SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

Estimating the vulnerability of industrial network infrastructure in Central and Eastern Europe

Mateusz Grzegorz Twardawa[1], Marek Smolik[2], Franciszek Rakowski[3], Jakub Kwiatkowski[4], Norbert Meyer[5]

[1]mtwardawa@man.poznan.pl

[1]https://orcid.org/0000-0003-0661-0128

[3]https://orcid.org/0000-0001-6133-8900

[4]https://orcid.org/0000-0001-7000-3862

[5]https://orcid.org/0000-0003-4020-5329

[1,4]ICT Security Department, Poznan Supercomputing and Networking Center (PSNC), affiliated to the Institute of Bioorganic Chemistry of the Polish Academy of Sciences, Jana Pawła II 10, 61-139, Poznań, Poland

[1,4]Institute of Computing Science, Poznań University of Technology, Piotrowo 2, 60-965, Poznań, Poland

[2]Chief Technology Officer, ICsec S.A., Wichrowa 1A, 60-449, Poznań, Poland

[3]Research and Development, Department, ICsec S.A., Wichrowa 1A, 60-449, Poznań, Poland

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

Abstract

Industrial infrastructure has suffered an unprecedented number of attacks in Central and Eastern Europe (CEE). This situation can be attributed to many geopolitical factors, including hybrid military conflicts and criminal activity. Industrial networks belonging to

Article info
Received: 28 December 2023
Revised: 14 June 2024
Accepted: 21 June 2024
Available online: 3 August 2024

Citation: Twardawa, M.G., Smolik, M., Rakowski, F., Kwiatkowski, J. and Meyer, N. (2024) 'Estimating the vulnerability of industrial network infrastructure in Central and Eastern Europe', *Security and Defence Quarterly*, 47(3), doi: 10.35467/sdq/190350.

the countries that were once under Soviet influence suffer from an elevated risk of cyberattacks. The goal of this work is to propose an easy way to estimate the vulnerabilities of industrial networks to cyber threats on a national level. Since analysis of the industrial vulnerability landscape is difficult, this study proposes an assessment based on the popularity of vulnerable technologies—VP_c. This metric is composed of search volume data on keywords related to industrial network technologies and reported security vulnerabilities associated with these words. Data on 116 keywords was analysed and a country-specific VP_c index was calculated for twenty states in CEE. The analysis of the popularity of industrial technologies and vendors in CEE reveals interesting information about the industrial security and vulnerability landscape. The results show that some countries (e.g. Estonia) have more resilient industrial infrastructure than others (e.g. Belarus). The results presented in this study are not in conflict with other data and estimation attempts, including the National Cyber Security Index (NCSI). As new vulnerabilities are noted every day, the industrial security landscape changes rapidly. Therefore, a new easy-to-use metric (VP_c) can be successfully used for general estimations. This work shows that the VP_c score agrees with other estimates and analyses, but as with any other general estimation tool, it must be used with caution.

Keywords

critical infrastructure, network security, cyberattack, industrial control systems, national vulnerability

Introduction

Industrial Control Systems (ICSs) are essential for modern life, as they provide automation in manufacturing, healthcare, transportation, and many other economic and industrial sectors, including critical infrastructure. Cyberattacks on power stations, water treatment facilities, or chemical plants can cause major incidents, ranging from power outages to explosions and massive ecological disasters. Moreover, ICSs are important military targets, as they are part of critical and industrial infrastructure.

After the collapse of the Union of Soviet Socialist Republics (USSR), some Central and Eastern European (CEE) countries underwent fast investment programmes, while others suffered from slow periods of growth and recessions (for more details, see: Stout and Williams, 1995; Walker, 2019). Concurrently in the 1990s and 2000s, Internet-related technologies were on the rise, including advancements in ICS technology. Consequently, CEE was diversified as a region in terms of industrial digitalisation and overall economic progress (Chataway, 1999; Filippov, 2010; Kelly *et al.*, 2017).

The Internet dramatically transformed the threat landscape for industrial systems for the following reasons. Firstly, the knowledge that was previously limited to small groups of specialists and engineers could now be accessed and spread publicly, rendering the so-called ‘security by obscurity’ ineffective (Alcaraz *et al.*, 2012, pp. 120–149). Secondly, since more and more internal networks and computer stations were connected to the Internet, as a consequence some ICSs were no longer operating in isolation (Alexopoulos *et al.*, 2018). For example, the Iranian attack on the New York Dam in 2013 was executed remotely, because the floodgate control system was accessible from the hacked computer (United States District Court, Southern District of New York, 2016). Thirdly, if a vulnerability of industrial standard, device, or protocol is discovered, this knowledge spreads rapidly (Stellios *et al.*, 2019). This creates an enormous advantage for the attackers, as updates of industrial systems often require planning and maintenance breaks. Moreover, device replacement in industrial systems is expensive, so it rarely occurs. It is estimated that a typical device in ICS is exploited for 20 years (controllers), but the security of industrial devices is thought to be obsolete after several years (Bryes, 2013).

There are many threats that can harm CEE industrial infrastructure. The most notable are insiders, cyber gangs, and state-sponsored groups. Insiders are familiar with industrial processes and infrastructure and are able to obtain authorised access to an industrial system. It can be a present or former employee that uses his or her knowledge and privileges to spy, sabotage, or damage an industrial system. Such incidents may be severe and seem to be the most difficult ones to prevent. Nonetheless, being aware of vulnerabilities and eliminating them should make insider threats mitigate the impact (Marco *et al.*, 2021). Ransomware attacks are common acts of cybercrime performed by financially motivated criminal groups that concern critical and industrial infrastructure without exception (Gazzan and Sheldon, 2023). Cyber gangs, however, rarely attack the ICS itself; instead, their attention is focused on related enterprise Information technology (IT) networks. For example, in 2022, incidents involving new ransomware called "Prestige" were reported in Ukraine and Poland, which targeted logistics industries and transportation, including railways (Microsoft, 2022). This malicious cyber activity was likely linked to Russia, since it was focused on important objectives from a military perspective. In fact, state-sponsored attacks in CEE are the most dangerous threats for industrial infrastructure (European Union Agency for Cybersecurity [ENISA], 2022). One of the most notorious acts of cyber terrorism happened on 23 December 2015 in Ukraine and was prepared and executed by the Sandworm Team, a Russian cyber military GRU unit. The attack was sophisticated, and disabled a power grid in numerous stages. The incident resulted in a blackout lasting 6 h, affecting more than 230 thousand people (Lee *et al.*, 2016).

Tracking the state of industrial cybersecurity is a crucial task that could help to supervise and facilitate the elimination of old and vulnerable technology from use. However, the general vulnerability of industrial systems in each country is difficult to assess. Industrial infrastructure is diversified between regions, varies in industrial sectors, and applies multiple standards. Nonetheless, some information can be gathered to create a general estimation. It can be assumed that popular and widespread technologies are visible in online search data, since many people learn how to operate and maintain them. Moreover, it seems reasonable for malicious actors to target known and existing vulnerabilities, especially if affected technology is popular (Li and Liu, 2021). Due to many aspects, such as market shares of companies, historical background, geography, activity in specific industrial sectors, standards and technological solutions, the popularity of specific elements of industrial infrastructure, may differ from region to region.

The main goal of this work is to develop and test an indirect and objective metric that is able to accurately estimate the state of national industrial cybersecurity. The metric should also be easy to calculate and do not rely on additional extensive data collection, such as field studies or surveys. Therefore, it can be easily deployed to measure, monitor, and compare national vulnerability to cyberattacks on industrial infrastructure.

The idea presented in this paper shows that it is possible to estimate the state of national industrial cybersecurity based on combined analysis of online search data and an industrial vulnerability database. The new metric proposed in this work assesses national interest in vulnerable technologies and can be calculated based on publicly available information. The analysis was performed for search terms that are divided into three categories: Programmable Logic Controllers (PLCs), vendors, and industrial communication protocols. Since data for the Russian Federation was inaccessible, 20 CEE countries were examined during this study. In order to validate the estimations obtained, the results were compared with the National Cyber Security Index (NCSI, n.d.) and Global Cybersecurity Index (GCI) (International Telecommunication Union, 2020), which served as a reference.

Methods

This study attempts to estimate the industrial vulnerability landscape in CEE by a new proposed metric, that is, the popularity of vulnerable technologies. This metric describes national interest in technologies that have known security concerns. Calculations were carried out for 20 countries that are commonly known to be a part of CEE: Albania, Belarus, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Estonia, Germany, Hungary, Latvia, Lithuania, North Macedonia, Moldova, Montenegro, Poland, Romania, Serbia, Slovakia, Slovenia, and Ukraine. The popularity of vulnerable technologies was estimated based on the Google Keyword Planner (Google Ads, n.d.) and the National Vulnerability Database (NVD) (National Institute of Standards and Technology [NIST], n.d.). Since Google does not provide data about the volume of the searched terms for Russia, this country was omitted from the analysis.

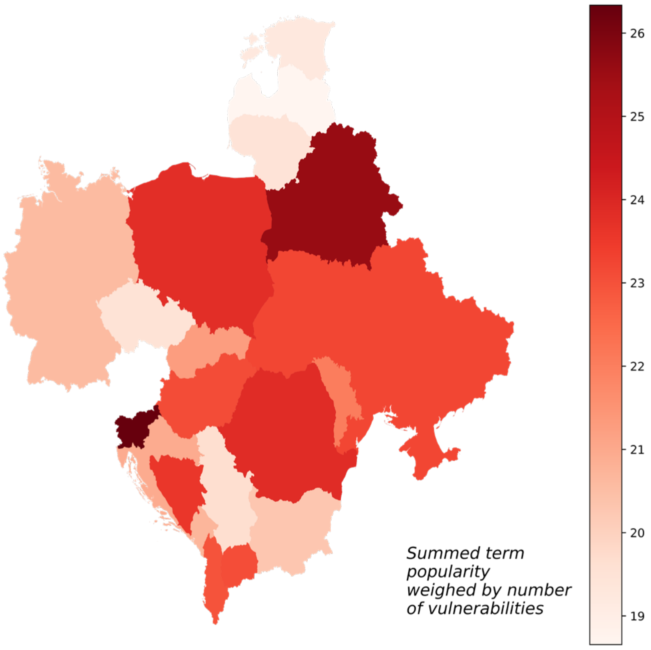
The estimation of national interest in vulnerable technologies was performed by juxtaposing the popularity (volume) of search terms obtained from Google Keyword Planner (Google Ads, n.d.) with a number of vulnerabilities associated with the term or search phrase listed in the NVD provided by the NIST (n.d.). The analysis was based on 116 search phrases divided into three categories: companies (i.e. industrial vendors and manufacturers) with fifty-nine search terms, PLCs and related equipment with forty-four entries, and industrial communication protocols with thirteen phrases. The keywords included in the study were selected based on two types of sources, the external reports on the ICS market in Europe (European Cybersecurity Organisation, 2018; Ladder Logic World, n.d.) and online product catalogues from private vendors (Aserto Sp. z o.o, n.d; ASTOR, n.d.; Sterowniki-PLC.net, n.d.). The selection procedure was supervised by industrial automation practitioners that were checking whether products mentioned in the reports were available to buy in CEE based on online catalogues. Data on search volume was collected in Google Keyword Planner for every country defined above for CEE. Since this work is focused on the present industrial vulnerability landscape, the search volume data is limited to 2022 (1 complete year). However, the number of vulnerabilities was recorded for all database entries recorded in NVD before January 2023.

The proposed metric is country-specific and can be explained as the search popularity of terms related to industrial technologies weighted by the associated number of vulnerabilities. For each country, search volume data on terms of interest was collected from Google Keyword Planner. The values obtained were later transformed with a decimal logarithm and normalised according to the highest search volume value observed for each individual country. The data obtained from NVD on the number of vulnerabilities also underwent transformation with a common logarithm and was later normalised to a range of [0,1]. The final values for every search term were calculated for all analysed countries separately as a sum of derived logarithmised search volumes multiplied by their respective logarithmised and normalised vulnerabilities count. The procedure is expressed by the following Equation 1:

$$VP_c = \sum_{i=1}^{n} \left(\frac{log_{10}(p_i)}{log_{10}(p_{c_{max}})} \times \frac{log_{10}(v_i)}{log_{10}(v_{max})} \right)$$

where VP_c stands for summed term popularity weighed by the associated number of vulnerabilities for a given country c, n is the total number of analysed terms, p_i is the

Figure 1. Visualisation of total estimated vulnerability to cyberattacks on industrial systems in CEE. The values represented on the map are summed search term popularity multiplied by the number of known vulnerabilities found in NVD database for the same term (more details in the text).



popularity of *i*th term, $p_{c_{max}}$ relates to the highest country-specific search volume, v_i represents the number of vulnerabilities associated with the *i*th term, and $v_{\max}$ is the highest number of vulnerabilities seen in the whole dataset.

Results for all terms, as well as for distinguished categories, have been visualised on maps. The first visualisation takes all the data into account (Figure 1), the second is created for companies (Figure 2), the third for PLC-related terms (Figure 3), and the last one for industrial protocols (Figure 4). The detailed values of summed search term popularity multiplied by the number of known vulnerabilities, that is, $VP_{c,}$ are also included in Table 1 for clarity. Additionally, Table 1 contains reference values obtained from the NCSI (n.d.) project website and GCI (International Telecommunication Union, 2020). Data used to calculate VP_c scores (exact keywords with national search volume and associated number of vulnerabilities for each country) was added to the supplementary file (Table S1).

In order to compare VP_c results with a reference, three values from the NCSI project were used: NCSI, Digital Development Level (DDL), and the difference between the NCSI and DDL for every country analysed in this work. For the same reason, the main GCI score was analysed. VP_c scores were compared with values provided by the NCSI project and GCI by Spearman correlation on ranks.

Results

The analysis performed in this study shows that the VP_c score agrees with expectations and external reference indexes (NCSI and GCI). The results presented in this work point out the relevancy of the VP_c score, although the metric is not flawless and the least expected cases are described in detail below.

As for all terms, the highest total VP_c score was detected for Slovenia and Belarus (see Figure 1). A little lower, but high values, nevertheless, were calculated for Albania, Bosnia

Figure 2. Visualisation of estimated vulnerability to cyberattacks on industrial systems related to vendors and specialised companies in CEE. The values represented on the map are summed search term popularities multiplied by the number of known vulnerabilities in the NVD database for the same term (more details in the text).

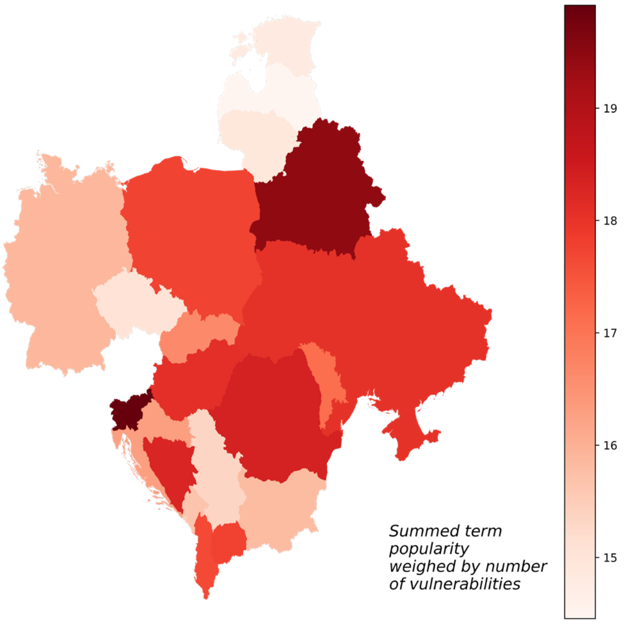
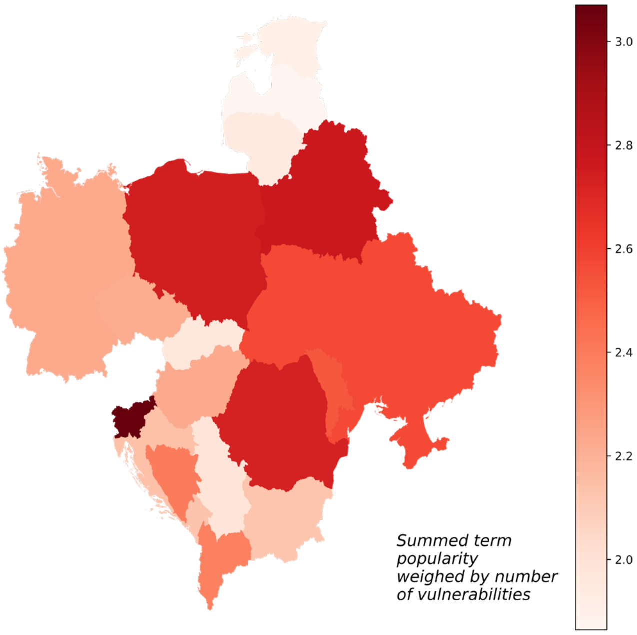
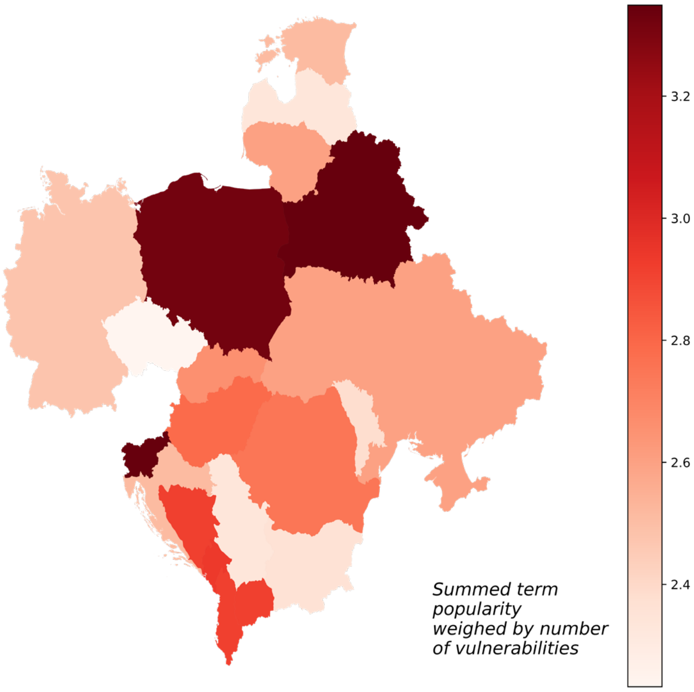


Figure 3. Visualisation of estimated vulnerability to cyberattacks on industrial systems in CEE related to PLCs and industrial equipment. The values represented on the map are summed search term popularities multiplied by number of known vulnerabilities in the NVD database for the same term (more details in text).



and Herzegovina, Hungary, North Macedonia, Poland, Romania, and Ukraine. On the other side, Czech Republic, Estonia, Latvia, Lithuania, and Serbia had the lowest total VP_c scores. Since terms related to vendors and companies dominated the keyword dataset, similar results were observed for this category. All details are seen in Figure 2 and Table 1.

Figure 4. Visualisation of estimated vulnerability to cyberattacks on industrial systems in CEE related to industrial network protocols. The values represented on the map are summed search term popularities multiplied by the number of known vulnerabilities in the NVD database for the same term (more details in text).



According to Table 1 and the visualisation on Figure 3, for PLC and related equipment, the most vulnerable infrastructure seems to be in Slovenia, Belarus, Poland, and Romania. In addition to that, Moldova and Ukraine also have scores that can be classified as elevated. Some countries score low in the PLC category, that are, Estonia, Latvia, Lithuania, Serbia, and Slovakia. The last analysed group contained terms related to industrial communication protocols and are given in Figure 4. The highest scores in this category were calculated for Belarus, Poland, and Slovenia. High values for industrial protocols were also observed for Albania, Bosnia and Herzegovina, Montenegro, and North Macedonia. In contrast, Bulgaria, Czech Republic, Latvia, Moldova, and Serbia have the lowest VP_c score values for terms related to industrial protocols.

Estimation is split into three search term categories: vendors and companies, PLCs and industrial equipment, and industrial network protocols. A column with respective total values (the sum of all categories) is also included. The NCSI, DDL, and the difference between them, as well as GCI in the last column, serve as reference values for VP_c and originate from the NCSI (n.d.) project website and International Telecommunication Union (2020) report. Colours are used to show the similarities of VP_c scores to NCSI and GCI reference. Red represents the presence of insecure infrastructure in a given country. Red is associated with high VP_c scores and low values of NCSI parameters. Low VP_c scores and high values from NCSI are marked in blue and correspond to national cybersecurity being in a good state.

The results of Spearman correlation show that a significant relationship exists between total VP_c and NCSI ($\rho = -0.4712$ and p-value = 0.036). DDL ($\rho = -0.3669$ and p-value = 0.1115), and the difference between NCSI and DDL ($\rho = -0.2706$ and p-value = 0.2484) do not possess detectable correlations with the total VP_c score. The correlation between NCSI and total VP_c is moderate but clear. The case for GCI seems to be similar.

Table 1. Summed logarithmised term popularity weighed by logarithmised number of vulnerabilities (calculated according to Equation 1) for each country in CEE.

Country	Summed term popularity weighed by number of vulnerabilities (VP_c)				National Cyber Security Index (NCSI)	Digital Development Level (DDL)	NCSI and DDL Difference	GCI
	Vendors and Companies	PLCs	Industrial Protocols	Total				
Albania	17.66	2.38	2.91	22.95	62.34	48.74	13.6	64.32
Belarus	19.46	2.77	3.35	25.58	53.25	62.33	-9.08	50.57
Bosnia and Herzegovina	18.28	2.40	2.91	23.59	28.53	49.31	-20.78	29.44
Bulgaria	15.81	2.12	2.36	20.30	74.03	62.06	11.97	67.38
Croatia	16.31	2.14	2.51	20.96	83.12	64.63	18.49	92.53
Czechia	15.07	2.22	2.23	19.52	92.21	69.21	23	74.37
Estonia	14.84	1.91	2.51	19.26	93.51	75.59	17.92	99.48
Germany	15.89	2.23	2.48	20.60	90.91	80.01	10.9	97.41
Hungary	18.09	2.23	2.79	23.11	67.53	64.25	3.28	91.28
Latvia	14.46	1.86	2.34	18.66	75.32	66.23	9.09	97.28
Lithuania	14.94	1.95	2.60	19.49	93.51	67.34	26.17	97.93
Moldova	17.12	2.53	2.38	22.03	50.65	56.79	-6.14	75.78
Montenegro	15.65	2.13	2.94	20.72	35.06	57.79	-22.73	53.23
North Macedonia	17.78	2.38	2.91	23.07	55.84	55.36	0.48	89.92
Poland	17.75	2.74	3.32	23.81	87.01	65.03	21.98	93.86
Romania	18.38	2.73	2.75	23.86	89.61	59.84	29.77	76.29
Russia	-	-	-	-	71.43	65.12	6.31	98.06
Serbia	15.35	1.99	2.34	19.67	80.52	59.81	20.71	89.8
Slovakia	16.65	1.97	2.66	21.28	83.12	65.44	17.68	92.36
Slovenia	19.92	3.07	3.35	26.34	59.74	69.74	-10	74.93
Ukraine	18.06	2.57	2.60	23.23	75.32	55.96	19.36	65.93

The correlation between GCI and VP_c is comparable to the results obtained for the NSCI scores ($\rho = -0.4827$ and p-value = 0.0311). It is worth noting that NCSI scores and GCI are more correlated with each other than with VP_c. The relationship between NCSI and GCI is strongest in this data ($\rho = 0.7196$ and p-value = 0.0003). Nevertheless, it was not expected that industrial cybersecurity would reflect the IT one. In conclusion, the VP_c score seems to be a promising estimation for the national industrial vulnerability landscape and could be adopted by security monitoring agencies.

Discussion

There are many general measures and indicators for assessment of regional cybersecurity conditions. Such measures are used by various institutions, such as public agencies and private companies. In general, three main types of indicators commonly used in cybersecurity are distinguished, that is, marker-, survey- and expert-based, each with its own set of advantages and disadvantages.

Marker-based indicators rely on specific measurable events or artefacts within the system, such as the number of instances of detected malware, frequency of unauthorised access attempts, and patch management statistics. In fact, the VP_c score is another marker-based indicator, since it relies on statistical data of a number of vulnerabilities and keyword search popularity, all of which is assumed to be correlated with the state of industrial cybersecurity. There are some advantages associated with these types of indicators. One of the most important advantages is that marker-based measures are easily deployed objective methods for assessing cybersecurity situations. These indicators provide quantifiable data that allows comparison and tracking over time, which is important for bias elimination. Marker-based indicators are also easy to automate. For the VP_c score, it is possible to create a simple online data analyser that presents current and past values without any additional manual work. Another good trait of marker-based indicators is that they can be tuned or redesigned to track very specific security aspects, for example, the VP_c score can be easily adapted to focus on different regions or sets of technologies. Nonetheless, there are some major disadvantages to the metric-based approach. One of the most important drawbacks is issues related to interpretation struggles. It is a common case that a high number of independent variables may influence a marker value, the case for VP_c is no different. In addition to this, markers are data-dependent, so their focus is limited, based on information they encompass. Finally, although markers are usually correlated with cybersecurity state, they can become unreliable over time, especially due to new technological breakthroughs (Meland *et al*., 2021).

Survey-based indicators are most popular in the cybersecurity domain. On the one hand, surveys are able to provide more holistic views, measuring multiple security aspects. This is a highly flexible security estimation technique, since a survey can be designed to address chosen security issues. Moreover, there are aspects where surveys are the best source of information, and this is especially true for behaviour-related security assessments (Chaudhary *et al*., 2022). On the other hand, survey accuracy suffers from badly designed forms that may lead to misinterpretation and bias. In some cases, a low number or false responses may strongly influence an indicator. In fact, response rates may be subject to manipulation and artificially augmented, which can lead to misinformation. On top of that, surveys are resource-consuming, requiring time to be designed, distributed, and analysed (Cadena *et al*., 2020).

Lastly, there are expert-based indicators that are usually presented in the form of articles or reports. Experts can provide a deep, nuanced understanding of cybersecurity risks, incorporating both technical and strategic perspectives. Their experience allows potential future threats and vulnerabilities to be identified, offering predictive insights that can guide proactive measures. Experts can also consider the unique context of the organisation, including industry-specific threats and the specific operational environment. However, expert-based indicators can be affected by personal bias and subjective judgements, which undermine objectivity. Engaging experts for assessments can be expensive and time-consuming, limiting the frequency of evaluations. Finally, relying on expert assessments may not be scalable for large organisations with extensive and diverse operations, where continuous monitoring is required (Krisper *et al*., 2020).

In the report published by the European Union (EU) on cybersecurity indexes, there are at least sixty different indicators used to monitor the security state in member countries (ENISA, 2024) and all of them are marker- or survey-based. These indicators are designed to measure investment project impact based on normalised statistical data (EUROSTAT), the number of reported incidents (ENISA), legislative data (Council of Europe), and surveys filled in by companies and public institutions (MS Survey). Unfortunately, none of the indicators published in the report was strictly dedicated to industrial cybersecurity. The EU also suggested a specification based on twenty-two quality features that all reliable indicators should have. The traits of a good indicator include precision, validity, ability to systematically collect data, neutrality, and transparency (ENISA, 2024).

It is important to mention that the EU uses online device scans and statistics provided by Shodan (no date). Although this commercially available portal is valuable for regular IT cybersecurity, it is not the case for the industrial sector. Shodan scans devices connected to the Internet and reports back on non-secure entities based on defined features. Most industrial devices are, in general, isolated from the Internet and therefore unreachable for Shodan. Nonetheless, there are attackers, such as the currently common Russian hacktivists, that target industrial devices reachable online (Cybersecurity and Infrastructure Security Agency [CISA], 2024). In fact, professional hackers are able to access industrial networks by other means, for example, supply chain compromise and infected removal media.

The presented estimation of the vulnerability landscape for industrial systems in CEE is not difficult to perform, but the results rely on markers and should be interpreted with caution for the following reasons. Firstly, there are multiple causes for which certain terms are searched, even if the phrase is very specific for ICSs (e.g. RX3i). For example, the term may be googled by students, because certain technology is simply popular in educational laboratories and textbooks (Adamo *et al.*, 2007). It is possible that foreign entities may be interested in devices used in other countries. Terms may also be googled in a different context that is not related to ICSs at all. Secondly, it shall be noted that the analysis was performed using the assumption that all terms were searched in English. This may not be true in Europe, where the popularity of English language varies (Sim, 2008). Moreover, countries, such as Serbia and Ukraine, use Cyrillic script, which can cause the results to be biased. Another major issue may be the choice of search engine; this analysis assumes that Google is equally popular in complete CEE (StatCounter, n.d.). In addition to that, Google Keyword Planner is actually one of many tools used for advert placement and trend monitoring and it will never replace accuracy that can be achieved by incorporation of sales data and on-site asset stocktaking. Furthermore, it is worth noting that VP_c has a statistical character, that is, it gains accuracy and reliability when calculated on massive and diverse datasets. Therefore, relying solely on NVD may introduce additional biases. A proper index should operate on multiple data sources, especially if they originate from an area under investigation. Lastly, it is possible to carefully pick a set of terms that are capable of supporting any narrative. In fact, it would be extremely difficult to eliminate bias in any of general indexes and matrices that estimate properties of infrastructure, and VP_c is not an exemption. Nonetheless, large sets of search phases ought to be less easily manipulated (Skelly *et al.*, 2012). All the reasons listed above should be kept in mind while interpreting the VP_c score.

In general, the values of VP_c indicate national interest in vulnerable industrial technologies and may be useful for industrial security state estimation. Although the proposed VP_c metric may have some drawbacks, the obtained values of VP_c seem to be reasonable in most cases. In order to create a reference for VP_c, three additional columns are placed in Table 1, that is, the NCSI, DDL, and the difference between them. These security parameters were taken from the NCSI (n.d.) project website. NCSI data, in general, agrees with the proposed metric; however, there is a possible normalisation issue that must be mentioned. Although Slovenia was assigned a low NCSI, it has the highest VP_c score. The reason for this may be the chosen normalisation scheme that made the VP_c values strongly dependent on the highest normalised search volume of the most popular keyword. If search terms are not properly chosen, then the results can be biased. Hopefully, the risk is minimised for larger sets of search phases; nonetheless, this issue is the weakest element of the VP_c score.

The International Telecommunication Union (2020) publishes GCI, which is composed of the following five domains: legal, technical, organisational, capacity development, and cooperative. The Index is designed to measure the commitment of countries to cybersecurity at a global level based on replies to a questionnaire prepared by experts. Information on GCI values for analysed countries are mentioned in Table 1. Correlation between the VP_c and GCI values revealed the same degree of correlation between these metrics as was detected for VP_c and NCSI. This may be explained by the strong correlation between NCSI and GCI. Both of these metrics are used to assess cybersecurity states of countries suffering cyberattacks from Russia (Ukraine, Georgia, and Estonia), showing their importance as estimators of digital development (Yerina *et al*., 2021), which can also partly be reflected in the level of cyber defence ICSs.

Industrial cybersecurity assessments are dominated by expert opinions. The reports are often prepared by industrial cyber intelligence teams associated with major industrial cybersecurity solutions. Companies such as Dragos or Kaspersky prepare periodical and specialised reports that address current threats for industrial networks and major regional security issues. Unlike marker- and survey-based assessments, experts are known to express predictions and anticipations of changes in technology. For example, the operational technology (OT) cybersecurity review of 2023 published by Dragos Inc. (2024) is focused on current conflicts and new threats, rather than vulnerability assessment. Similarly, periodical expert reports on industrial cybersecurity developed by Kaspersky mainly cover new threats to ICSs (Kaspersky ICS CERT, 2024).

Finally, there are reports related to vulnerability of indusial automation technologies in CEE that can be comparted with VP_c results. According to the report about the readiness of central and eastern EU countries for Industry 4.0 (Naudé *et al*., 2019), the Czech Republic, Lithuania, Hungary, and Slovenia have the highest potential for adoption and deployment of new industrial technologies. However, Bulgaria, Slovakia, Romania, and Poland are least prepared for adoption of technologies related to Industry 4.0. These conclusions are obtained by combining the most crucial aspects of industrial transformation capacity (i.e. technological, entrepreneurial, and governance competencies). In general, the VP_c scores reflect conclusions presented in the report for six out of eight analysed countries. Not in line with the report, the VP_c values obtained for Hungary and Slovenia are higher than average. A similar argument may be made for NCSI. As mentioned before, the VP_c score for Slovenia might be biased by normalisation, but this is less likely for Hungary. Despite these differences, the conclusions in the report match with most VP_c scores, especially in the case of Poland and Romania. These countries have been estimated by VP_c as more vulnerable to cyberattacks on ICSs which was in disagreement with NCSI.

Conclusions

Many different industrial technologies exist in CEE. Regions differ in their deployment of novel technologies and there are many facilities that still operate on vulnerable devices and systems. As described in this work, the VP_c score shows the industrial vulnerability landscape for multiple countries in CEE. The VP_c score aligns with expectations and correlates with external benchmarks, such as NCSI, GCI, and EU reports. It highlights Slovenia and Belarus as having the highest/worst VP_c scores overall, with several other countries in Eastern Europe also showing elevated scores. Conversely, countries such as Czech Republic, Estonia, Latvia, Lithuania, and Serbia had the lowest VP_c scores, which can be interpreted as high cyberattack resilience in the industrial automation sector. Vulnerabilities related to PLC and industrial communication protocols were particularly notable in Slovenia, Belarus, Poland, and Romania. Statistical analysis revealed a moderate correlation between the VP_c and reference scores (NCSI and GCI), which was anticipated, since industrial cybersecurity does not have to perfectly mirror the IT one.

Based on the findings of this study, several recommendations for policymakers and investors can be derived. Firstly, there is a clear need for increased investment in industrial control and automation systems in Romania, Bosnia and Herzegovina, Albania, Bulgaria, Poland, Belarus, and Slovakia. These countries appear to rely on outdated and vulnerable technologies that require modernisation. Secondly, the Baltic states, namely Estonia, Latvia, and Lithuania, exhibit high resilience to potential cyberattacks, indicating that their defence strategies are effective and should be maintained and supported. Lastly, the VP_c measure provides insights into vendor market shares in Romania, Belarus, and Bosnia and Hercegovina, where companies with a greater number of vulnerabilities are common. VP_c can serve as a valuable tool in reports aimed at informing political decisions and guiding investment strategies. In this case, both legal and commercial actions are needed to promote trustworthy industrial vendors and standards.

Tracking general security trends in industrial infrastructure is difficult and time-consuming. VP_c is able to overcome these limitations, but at a cost associated with susceptibility to bias. Firstly, search term popularity is influenced by various non-industrial factors, such as academic or educational interest in specific technologies. Secondly, English-language dominance in search queries may overlook regional preferences, such as the use of Cyrillic script in countries such as Serbia or Ukraine, potentially skewing results. Additionally, relying solely on Google Keyword Planner may not capture the full spectrum of data, as it primarily serves advertising. Moreover, the VP_c score's statistical nature implies greater accuracy with larger and more diverse datasets, suggesting that exclusive reliance on sources such as NVD could introduce biases. To mitigate these issues, a robust index should integrate multiple data sources relevant to the specific area of investigation. Finally, careful selection of search terms is crucial to avoid bias and ensure the VP_c score's reliability in reflecting infrastructure properties. Although VP_c has many drawbacks, it can be useful as a general metric and help to track changes in national industrial cybersecurity.

Industrial infrastructure is one of the main targets in modern hybrid warfare. European countries are already suffering from intense cyberattacks from both foreign state agencies and criminal organisations. Therefore, multidimensional and complex analysis of the industrial cyber vulnerability landscape, as well as monitoring its development, is important to prepare and deploy proper defence plans (Kayan *et al.*, 2022). The VP_c score can only be a part of realistic infrastructure security assessment; however, it reveals information about general interest in vulnerable technologies. The interest itself may also point out which attacks are more (or less) likely or signal that more investments are needed to modernise and secure industrial infrastructure. In addition, the score may trigger changes in the education of skilled personnel that is essential in specific industrial sectors. It is worth noting that the VP_c score can be used by security researchers to identify and predict spreading across different countries. The VP_c score may also be deployed to plan and coordinate investments in industrial security at international (EU) level as well as regulate usage of vulnerable industrial technology and standards by law, enforcing cybersecurity standards.

Finally, the VP_c score introduced in this work should be validated by regional infrastructure studies. Vulnerability analysis of industrial technologies and equipment based on real inventory lists may be a better source of data. This can be achieved by modern security systems for industrial networks that are capable of inventory analysis and vulnerability detection, such as the SCADvanceXP (Twardawa *et al.*, 2024). Future work on the VP_c score should also improve scaling and the normalisation procedure. For example, creating a list of referential and validated search terms may to a large extent eliminate the problem of wrong scaling of search volume. Additional effort should also be made to take into account search phrases in the official language of each analysed country. Nevertheless, the VP_c score has a great potential for studying regional industrial infrastructure vulnerability to cyberattacks.

Funding

This research received no external funding.

Author Contributions

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

Data Availability Statement

Data is contained in supplementary materials.

Disclosure statement

Marek Smolik reports a relationship with ICsec S.A. that includes board membership and employment. Franciszek Rakowski reports a B2B cooperation with ICsec S.A. ICsec S.A. offers the SCADvanceXP system, which is an IDS for industrial control systems. The authors obtained copyright permission for the maps and images published in the paper. All images and maps were created by the authors based on publicly available data.

References

Adamo, F., Attivissimo, F., Cavone, G. and Giaquinto, N. (2007) 'SCADA/HMI systems in advanced educational courses'*, IEEE Transactions on Instrumentation and Measurement,* 56(1), pp. 4–10. doi: 10.1109/TIM.2006.887216.

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_7.

Alexopoulos, K., Koukas, S., Boli, N. and Mourtzis D. (2018) 'Architecture and development of an industrial internet of things framework for realizing services in industrial product service systems', *Procedia CIRP*, 72, pp. 880–885. doi: 10.1016/j.procir.2018.03.152.

Aserto Sp. z o.o. (n.d.) *Optiba – sklep online*. Available at: https://optiba.com/automatyka-przemyslowa-i-elektrotechnika (Accessed : 21 March 2023).

ASTOR (n.d.) *ASTOR online shop.* Available at: https://www.astor.com.pl/sklep/ (Accessed: 21 March 2023).

Bryes, E. (2013) '*Rip and replace*' *approach to SCADA security is unrealistic.* Available at: https://www.tofinosecurity.com/blog/%E2%80%9Crip-and-replace%E2%80%9D-approach-scada-security-unrealistic (Accessed: 27 September 2023).

Cadena, A., Gualoto, F., Fuertes, W. Tello-Oquendo, L., Andrade, R., Tapia Leon, F. and Torres J. (2020) 'Metrics and indicators of information security incident management: A systematic mapping study', in Rocha A. and Pacheco Pereira R. (eds.) *Smart innovation, systems and technologies.* Singapore: Springer Nature, pp. 507–519. doi: 10.1007/978-981-13-9155-2_40.

Chataway, J. (1999) 'Technology transfer and the restructuring of science and technology in central and eastern Europe', *Technovation*, 19(6–7), pp. 355–364. doi: 10.1016/S0166-4972(99)00029-2.

Chaudhary, S., Gkioulos, V. and Katsikas, S. (2022) 'Developing metrics to assess the effectiveness of cybersecurity awareness program', *Journal of Cybersecurity*, 8(1), tyac006. doi: 10.1093/cybsec/tyac006.

Cybersecurity and Infrastructure Security Agency (CISA) (2024) *Defending OT operations against ongoing pro-Russia hacktivist activity.* Available at: https://www.cisa.gov/resources-tools/resources/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity (Accessed: 13 June 2024).

Dragos Inc. (2024) *OT cybersecurity – the 2023 year in review.* Available at: https://www.dragos.com/ot-cybersecurity-year-in-review/ (Accessed : 14 June 2024).

European Cybersecurity Organisation (2018) *Industry 4.0 and ICS sector report: Cyber security for the industry 4.0 and ICS sector, WG3 I sectoral demand*. Available at: https://ecs-org.eu/ecso-uploads/2022/10/5fdb2628a0318.pdf (Accessed: 21 March 2023).

European Union Agency for Cybersecurity (ENISA) (2022) *ENISA threat landscape 2022*. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (Accessed: 28 September 2023).

European Union Agency for Cybersecurity (ENISA) (2024) *EU cybersecurity index – Framework and methodological note*. Available at: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/eu-cybersecurity-index/eu_csi_methodological_note_v1-0.pdf (Accessed: 13 June 2024).

Filippov, S. (2010) 'Central and Eastern Europe: Innovation-led transition', *Problemy Eksploatacji*, 3, pp. 139–148.

Gazzan, M. and Sheldon, F.T. (2023) 'Opportunities for early detection and prediction of ransomware attacks against industrial control systems', *Future Internet*, 15, p. 144. doi: 10.3390/fi15040144.

Google Ads (n.d.) *Keyword planner.* Available at: https://ads.google.com/home/tools/keyword-planner/ (Accessed: 21 March 2023).

International Telecommunication Union (2020) *Global cybersecurity index—Measuring commitment to cybersecurity*. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (Accessed: 13 June 2024).

Kaspersky ICS CERT (2024) *Threat landscape for industrial automation systems. Q1 2024*. Available at: https://ics-cert.kaspersky.com/publications/reports/2024/05/27/threat-landscape-for-industrial-automation-systems-q1-2024/ (Accessed: 14 June 2024).

Kayan, H., Nunes, M., Rana, O., Burnap, P. and Perera C. (2022) 'Cybersecurity of industrial cyber-physical systems: A review', *ACM Computing Surveys (CSUR)*, 54(11s), Article No. 229, pp. 1–35. doi: 10.1145/351041.

Kelly, T., Liaplina, A., Tan, S.W. and Winkler, H.J. (2017) *Reaping digital dividends: Leveraging the internet for development in Europe and Central Asia.* Washington, DC: World Bank. doi: 10.1596/978-1-4648-1025-1.

Krisper, M., Dobaj, J. and Macher, G. (2020) 'Assessing risk estimations for cyber-security using expert judgment', in Yilmaz M., Niemann J., Clarke P. and Messnarz R. (eds.) *European conference on software process improvement*. New York, NY: Springer, pp. 120–134. doi: 10.1007/978-3-030-56441-4_9.

Ladder Logic World (n.d.) *PLC manufacturers: The latest PLC brands, rankings & revenues.* Available at: https://ladderlogicworld.com/plc-manufacturers/ (Accessed: 21 March 2023).

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 (Accessed: 2 December 2022).

Li, Y. and Liu, Q. (2021) 'A comprehensive review study of cyber-attacks and cyber security, emerging trends and recent developments', *Energy Reports*, 7, pp. 8176–8186. doi: 10.1016/j.egyr.2021.08.126.

Marco, G.D., Loia, V., Karimipour, H. and Siano, P. (2021) 'Assessing insider attacks and privacy leakage in managed IoT systems for residential prosumers', *Energies*, 14(9), 2385. doi: 10.3390/en14092385.

Meland, P.H., Tokas, S., Erdogan, G., Bernsmed, K. and Omerovic, A.A (2021) 'Systematic mapping study on cyber security indicator data', *Electronics*, 10(9), 1092. doi: 10.3390/electronics10091092.

Microsoft (2022) *New 'Prestige' ransomware impacts organizations in Ukraine and Poland.* Microsoft Threat Intelligence. Available at: https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/ (Accessed: 28 September 2023).

National Cyber Security Index (NCSI) (n.d.) *National Cyber Security Index*. Available at: https://ncsi.ega.ee/ncsi-index/ (Accessed: 28 September 2023).

National Institute of Standards and Technology (NIST) (n.d.) *National vulnerability database.* Available at: https://nvd.nist.gov/vuln (Accessed: 21 March 2023).

Naudé, W., Surdej, A. and Cameron, M. (2019) *The past and future of manufacturing in Central and Eastern Europe: Ready for Industry 4.0?* Report IZA DP No. 12141. Bonn: Institute of Labor Economics (IZA).

Shodan (n.d.) *Search Engine for the Internet of Everything*. Available at: https://www.shodan.io/ (Accessed: 13 June 2024).

Sim, M.A. (2008) 'Teaching English in several Central and Eastern European countries', *Annals of Faculty of Economics*, 1(1). pp. 644–648.

Skelly, A.C., Dettori, J.R. and Brodt, E.D. (2012) 'Assessing bias: The importance of considering confounding', *Evidence-Based Spine-Care Journal*, *3*(1), pp. 9–12. doi: 10.1055/s-0031-1298595.

StatCounter (n.d.) *Search engine market share in Europe.* Available at: https://gs.statcounter.com/search-engine-market-share/all/europe (Accessed: 29 September 2023).

Stellios, I., Kotzanikolaou, P. and Psarakis, M. (2019) 'Advanced persistent threats and zero-day exploits in industrial Internet of things', in Alcaraz, C. (ed.) *Security and privacy trends in the industrial internet of things. Advanced sciences and technologies for security applications*. Cham: Springer. pp. 47–68. doi: 10.1007/978-3-030-12330-7_3.

Sterowniki-PLC.net (n.d.) *Sterowniki-plc.net – sklepinternetowy.* Available at: https://sterowniki-plc.net/ (Accessed: 21 March 2023).

Stout, T.M. and Williams, T.J. (1995) 'Pioneering work in the field of computer process control', *IEEE Annals of the History of Computing*, 17(1), pp. 6–18. doi: 10.1109/85.366507.

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

United States District Court, Southern District of New York (2016) *United States of America v. Ahmad Fathi, Hamid Firoozi, Amin, Shokohi, Sadegh Ahmadzadegan a/k/a 'Nitr0jen26', Omid Ghaffarinia a/k/a 'PLuS', Sina Keissar, and Nader Saedi, a/k/a 'Turk Server'*. Indictment, 24 March, pp. 14–16. Available at: https://www.justice.gov/media/824691/dl?inline (Accessed: 27 September 2023).

Walker, S. (2019) '"This is the golden age": Eastern Europe's extraordinary 30-year revival', *The Guardian*, 26 October. Available at: https://www.theguardian.com/world/2019/oct/26/this-is-the-golden-age-eastern-europes-extraordinary-30-year-revival (Accessed: 26 September 2023).

Yerina, A., Honchar, I. and Zaiets, S. (2021) 'Statistical indicators of cybersecurity development in the context of digital transformation of economy and society', *Science and Innovation*, 17(3), pp. 3–13. doi: 10.15407/scine17.03.003.

Supplementary

Table S1. Data used to calculate VPc scores for each country. Search terms volume taken from Google Keyword Planner have been obtained for each country and transformed with decimal logaritm. Addictionaly number of vulnabilites associated with search term are provided in separated column. Information about type of keyword (company, protocol, plc) is also included.

Terms	Albania	Belarus	Bosnia and Herze-govina	Bulgaria	Croatia	Czechia	Estonia	Germany	Hungary	Latvia	Lithuania	North Mace-donia	Moldova	Montenegro	Poland	Romania	Serbia	Slovakia	Slovenia	Ukraine	Vulner-abilities	Type
3s smart software solutions gmbh	0	2	1	2	2	2	2	2	2	2	2	1	1	0	2	2	2	2	2	2	6	company
abb	3	3	3	4	4	4	4	5	4	3	4	3	2	3	4	4	3	4	3	4	921	company
ac500	2	2	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2	7	plc
adcon	2	2	2	2	3	2	2	3	2	2	2	2	2	2	3	2	2	2	2	2	48	company
adcon telemetry	2	1	2	2	2	2	1	2	2	1	1	1	1	0	2	2	2	2	2	2	5	company
advantech	2	2	2	2	2	3	2	4	3	2	2	2	2	2	3	3	2	2	2	3	211	company
ah plc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	plc
allen bradley	2	2	2	2	2	3	2	4	3	2	2	2	2	2	3	3	2	3	2	3	46	company
AS300	1	1	0	1	1	2	2	2	0	1	1	0	1	1	2	2	2	2	0	2	1	plc
axc phoenix	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	plc
b&r automation	2	2	2	2	2	3	2	4	2	2	2	2	2	1	3	2	2	2	2	2	21	company
b1 b1z	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	plc
bac net	2	2	2	2	2	2	2	3	2	2	2	2	1	1	2	2	2	2	2	2	37	protocol
beckhoff	2	2	2	2	2	3	2	5	3	2	2	2	2	2	4	3	2	3	3	2	17	company
canopen	2	2	2	2	2	2	2	4	2	2	2	2	2	2	3	2	2	2	2	2	1	protocol
carel	2	2	2	2	3	3	2	4	2	2	2	2	3	2	3	3	2	2	2	3	27	company
cc link	2	2	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2	3	protocol
cutler hammer	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	0	company
delta electronic	2	2	2	2	2	3	2	4	2	2	2	2	2	2	3	3	3	3	2	3	120	company
devicenet	2	2	2	2	2	2	2	3	2	2	2	2	2	2	3	2	2	2	2	2	3	protocol
dnp3	2	2	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2	59	protocol
dvp eh3	0	2	0	2	2	1	1	2	0	0	1	2	0	0	2	2	0	1	1	2	1	plc
dvp es2	1	2	2	2	1	1	0	2	2	1	1	0	0	0	2	2	1	2	2	2	1	plc
dvp es3	0	2	2	2	2	1	0	2	2	0	2	0	0	0	2	2	0	1	2	2	0	plc

(*Continues*)

Terms	Albania	Belarus	Bosnia and Herze-govina	Bulgaria	Croatia	Czechia	Estonia	Germany	Hungary	Latvia	Lithuania	North Mace-donia	Moldova	Montenegro	Poland	Romania	Serbia	Slovakia	Slovenia	Ukraine	Vulner-abilities	Type
dvp plc	2	2	1	1	2	2	2	2	2	2	2	2	2	1	2	2	2	1	2	2	1	plc
easye4	0	2	2	2	2	2	2	3	2	2	2	1	2	2	3	2	2	2	2	2	0	plc
eaton	2	3	2	3	3	4	3	5	4	3	3	2	2	2	4	4	3	3	3	4	40	company
emerson	2	2	2	3	3	3	3	5	4	3	3	2	2	2	4	4	3	3	3	3	69	company
emerson electric co	2	2	2	2	2	2	2	2	2	2	2	2	2	0	2	2	2	2	2	2	6	company
ethercat	2	2	2	2	2	3	2	4	3	2	2	2	2	2	3	2	2	2	2	2	2	protocol
ewon	2	2	2	2	2	2	2	3	2	2	2	2	2	2	3	2	2	2	2	2	24	company
exemys	0	0	1	1	2	2	0	2	2	0	2	1	1	0	2	1	2	2	2	2	1	company
fatek	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	2	2	2	2	2	28	company
fbs plc	0	0	1	1	2	1	0	2	1	1	0	1	0	0	2	2	2	1	1	1	0	plc
fd5 kinco	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	plc
fd5 plc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	plc
fp panasonic	0	0	0	0	1	1	0	2	0	0	0	0	0	0	2	2	0	0	1	1	7	plc
fuji electric	2	2	2	3	2	2	2	3	2	2	2	2	2	2	3	2	2	2	2	2	47	company
g7ddt11	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	1	0	0	0	plc
garrettcom	2	2	2	2	2	2	1	2	2	1	2	1	2	1	2	2	2	2	2	2	5	company
general industrial controls	0	2	0	2	2	2	1	2	1	0	2	1	0	0	2	1	1	1	0	2	0	company
glc controls inc	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	company
h hitachi	0	1	0	2	0	1	0	2	0	1	0	0	0	1	2	1	0	0	0	1	0	plc
hb1 plc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	plc
hitachi	3	3	3	4	4	4	3	5	4	3	3	3	3	2	4	4	3	4	3	4	268	company
hitachi eh	0	2	0	0	0	2	0	2	1	1	1	0	0	0	1	2	1	0	2	2	2	plc
honeywell	2	3	3	3	3	4	3	5	4	3	3	2	2	2	4	4	3	4	3	4	56	company
hospira	2	2	2	2	3	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2	17	company
ibc solar	2	2	2	2	2	3	2	4	2	2	2	2	2	2	3	2	2	2	2	2	14	company
iccp protocol	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	21	protocol

inductive automation	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	15	company
infinite automation systems	1	1	1	0	1	1	2	2	1	0	2	0	0	0	1	1	1	0	0	1	10	company
ininet solution gmbh	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9	company
juniper	3	3	3	3	3	4	3	4	4	3	3	3	3	2	4	4	3	3	3	4	928	company
juniper networks inc	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	515	company
k6 plc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	plc
kasa companies	1	0	2	1	0	1	1	2	2	1	2	2	0	0	2	2	2	1	2	2	0	company
kasa companies inc	0	0	0	1	0	0	0	2	0	0	1	1	0	0	0	1	1	0	0	1	0	company
kinco	2	2	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2	1	company
koyo	2	2	2	2	2	3	2	3	2	2	2	2	2	2	3	3	2	2	2	3	6	company
ks plc	0	0	0	0	0	1	0	1	0	0	0	0	0	0	1	2	0	0	1	0	16	plc
kv keyence	0	0	0	1	0	2	0	2	1	0	0	0	0	0	2	1	0	2	0	0	0	plc
kw plc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	plc
lx3v plc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	plc
lx5s plc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	plc
lx5v plc	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	plc
master k	2	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2	3	30	plc
melsec	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	52	plc
micrex	1	1	1	2	2	1	2	2	2	2	0	1	1	0	2	2	2	2	2	1	0	plc
mitsubishi electric corporation	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	5	company
modbus	2	3	2	3	3	3	3	4	3	2	3	2	2	2	4	3	2	3	3	3	120	protocol
modicon	2	2	2	2	2	2	2	3	2	2	2	2	2	2	3	2	2	2	2	2	139	company
motorola	3	3	3	4	4	5	3	5	4	3	3	3	3	3	4	4	4	4	3	4	87	company
moxa	2	3	2	2	2	3	2	4	3	2	2	2	2	2	4	4	2	3	3	3	241	company
omron	2	3	2	3	3	4	3	5	4	3	3	2	2	2	4	4	3	4	3	4	50	company

(*Continues*)

Terms	Albania	Belarus	Bosnia and Herze-govina	Bulgaria	Croatia	Czechia	Estonia	Germany	Hungary	Latvia	Lithuania	North Mace-donia	Moldova	Montenegro	Poland	Romania	Serbia	Slovakia	Slovenia	Ukraine	Vulner-abilities	Type
omron corporation	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	0	company
opc ua	2	2	2	2	2	3	2	4	3	2	2	2	2	2	3	3	2	2	2	3	110	plc
open automation software	1	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	24	company
pc10ac2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	plc
pc10bd14002d1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	plc
pc10bd14003d1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	plc
pc10bd16001d1	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	1	0	2	0	0	0	plc
pc10ea04001n	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	plc
pc10ed16003n	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	plc
phoenix contact	2	3	2	3	3	4	3	5	4	3	3	2	2	2	4	3	3	3	3	3	65	company
powerlink	2	2	2	2	2	2	2	3	2	2	2	2	2	2	3	2	2	2	2	2	2	protocol
profibus	2	2	2	2	2	3	2	4	3	2	3	2	2	2	4	3	2	2	2	3	11	protocol
profinet	2	2	2	2	2	3	2	4	3	2	2	2	2	2	4	3	2	3	2	2	55	protocol
rexroth	2	3	2	3	2	3	2	4	3	2	2	2	2	2	4	3	2	3	3	3	3	company
rexroth icl	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	company
rockwell automation	2	2	2	2	3	3	2	4	3	2	2	2	2	2	2	3	2	2	2	3	131	company
rs enterprises	2	2	2	2	2	2	2	2	2	1	2	1	1	0	2	2	2	2	0	2	20	company
rx3i	1	2	2	2	2	2	1	2	2	2	1	1	2	2	3	2	2	2	2	2	2	plc
sauter	2	2	2	2	2	4	2	5	3	2	2	2	2	2	2	3	2	3	3	2	6	company
scada engine	0	1	0	1	2	2	1	2	2	0	1	0	1	0	4	2	1	1	2	2	13	plc
schneider	3	3	3	4	4	4	3	5	4	3	3	3	3	2	4	4	3	4	3	4	483	company
schneider electric	3	3	3	4	4	4	3	6	4	4	3	3	3	3	2	4	4	4	3	4	472	company

sercos iii	1	2	2	2	2	2	1	2	2	2	2	1	1	2	4	2	2	2	2	2	0	protocol
simatic	2	2	2	2	2	3	2	4	2	2	2	2	2	2	2	2	2	2	2	2	239	plc
sma solar technology ag	2	2	2	2	2	2	2	4	2	2	2	2	2	2	2	2	2	2	2	2	3	company
sourcefire inc	1	0	0	1	1	2	1	2	2	1	1	1	1	1	2	1	2	0	1	2	3	company
sysmac	1	2	2	2	1	2	2	2	2	2	2	2	1	1	2	2	2	2	2	2	5	company
tase 2	1	2	1	1	2	2	2	2	2	2	2	1	0	2	2	2	2	2	2	2	62	protocol
tofino security	1	1	2	1	2	2	2	2	1	2	1	1	0	0	3	2	1	2	2	2	10	company
unitronics	2	2	2	2	2	3	2	3	3	2	2	2	2	2	0	2	3	2	3	3	5	company
v box	2	2	2	4	2	3	2	3	2	2	2	2	2	2	0	2	2	2	2	2	7	plc
v8000 keyence	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	1	plc
versamax	2	2	2	2	2	2	2	2	2	2	2	2	2	2	4	2	2	2	2	2	0	plc
wago	2	3	2	3	3	4	3	5	4	3	3	2	2	2	0	4	3	3	3	4	97	company
wecon	2	2	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2	25	company
wecon technology	0	2	0	2	2	2	1	2	2	0	2	2	1	0	2	1	2	1	2	2	6	company
westermo	2	2	2	2	2	2	2	3	2	2	2	2	1	1	0	2	2	2	2	2	11	company
x20 abb	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	plc
x90 abb	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	plc
xg5000	2	2	2	2	2	2	2	2	2	2	2	2	2	0	3	2	2	2	2	2	1	plc
yokogawa	2	2	2	2	2	3	2	4	3	2	2	2	2	2	0	3	2	2	2	3	41	company