-applicable
EKANS	Ransomware targeting popular ICS software frameworks (e.g. Honeywell HMIWeb or GE PROFICY) (Belding, 2020).	EU and USA	Non-applicable
STUXnet	Worm designed to sabotage industrial processes and exploiting Siemens Step7 PLCs (Langner, 2013).	Iran, Global	Yes
Duqu	Closely related to STUXnet malicious espionage worm used to prepare future attacks (Paganini, 2019).	Austria, Russia, and Switzerland	Yes
Havex	Espionage tool that affected thousands of victims in whole energy sector, including solution providers (Slowik, 2021).	Europe, Canada, and USA	Yes
Triton	Malicious framework for exploitation of Triconex Safety Instrumented System controllers (Johnson <i>et al.</i> , 2017).	Europe, Canada, and USA	Yes

Note: Only the most common and dangerous malware strains were picked for evaluation of the SCADvanceXP detection potential. The caption “Non-applicable” was used to mark examples of malware that do not interfere directly with industrial networks.

a representative example and its detection potential was described extensively. Based on this example, a better explanation of SCADvanceXP detection power could be presented in the context of other threats.

In order to evaluate the detectability potential of SCADvanceXP modules, twenty defined malicious actions were picked and associated with selected malware strains. Table 3 shows the connections and how different malware strains can interfere with industrial networks. For each malicious action, the detectability potential by SCADvanceXP was also determined. The detection potential of every SCADvanceXP module was evaluated for each malicious capability defined in Table 4. Additionally, the same information was added for the IT security solution for corporate networks that are not able to analyse industrial networks and devices.

Industroyer (or CRASHOVERRIDE) is a malicious framework that is known from one of the most infamous cyber attacks affecting power grid systems, which took place in Ukraine on 17 December 2016 ([Cherepanov and Lipovsky, 2018](#)). The attack was thoroughly prepared, with extensive knowledge of the industrial-type communication network. Effectively carried out attacks and malware development is attributed to the notorious Sandworm team ([Dragos Inc., n.d.](#)). Industroyer was an attempt to automate attacks on power grids, executed manually by the same team a year before ([Lee et al., 2016](#)). An updated version of this malware still exists, namely Industroyer 2, which has been used to execute attacks in 2022 on Ukrainian power grid systems ([Kapellmann-Zafra et al., 2022](#)).

The Industroyer attack vector, which might also be considered as an exemplary case for the methods used in other OT attacks, consists of several components. The first, allowing for general intrusion, was an installation of the malware on the main SCADA server, breaking through by spear phishing. The main backdoor was then supported by installation of an additional backdoor—letting the attackers keep control over the SCADA server while the main backdoor was out of order. These pair of backdoors enabled an obscure connection with the attackers' Control & Command system and execution of the next attack steps. However, the proper monitoring of the system topology, as is done by the SCADvanceXP EWL module, discovers the appearance of new Internet protocols (IPs) for which new regular connections have been established by means of passive packet monitoring. It raises one of the first security alerts generated by the intrusion detection system (IDS).

Secondly, the attacker scans for the presence of other supervisory computers (master stations for RTUs or PLCs), and when they are discovered installs the launcher malware and protocol-specific libraries. Industroyer toolbox had a specialised network mapping tool for scanning network topology. The act of scanning leaves a trace in the network activity log in the form of sent packets and can be detected by IDS tools, such as SCADvanceXP.

Once the launcher is installed on one or many supervisory computers, which gather data and sent control commands to RTUs or PLCs, execution of malicious commands becomes possible, including scanning and modifying the register values and functions sent to terminal devices.

The Industroyer was designed to modify the payloads of the packets transmitted within four industrial protocols: (1) IEC 60870-5-101, (2) IEC 60870-5-104, (3) IEC 61850, and (4) OLE for process control data access ([Kapellmann-Zafra et al., 2022](#)). This is an important and advanced feature making it possible for this malware to directly interfere with industrial network communication. Physical value monitoring (PVM) is part of the SCADvanceXP system for monitoring the variable values defined by the user specification

Table 3. Selected capabilities of malware strains chosen in this study.

Malicious action	Black Energy	Grey Energy	Indu- stroyer	Pipe Dream	Con- flicker	Not Petya	Conti	EKANS	STUX- net	Duqu	Havex	Triton
Disruptions to ICS operations	X	X	X	X	X	X	X	X	X		X	X
Windows workstation corruption	X	X	X	X	X	X	X	X	X	X	X	X
Industrial network scanning	X		X	X		X			X	X	X	X
Propagation within industrial networks				X		X			X		X	
Vulnerable device profiling			X	X					X	X		X
Manipulation of industrial devices (including register values and commands)	X		X	X					X			X
Industrial traffic and payload manipulation			X	X					X			X
Industrial DoS attacks	X	X	X	X								
Password brute force on PLC			X	X								
Industrial network traffic recording	X	X	X	X					X			
Destruction of data on industrial devices			X	X								
Modification of project and configuration files			X	X					X			X
Manipulation of view	X	X	X	X					X			X
Loss of view	X	X	X	X	X	X	X	X	X			
ICS-related processes killing			X	X		X		X	X			X
Remote connection to C&C	X	X	X	X	X		X		X	X	X	
Local network scanning	X	X	X	X	X	X	X	X	X	X	X	X
Data exfiltration	X	X	X	X	X		X		X	X	X	X
Propagation within network	X	X	X	X	X	X	X	X	X	X	X	X
System process modification and injection	X	X	X	X	X	X	X	X	X	X	X	

Note: The list of 20 capabilities is not exhaustive, but it provides a general overview on malicious actions performed by different malware strains evaluated in this work. Each malware strain that is able to exhibit defined malicious behaviour is marked with “X” in the respective row.

**Table 4. Detectability of selected malicious capabilities by SCADvanceXP and regular IT security solutions.**

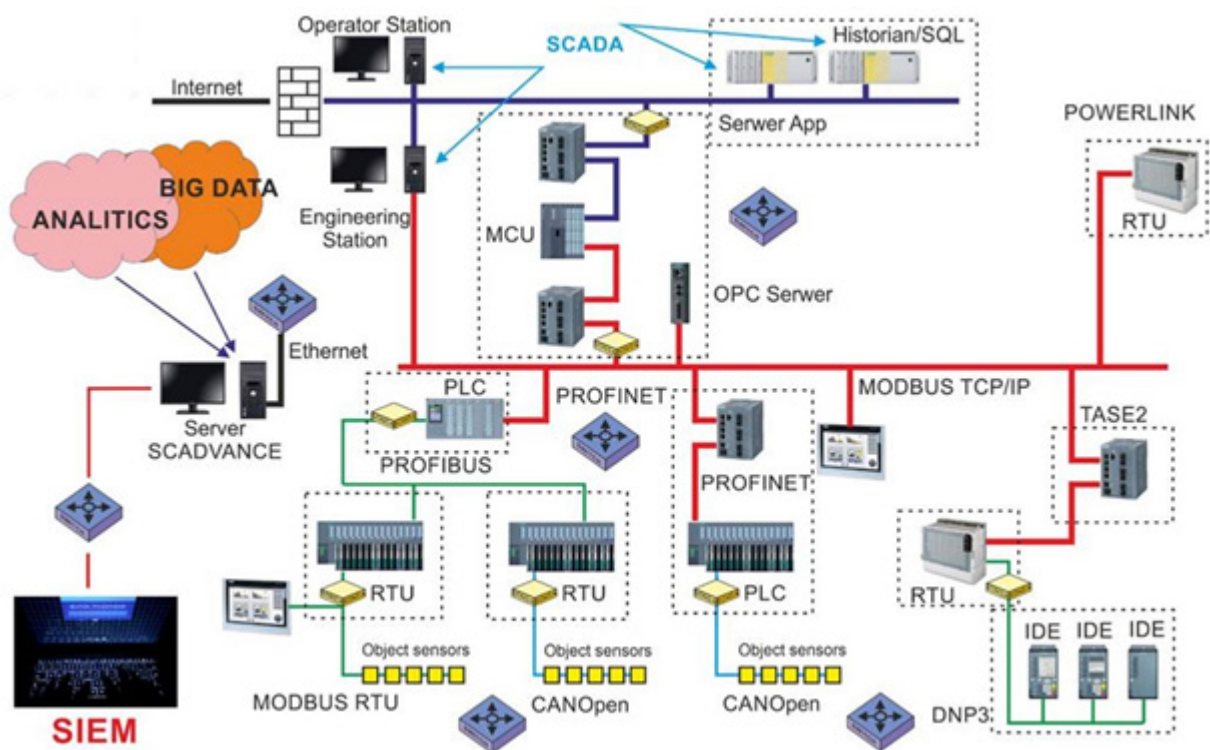
Malicious action	Asset management and inventory monitoring	Industrial traffic monitoring and anomaly detection (AI)	Process value monitoring	Vulnerability scanning	Deep packet inspection	Signature matching	Modern IT security solutions
Disruptions to ICS operations	X	X	X	X	X	X	
Windows workstation corruption	X			X		X	X
Industrial network scanning	X	X				X	
Propagation within industrial networks	X	X		X		X	
Vulnerable device profiling	X	X		X		X	
Manipulation of industrial devices (including register values and commands)		X	X	X	X	X	
Industrial traffic and payload manipulation	X	X	X	X	X	X	
Industrial DoS attacks	X	X				X	
Password brute force on PLC		X		X		X	
Industrial network traffic recording	X	X	X		X	X	
Destruction of data on industrial devices		X	X	X	X	X	
Modification of project and configuration files	X		X	X		X	
Manipulation of view		X	X		X	X	
Loss of view		X	X		X	X	
ICS-related processes killing	X	X				X	
Remote connection to C&C	X						X
Local network scanning	X						X
Data exfiltration							X
Propagation within network	X						X
System process modification and injection				X			X

**Note:** For each distinguished SCADvanceXP module (in columns), the letter “X” appeared for every malicious action (in rows) it can detect. The last column contained general modern IT solutions (e.g. firewalls and antiviral software) that operate in corporate networks.

Figure 2. Photo of the SCADvanceXP desktop screen and the X1 probe (provided by ICsec S.A. [n.d.]).



Figure 3. Graphic showing SCADvanceXP deployment within industrial network.



of register addresses and values format on RTU. In the family of IEC protocols for power system automation, the RTU registers are called Application Service Data Unit (ASDU) and referring pointers are called Information Object Addresses (OAs). The dedicated malware installed by the main door launcher altered the values in ASDU (Kapellmann-Zafra *et al.*, 2022). The SCADvanceXP system allows the constant monitoring of these values. PVM raises alerts when user-defined limits are exceeded. It might be a powerful tool for securing OT infrastructures, although it requires the active participation of human beings (security officers) in defining the registers to be monitored. The step forward is the automatic detection of anomalous behaviour applied in AI modules.

One of the most advanced and novel techniques for OT network monitoring is the usage of machine learning for detecting the anomalous behaviour of the systems. This might be manifested by rapid and significant change of patterns in data exchange dynamics given by network traffic. The starting point is a definition of the typical behaviour of a network or its components—sub-networks and individual connections. The claim is that each installation, composed of configured, node devices (servers and RTUs) of closed set manufactures running in operation, exhibits typical patterns that can be monitored and characterised by passive systems, such as SCADvanceXP. On the one hand, the choice of features which describe those patterns is a subject of expert research and is based on the packet content, all of which is readable, might be a constituent of the feature. On the other hand, the passiveness of the cybersecurity system limits the number of detection methods for threats. The packet content can be read out in explicit mode for depicting basic information defined in protocol specification (such as the MAC addresses, protocols of existing layers, IP addresses, and many others). Simultaneously, the packet or series of packets might be treated as an encapsulated portion of information and described by its external or non-encoded parameters. The ones which are often reliable are frequency of packets, time interval between packets, packet (or payload) length, and payload entropy. SCADvanceXP uses this information (and more) to learn network behaviour and report anomalies based on machine-learning models.

In the event of an Industroyer attack, the RTUs were affected with the usage of four low-level malicious codes (DLLs) executed by the launcher installed directly by the main backdoor malware: (1) 101 payload, (2) 104 payload, (3) 61850 payload, and (4) OPC DA payload ([Kapellmann-Zafra et al., 2022](#)). The goal of the first one, 101 payload (named after IEC 60870-5-101 protocol) was to interact with all discovered IOAs (information data object) on a given RTU, and switch their state between off and on. Such an abnormal way of functioning clearly manifested in the modification of the interaction frequency of controlling and controlled stations and, to some extent, in packet payload content, thus in its entropy and length. The alteration of those features can be detected by the AI models employed in the SCADvanceXP system, even though they are subtle and dispersed in the entire phase space of features. The system is capable of precisely defining and configuring the volume (the subspace) for the proper detection of anomalies while keeping control over the number of false positives cases.

The SCADvanceXP cybersecurity system is also equipped with a vulnerability checker module. The principal functionality of the module is directed towards detection, identification, and information about the devices and services present in the network, which might be vulnerable for malicious software installations. The module is combined with a large CVE Program (n.d.) database and CPE database issued by the National Institute of Standards and Technology (n.d.) organisation and updated continuously. These databases contain the list of all platforms (i.e. the operating systems, software, services, devices) in which vulnerability has been identified. The CVE lists those vulnerabilities and refers to the recommended actions which have to be taken to secure the system. The list of platforms existing in the network and assigned to the network nodes is created automatically by the SCADvanceXP system and aligned with CPE and CVE datasets.

It is known that the Industroyer toolbox also contains malware exploiting a vulnerability tagged as CVE-2015-5374, already known at the time of the attack, and part of the Siemens SIPROTEC device. It calls up the Denial of Service function, after which a manual reboot of the device is required.

Industroyer was able to cause a blackout for less than 2 hours in 2016 ([Cherepanov and Lipovsky, 2018](#)). Since then, it has been upgraded and in April 2022, a new malware toolkit

was discovered related to Industroyer, namely Pipedream (also known as Chernovite and Incontroller) ([HeadMind Partners, 2022](#)). Both of them are designed to attack a wide range of industrial networks, spy on them, and sabotage or directly damage them by sending crafted messages created to resemble valid commands. Pipedream tools are able to modify payloads of the packets transmitted within many industrial protocols and probably many more malicious actions. In this case, vulnerable devices include Schneider Electric PLCs, OMRON Sysmac NEX PLCs, and Open Platform Communications Unified Architecture (OPC UA) servers ([HeadMind Partners, 2022](#)). The SCADvanceXP system was designed to detect unique and advanced threats similar to this. Both Industroyer and Pipedream perform malicious actions that by their very nature must interfere with industrial network communication and devices. The methods employed by SCADvanceXP quickly track and report such interference as suspicious behaviour or directly disclose it as a confirmed incident.

Since Industroyer was described in such detail, the rest of the threats are summarised briefly, especially in the case of regular malware attacking industrial infrastructure. Ransomware and wipers (Conflicker, NotPetya, Conti, and EKANS) affecting operator computer stations are beyond the detection capabilities of SCADvanceXP. Since only attack consequences can be detected (such as loss of the command centre), SCADvanceXP does not detect these forms of malware.

Conflicker is a computer worm affecting computers running on Windows OS. Although this malware is not designed to interfere with industrial control systems, it can halt whole industrial infrastructure. This happened in 2016, when a German nuclear power plant was shut down due to the Conflicker virus being found in the engineering station, which could be under the control of remote malefactors ([Trend Micro Inc., 2016](#)).

NotPetya is a wiper specially designed to attack Ukrainian facilities, including companies, factories, and critical infrastructure. NotPetya spreads quickly and pretends to encrypt the memory of infected computers; however, in reality, data is also modified, making recovery impossible. The activity of this piece of malware can lead to the shutting down of large industrial infrastructures (e.g. the MAERSK incident), since ICS stations, servers, business, and other crucial items for computer operation are completely neutralised ([Greenberg, 2018](#)).

Conti is a widespread malware strain that operates in the form of Ransomware-as-a-Service (RaaS). Conti steals and encrypts sensitive or information crucial for business. As in the case of NotPetya, attacks on crucial IT equipment can in consequence affect industrial processes ([Cimpanu, 2020](#)).

EKANS is the ransomware strain that hides and encrypts infected computers. It can masquerade as a proper update file and is designed to target computers connected to industrial networks. EKANS has a hardcoded list of processes to kill that enumerates GE Proficy and Honeywell HMIWeb services. This malware strain was detected in the Honda manufacturing plant, causing production losses ([Belding, 2020](#)).

BlackEnergy is another malicious toolkit, known since the Georgian conflict ([Stewart, 2010](#)). It is suspected that the infamous Sandworm team created it to interfere with energy grids ([Khan et al., 2016](#), pp. 1–11). Upgraded versions of BlackEnergy were deployed in Ukraine during power grid attacks in 2015 ([Khan et al., 2016](#), pp. 1–11). A new updated successor version of this malware strain is called GreyEnergy ([Di Pinto \[Nozomi Networks\], 2019](#)). These malware toolkits serve to facilitate unauthorised access to the operator station, steal data, and take control via a remote desktop client.

Since SCADvanceXP operates inside the industrial network, it is not possible to detect BlackEnergy and GreyEnergy on regular Windows computers. However, SCADvanceXP does detect any action executed from an infected operator workstation. This type of threat is similar to insider attacks and the SCADvanceXP system is programmed to report malicious and untypical actions performed by privileged users, including data acquisition as well as changes made in industrial process control (even ineffective ones).

One of the most notorious examples of malware used to compromise and inflict damage to industrial control systems is STUXNET. Designed to slow down and sabotage the Iranian nuclear programme, STUXNET was successfully planted at Natanz nuclear facility ([Langner, 2013](#)). At the time, some considered this malware to be state-of-the-art within the industrial sector. Along with many capabilities, STUXNET was able to self-replicate, check the type of machine it was working on, and adjust its behaviour. STUXNET could download updates for itself from a remote server and attack specific industrial devices (PLC). Interfering with industrial processes, STUXNET was able to change control commands to uranium centrifuges and, at the same time, replay previously recorded data to SCADA in order to hide the malicious act of sabotage ([Langner, 2013](#)).

Duqu is a version of STUXNET that was upgraded mainly for espionage purposes ([Paganini, 2019](#)). In contrast to Stuxnet, Duqu does not possess modules to directly interfere with the industrial process, since it serves only for sensitive data theft and collection of material that helps in preparation of future attacks. Duqu is also programmed to self-delete after 36 days ([Paganini, 2019](#)). Since STUXNET is able to interfere with the industrial network, it can be detected by SCADvanceXP machine-learning modules; this, however, cannot be said for Duqu, which operates on a higher level. Nonetheless, Duqu can be recognised by rule-based mechanisms embedded in SCADvanceXP's functionality.

Havex or Backdooroldrea is a Remote Access Trojan (RAT) able to conduct espionage of industrial infrastructure ([Slowik, 2021](#)). This malware tool scans industrial networks, targets industrial devices, and maps the network. This scanning activity is easily detected by SCADvanceXP modules and can be quickly reported as it happens to network operators.

Triton was specifically developed to exploit Schneider Electric Triconex Safety Instrumented System (SIS) controllers ([Kovacs, 2018](#)). This complex malware reprograms safety procedures of vulnerable devices. It can either make them ignore an unsafe state to allow potentially dangerous conditions to persist and lead to damage (or, in addition, interfere with the industrial process to induce real hazard) or force them to turn off full alerts and safety protocols. This may lead to the shutting down of all industrial operations, even if there are no threats to the industrial process and infrastructure at the time ([Johnson et al., 2017](#)). SCADvanceXP is able to detect such reconfiguration, changes in protocol, physical values, and vulnerable devices. Triton malware and similar attacks should therefore be detected by SCADvanceXP.

## Conclusions

In summary, SCADvanceXP is an advanced and specialised system for protecting industrial networks. Among many threats currently present in Europe, SCADvanceXP is able to detect all those that interfere with industrial/OT wired networks (according to the authors' knowledge). Thanks to machine-learning techniques and advanced detection and scanning modules, SCADvanceXP is a powerful system that is able to significantly improve the protection level of industrial infrastructure. On the other side, there are many attacks on industrial systems affecting IT systems that SCADvanceXP will not detect.



Attacks on enterprise-level servers or elements of an IT network that do not affect industrial control systems are not in the scope of current SCADvanceXP detection capability. SCADvanceXP is a specialised system dedicated to analysing data from industrial communication systems and devices by design. Although SCADvanceXP is not a universal solution, its detection capabilities are unique and there are few similar solutions available (see: [Kaouk \*et al.\*, 2019](#), pp. 1699–1704; [Kim \*et al.\*, 2023](#); [Yask and Kumar, 2019](#)). Therefore, SCADvanceXP fills a security gap and provides safety for industrial infrastructure in a way that covers all aspects of industrial communication. All the arguments mentioned and its functionalities show that SCADvanceXP can be viewed as a holistic system for protecting industrial control systems.

Current conflicts, economic interests, and complex dependencies create a unique threat and vulnerability landscape. Many attacks on critical infrastructure are prepared by groups sponsored by states. Moreover, industrial networks can become military targets. Since the escalation of the Russo-Ukrainian war, attacks on critical and industrial systems have intensified. It has been shown that hackers often analyse and study industrial networks after they are initially compromised. The initial reconnaissance period, as well as other attack stages, may be detected by SCADvanceXP. Being able to detect even advanced attacks in the early stages, SCADvanceXP may truly protect industrial infrastructure before any damage is done. As military and economic tensions escalate in Central and Eastern Europe, systems like SCADvanceXP may prevent major incidents within the industry, and manufacturing and critical infrastructure sectors. It is worth remembering that industrial systems' security is important for electro-energetic sector stability in Europe, which remains one of the primary targets of Russian forces in Ukraine ([Przetacznik and Tarpova, 2022](#)).

The paradigm of defence in depth states that successful infrastructure protection requires deployment of all available means, rather than selected assets and actions. It is common for industrial systems to rely on IT security tools and programs, but these are not enough, especially if the threat is located within the industrial network. In such cases, solutions for the IT sector appear powerless. Therefore, the SCADvanceXP system seems to answer the current needs of the industrial cybersecurity landscape.

#### **Funding**

This research received no external funding.

#### **Author Contributions**

Conceptualization, M.G.T, M.S., F.R., and N.M.; methodology, M.G.T, M.S., and F.R.; software, M.G.T, M.S., and J.K.; validation, M.G.T, M.S., F.R., J.K., and N.M.; formal analysis, M.S., F.R., and J.K.; investigation, M.G.T, M.S., F.R., and J.K.; resources, F.R.; data curation, F.R. and J.K.; writing—preparation of original draft, M.G.T, M.S., and F.R.; writing—review and editing, M.G.T, F.R., and J.K.; visualization, M.G.T and J.K.; supervision, M.S. and N.M.; project administration, M.S. and N.M.; funding acquisition, M.S. and N.M.

#### **Data Availability Statement**

Data sharing not applicable. No new data was created or analysed in this study.

#### **Disclosure statement**

Marek Smolik reports a relationship with ICsec S.A. that includes board membership and employment. Franciszek Rakowski reports a relationship with ICsec S.A. that includes B2B cooperation. SCADvanceXP system was developed, thanks to the SCADvance R&D project, conducted by ALMA S.A. (beneficiary of EU co-financed programme, project ID: RPWP.01.02.00-30-0055/16-00) and several renowned partners, including Poznan Supercomputing and Networking Centre and Poznan University of Technology. The R&D project ended with a fully functional prototype (VI TRL level). Based on the promising results of the R&D project, ICsec S.A. designed the market-ready product, marketed it, and by ICsec S.A., continues to further develop and support it.

## References

- Alcaraz, C., Fernandez, G. and Carvajal, F.** (2012) 'Security aspects of SCADA and DCS environments', in Lopez, J., Setola, R. and Wolthusen, S. (eds.) *Critical infrastructure protection: Information infrastructure models, analysis, and defense*. Berlin: Springer, pp. 120–149. doi: [10.1007/978-3-642-28920-0](https://doi.org/10.1007/978-3-642-28920-0).
- Belding, G.** (2020) *Malware spotlight: Ekans, infosec: Malware analysis*. Available at: <https://resources.infosecinstitute.com/topic/malware-spotlight-ekans/> (Accessed: 24 March 2023).
- Burgess, M.** (2022) 'A mysterious satellite hack has victims far beyond Ukraine', *Wired*, 23 March. Available at: <https://www.wired.co.uk/article/viasat-internet-hack-ukraine-russia> (Accessed: 20 October 2022).
- Byres, E.** (2013) "'Rip and replace" approach to SCADA security is unrealistic', *TOFINO security blog*, 30 January. Available at: <https://www.tofinosecurity.com/blog/%E2%80%9Crip-and-replace%E2%80%9D-approach-scada-security-unrealistic> (Accessed: 17 October 2022).
- Byres, E., Carter, J., Elramly, A. and Hoffman, D.** (2002) 'Worlds in collision-ethernet and the factory floor', in *ISA emerging technologies conference*, Instrumentation Systems and Automation Society, Chicago, IL.
- CAN in Automation (CiA)** (2011) *CANopen application layer and communication profile, DS-301, version 4.02*, technical documentation. Erlangen: CiA.
- Cherepanov, A. and Lipovsky, R.** (2018) 'New telebots backdoor: First evidence linking industroyer to NotPetya', *WeLiveSecurity* (ESET Research), 11 October. Available at: <https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/> (Accessed: 2 March 2023).
- Cimpanu, C.** (2020) 'Conti ransomware uses 32 simultaneous CPU threads for blazing-fast encryption', *ZD NET Tech.*, 8 July. Available at: <https://www.zdnet.com/article/conti-ransomware-uses-32-simultaneous-cpu-threads-for-blazing-fast-encryption/> (Accessed: 24 March 2023).
- Common Vulnerabilities and Exposures (CVE) Program** (n.d.) Common vulnerabilities and exposures database. Available at: <https://www.cve.org> (Accessed: 26 March 2023).
- De Andrade, R., Hodel, K.N., Justo, J.F., Lagana, A.M., Santos, M.M. and Gu, Z.** (2018) 'Analytical and experimental performance evaluations of CAN-FD BUS', *IEEE Access*, 6, pp. 21287–21295. doi: [10.1109/ACCESS.2018.2826522](https://doi.org/10.1109/ACCESS.2018.2826522).
- Di Pinto, A.** (Nozomi Networks) (2019) *GreyEnergy: Dissecting the malware from maldoc to backdoor*, research paper. Available at: [https://uploads-ssl.webflow.com/645a4534705010e2cb244f50/649131e3441ad51e4b0da155\\_Nozomi-Networks-GreyEnergy-Dissecting-the-Malware.pdf](https://uploads-ssl.webflow.com/645a4534705010e2cb244f50/649131e3441ad51e4b0da155_Nozomi-Networks-GreyEnergy-Dissecting-the-Malware.pdf) (Accessed: 6 September 2023).
- Dobski, M., Frankowski, G., Meyer, N., Pilc, M. and Twardawa, M.** (2018) 'Zastosowanie metod uczenia maszynowego i zaawansowanego przetwarzania zdarzeń dla ochrony przemysłowych sieci infrastruktury krytycznej', *Przegląd Policyjny*, 4(132), pp. 79–93. doi: [10.5604/01.3001.0013.668](https://doi.org/10.5604/01.3001.0013.668).
- Dragos Inc.** (n.d.) *ELECTRUM threat group operations*. Available at: <https://www.dragos.com/threat/electrum/> (Accessed: 2 March 2023).
- Eaton, C. and Volz, D.** (2021) 'Colonial pipeline CEO tells why he paid hackers a \$4.4 million ransom', *The Wall Street Journal*, 19 May. Available at: <https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636> (Accessed: 20 October 2022).

- Greenberg, A.** (2018) 'The untold story of NotPetya, the most devastating cyber attack in history', *Wired*, 22 August. Available at: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> (Accessed: 11 November 2022).
- Hajda, J., Jakuszewski, R. and Ogonowski, S.** (2021) 'Security challenges in industry 4.0 PLC systems', *Applied Sciences*, 11(21), 9785. doi: [10.3390/app11219785](https://doi.org/10.3390/app11219785).
- HeadMind Partners** (2022) Pipedream/Incontroller: ICS-specific malware attacks. Available at: <https://www.headmind.com/fr/pipedream-incontroller-ics-specific-malware-attacks/> (Accessed: 23 March 2023).
- Hemsley, K.E. and Fisher, R.E.** (2018) *History of industrial control system cyber incidents*. Idaho Falls, ID: Idaho National Laboratory. Available at: <https://www.osti.gov/servlets/purl/1505628> (Accessed: 22 March 2023).
- ICsec S.A.** (n.d.) *SCADvanceXP* (website). Available at: <https://icsec.pl/en/scadvance/> (Accessed: 31 March 2022).
- Jayalaxmi, P., Saha, R., Kumar, G., Kumar, N. and Kim, T.-H.** (2021) 'A taxonomy of security issues in industrial internet-of-things: Scoping review for existing solutions, future implications, and research challenges', *IEEE Access*, 9, pp. 25344–25359. doi: [10.1109/ACCESS.2021.3057766](https://doi.org/10.1109/ACCESS.2021.3057766).
- Johnson, B., Caban, D., Krotofil, M., Scali, D., Brubaker, N. and Glycer, C.** (2017) 'Attackers deploy new ICS attack framework "TRITON" and cause operational disruption to critical infrastructure', *MANDIANT Blog*, 14 December. Available at: <https://www.mandiant.com/resources/blog/attackers-deploy-new-ics-attack-framework-triton> (Accessed: 31 March 2023).
- Josephs, L.** (2021) 'Pipeline outage forces American airlines to add stopsto some long-haul flights, southwest flies in fuel', *CNBC*, 10 May. Available at: <https://www.cnn.com/2021/05/10/colonial-pipeline-shutdown-forces-airlines-to-consider-other-ways-to-get-fuel.html> (Accessed: 20 October 2022).
- Kaouk, M., Flaus, J.-M., Potet, M.-L. and Groz, R.** (2019) 'A review of intrusion detection systems for industrial control systems', in *2019 6th International conference on control, decision and information technologies (CoDIT)*, Le Cnam, Paris, France, IEEE, pp. 1699–1704. doi: [10.1109/CoDIT.2019.8820602](https://doi.org/10.1109/CoDIT.2019.8820602).
- Kapellmann-Zafra, D., Leong, R., Sistrunk, C., Proska, K., Hildebrandt, C., Lunden, K. and Brubaker, N.** (2022) 'INDUSTROYER.V2: Old malware learns new tricks', *MANDIANT Blog*, 25 April. Available at: <https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks> (Accessed: 31 March 2023).
- Khan, R., Maynard, P., McLaughlin, K., Laverty, D. and Sezer, S.** (2016) 'Threat analysis of BlackEnergy malware for synchrophasor based real-time control and monitoring in smart grid', in *Proceedings of the 4th international symposium for ICS & SCADA cyber security research 2016*, pp. 53–63. doi: [10.14236/ewic/ICS2016.7](https://doi.org/10.14236/ewic/ICS2016.7).
- Kim, B., Alawami, M.A., Kim, E., Oh, S., Park, J. and Kim, H.** (2023) 'A comparative study of time series anomaly detection models for industrial control systems', *Sensors*, 23(3), 1310. doi: [10.3390/s23031310](https://doi.org/10.3390/s23031310).
- Kleinmann, A., Amichay, O., Wool, A., Tenenbaum, D., Bar, O. and Lev, L.** (2018) 'Stealthy deception attacks against SCADA systems', in Katsikas, S.K., Cuppens, F., Cuppens, N., Lambrinouidakis, C., Kalloniatis, C., Mylopoulos, J., Anton, A. and Gritzalis, S. (eds.), *Computer security. SECPRE CyberICPS 2017, lecture notes in computer science, 10683*. Cham: Springer, pp. 93–109. doi: [10.1007/978-3-319-72817-9\\_7](https://doi.org/10.1007/978-3-319-72817-9_7).
- Knapp, E.D. and Langill, J.T.** (2015) 'Industrial cyber security history and trends', in Knapp, E.D. and Langill, J.T. (eds.), *Industrial network security*, 2nd edn. Boston, MA: Syngress, Chap. 3, pp. 41–57.

**Kovacs, E.** (2018) 'Triton malware linked to Russian government research institute', *SecurityWeek*, 23 October. Available at: <https://www.securityweek.com/triton-malware-linked-russian-government-research-institute> (Accessed: 24 October 2022).

**Krotofil, M., Larsen, J. and Gollmann, D.** (2015) 'The process matters: Ensuring data veracity in cyber-physical systems', in *ASIA CCS '15: Proceedings of the 10th ACM symposium on information, computer and communications security*, Association for Computing Machinery, New York, NY, pp. 133–144. doi: [10.1145/2714576.271459](https://doi.org/10.1145/2714576.271459).

**Kumar, R., Narra, B., Kela, R. and Singh, S.** (2022) 'AFMT: Maintaining the safety-security of industrial control systems', *Computers in Industry*, 136, 103584. doi: [10.1016/j.compind.2021.103584](https://doi.org/10.1016/j.compind.2021.103584).

**Langner, R.** (2013) *To kill a centrifuge—A technical analysis of what Stuxnet's creators tried to achieve*. The Langner Group, Hamburg. Available at: <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf> (Accessed: 2 December 2022).

**Lee, R.M., Assante, M.J. and Conway, T.** (2014) *German steel mill cyber attack, ICS: Defense use case*. SANS Industrial Control Systems, Rockville, MD. Available at: [https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltc79a41dbf7d1441e/607f235775873e466bcc539c/ICS-CPPE-case-Study-2-German-Steelworks\\_Facility.pdf](https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltc79a41dbf7d1441e/607f235775873e466bcc539c/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf) (Accessed: 2 December 2022).

**Lee, R.M., Assante, M.J. and Conway, T.** (2016) *Analysis of the cyber attack on the Ukrainian power grid: Defense use case*. SANS Industrial Control Systems. Available at: [https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_5.pdf](https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf) (Accessed: 2 December 2022).

**Lin, Z. and Pearson, S.** (2018) *An inside look at industrial ethernet communication protocols*. Texas Instruments. Available at: <https://www.ti.com/lit/wp/spry254b/spry254b.pdf?ts=1693988436464> (Accessed: 12 December 2022)

**Liu, Y., Ning, P. and Reiter, M.K.** (2011) 'False data injection attacks against state estimation in electric power grids', *ACM Transactions on Information and System Security* 14(1), pp. 1–33. doi: [10.1145/1952982.1952995](https://doi.org/10.1145/1952982.1952995).

**Mitchell, R.W.** (2003) *PROFIBUS: A pocket guide*. Pittsburgh, PA: International Society of Automation, pp. 1–20.

**Modbus Organization Inc.** (2012) *MODBUS application protocol specification V1.1b3*. Available at: [https://modbus.org/docs/Modbus\\_Application\\_Protocol\\_V1\\_1b.pdf](https://modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf) (Accessed: 11 December 2022).

**National Institute of Standards and Technology** (n.d.) *Official common platform enumeration (CPE) dictionary, national vulnerability database*. Available at: <https://nvd.nist.gov/products/cpe> (Accessed: 23 January 2023).

**Paganini, P.** (2019) *Duqu 2.0: The most sophisticated malware ever seen*. Malware analysis. Infosec Resources, Madison, WI. Available at <https://resources.infosecinstitute.com/topic/duqu-2-0-the-most-sophisticated-malware-ever-seen/> (Accessed: 31 March 2023).

**Pei, C., Xiao, Y., Liang, W. and Han, X.** (2018) 'Trade-off of security and performance of lightweight block ciphers in industrial wireless sensor networks', *EURASIP Journal on Wireless Communications and Networking*, 117(2018), pp. 1–18. doi: [10.1186/s13638-018-1121-6](https://doi.org/10.1186/s13638-018-1121-6).

**Policja.pl** (2008) '14-latek przestawiał zwrotnice', 09 January. Available at: <https://policja.pl/pol/aktualnosci/13278,14-latek-przestawial-zwrotnice.html> (Accessed: 20 February 2023).

**Przetacznik, J. and Tarpova, S.** (2022) *Russia's war on Ukraine: Timeline of cyber-attacks*. Briefing PE 733.549. Brussels: European Parliamentary Research Service.

**Repository of Industrial Security Incidents (RISI)** (2015) *The repository of industrial security incidents*. Available at: <https://www.risidata.com/> (Accessed: 13 October 2022).

**Slay, J. and Miller, M.** (2008) 'Lessons learned from the Maroochy water breach', in Goetz, E. and Sheno, S. (eds.), *Critical infrastructure protection*. Boston, MA: Springer, pp. 73–82. doi: [10.1007/978-0-387-75462-8\\_6](https://doi.org/10.1007/978-0-387-75462-8_6).

**Slowik, J.** (2021) 'The baffling berserk bear: A decade's activity targeting critical infrastructure, report', *Virus Bulletin Conference* October 2021. Available at: <https://vblocalhost.com/uploads/VB2021-Slowik.pdf> (Accessed: 14 December 2022).

**Soltero, M., Zhang, J., Cockril, C., Zhang, K., Kinnaird, C. and Kugelstadt, T.** (2002) *RS-422 and RS-485 standards overview and system configurations*. Texas Instruments, pp. 3–12. Available at: <https://www.ti.com/lit/an/slla070d/slla070d.pdf?ts=1693930089541> (Accessed: 6 September 2023).

**Spurgeon, C.E.** (2000) 'The evolution of ethernet', in Stone, M. and Toporek, C. (eds.) *Ethernet: the definitive guide*. Sebastopol, CA: O'Reilly& Associates, pp. 3–22.

**Stewart, J.** (2010) 'BlackEnergy version 2 threat analysis', *Secure works: Threat intelligence research*, 3 March. Available at: <https://www.secureworks.com/research/blackenergy2> (Accessed: 24 March 2023).

**Taherdoost, H.** (2022) 'Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview', *Electronics* 11(14), pp. 1–20. doi: [10.3390/electronics11142181](https://doi.org/10.3390/electronics11142181).

**Trend Micro Inc.** (2016) *Malware discovered in German nuclear power plant*. Available at: <https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/malware-discovered-in-german-nuclear-power-plant> (Accessed: 8 March 2023).

**Viasat Inc.** (2022) 'KA-SAT network cyber attack overview', *Viasat Corporate News*, 30 March. Available at: <https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview> (Accessed: 20 October 2022).

**Williams T.J.** (1994) 'The Purdue enterprise reference architecture', *Computers in Industry*, 24(2), pp. 141–158. doi: [10.1016/0166-3615\(94\)90017-5](https://doi.org/10.1016/0166-3615(94)90017-5).

**Yask and Kumar, B.S.** (2019) 'A review of model on malware detection and protection for the distributed control systems (industrial control systems) in oil & gas sectors', *Journal of Discrete Mathematical Sciences and Cryptography* 22(4), pp. 531–540. doi: [10.1080/09720529.2019.1642623](https://doi.org/10.1080/09720529.2019.1642623).