SECURITY TRENDS & VULNERABILITIES REVIEW
INDUSTRIAL CONTROL SYSTEMS

2016

POSITIVE TECHNOLOGIES

Contents

Introduction

Industrial control systems (ICS) are part and parcel of everyday life. Large plants controlled by analogue devices are rare today. The use of automated control systems is beneficial for an enterprise both in terms of economics and efficiency. The term "industrial control system" was introduced in 1980s and automation solutions were then focused on large enterprises. However, as information technologies developed and their cost decreased, ICS became more widely used. Modern ICS are used in various spheres, from home lighting control to nuclear power plant monitoring.

A lot of computerized smart home systems are based on technologies similar to those used in industrial plants. Modern energy supply control systems (smart grids) extend industrial networks to houses and apartments. In 2014 Positive Technologies specialists published research that revealed the low security level of such systems[1].

The development of ICS as well as the frequent use of popular technologies allow an intruder to exploit vulnerabilities typical not only for ICS but also for any other Ethernet-based network infrastructures.

The current trend of integrating ICS into enterprise networks, their access to and accessibility from the global network and the possibility of their remote control contributed to the emergence and development of various malware (Stuxnet, Duqu, Flame, Havex, BlackEnergy) and completely new threats. New vulnerabilities detected in industrial equipment are published constantly. For example, research on critical vulnerabilities in CareFusion medical equipment was published recently[2]. Protection of an ICS is not easy to achieve, first of all due to the complicated organization of an industrial control system and the requirement of its continuous operation.

It is also important to highlight that governmental organizations began to pay close attention to ICS security. In Russia, new documents on ICS security were created following the adoption of "The main directions of the government policy in the security of industrial control systems for production and technological processes of critical infrastructure objects of the Russian Federation" and after publishing the president's order No. Pr-3400 "Basic principles of the policy of protecting the population of the Russian Federation and protection of critical objects and potentially harmful objects against natural, anthropogenic hazards and terroristic acts until 2020" (published 15 November 2011).

Order of the FSTEC of Russia No. 13 as of 14 March 2014, "On the adoption of the requirements to information protection of industrial control systems for production and technological processes of critical and potentially harmful objects and objects that constitute a hazard to human life and health and to the environment" was introduced to supplement existing documents related to the information infrastructure's key systems. Positive Technologies experts juxtaposed new requirements with leading foreign standards for industrial automated systems (NERC CIP, ISA/IEC 62443, NIST SP 800-82, and 800-53)[3]. Additionally, a new base of threats that includes (as its foreign analogues) vulnerabilities and threats related to ICS is now published on the FSTEC site (bdu.fstec.ru).

We should note vendors' interest in the timely detection and elimination of vulnerabilities (they apply a policy of responsible disclosure and work with security researchers). This in particular explains an almost unchanged number of detected vulnerabilities in the period from 2012 to 2015 (in contrast to studies conducted earlier).

[1] blog.ptsecurity.com/2014/07/what-is-so-dangerous-in-smart-grids
[2] ics-cert.us-cert.gov/advisories/ICSMA-16-089-01
[3] ptsecurity.ru/download/FSTEC_N31_NERK_NIST_ISA_IEC.pdf

In 2012 Positive Technologies issued an analytical report "SCADA safety in Numbers", which demonstrated that a large number of ICS components are available via the internet[4]. According to the previous research, between 2009 and 2012 the number of ICS vulnerabilities discovered during testing increased dramatically, from 9 to 192, a factor of 20.

This report summarizes available data obtained during the period from 2012 to 2015 and outlines changes. It consists of two parts and includes results of an analysis of vulnerabilities in ICS components and the frequency of their availability in the internet.

Abbreviations

OPC — open platform communications.

RTU — a remote terminal unit.

SCADA — supervisory control and data acquisition.

CWS — a computer workstation.

ICS — industrial control systems.

BACS — a building automation and control system.

PLC — a programmable logic controller.

PSP — power system protection.

DCS — a distributed control system.

RTU — a remote terminal unit (for remote access and control).

HMI — a human-machine interface.

[4] ptsecurity.com/upload/ptcom/SCADA_WP_A4.ENG.0018.01.DEC.29.pdf

1. Results

This study examines components of ICS from different vendors. In the period from 2012 to 2015, a total of 743 vulnerabilities were discovered in ICS components; most of them were detected in products from well-known companies: Siemens, Schneider Electric, and Advantech. Most vulnerabilities are of either high or medium risk (47% high, 47% medium). If we assess the level of danger of a vulnerability factoring in the likelihood that the main threats to information security can be implemented (breach of confidentiality, integrity, and availability) as a result of vulnerability exploitation then more than half of the identified vulnerabilities would have high metrics of availability violation, which plays the key role in ICS. Combined with the possibility of remote exploitation of vulnerabilities and weak authentication mechanisms, this increases the risk of an attack.

Publicly available search systems allow detecting more than 150,000 various ICS components connected to the internet (as of March, 2016). In most cases, a dictionary password was used to authorize a system. The largest number of ICS components was detected in the U.S. (43%) and Germany (12%), followed by France, Italy, and Canada.

The most internet-available components are building automation systems from Tridium (25,264), a part of the Honeywell Group, and power monitoring and control systems including photovoltaics from SMA Solar Technology (17,275).

During the research, specialists detected automated systems that controlled production processes of various enterprises, transportation systems, water and energy supply. Due to the lack of adequate protection methods, an intruder doesn't need to possess special knowledge to get access to such systems and his or her actions may lead to serious consequences.

2. Research Methodology

2.1. Research methodology for vulnerabilities in ICS components

As a basis for the study, information from publicly available sources was used, such as vulnerability knowledge bases, vendors' advisories, exploit databases and packs, scientific papers, and posts on dedicated websites[5].

The following resources were used as vulnerability knowledge bases:

- ICS-CERT (ics-cert.us-cert.gov),
- NVD (nvd.nist.gov), CVE (cve.mitre.org),
- Positive Research Center (securitylab.ru/lab),
- Siemens Product CERT (siemens.com/cert).

Vulnerability knowledge bases do not include an indication of the specialization of products. In order to define whether a product is related to ICS, a list of companies that offers solutions in the automation sphere was generated. While preparing the list, we used our specialists' expertise and experience that they obtained while providing consulting services; they also used a list of products and companies published in ICS-CERT and a number of specialized analytical resources (arcweb.com, controlglobal.com, technavio.com).

A relationship between vendors was also considered. For example, Schneider Electric acquired Invensys in 2014, so in this study all the vulnerabilities detected in Invensys components were attributed to vulnerabilities in Schneider Electric products.

[5] digitalbond.com, scadahacker.com, immunityinc.com/products/canvas, exploit-db.com, rapid7.com/db/

During the research, features of available information on vulnerabilities were also considered:

1. One of the problems of standard vulnerability description is the lack of strict rules for description of a vendor, product, and versions. For example, see CVE-2013-6030 and CVE-2014-2350 below, the description of which is written in a free-form style.

   CVE-2013-6030

   Directory traversal vulnerability on the Emerson Network Power Avocent MergePoint Unity 2016 (aka MPU2016) KVM switch with firmware 1.9.16473 allows remote attackers to read arbitrary files via unspecified vectors, as demonstrated by reading the /etc/passwd file.

   CVE-2014-2350

   Emerson DeltaV 10.3.1, 11.3, 11.3.1, and 12.3 uses hardcoded credentials for diagnostic services, which allows remote attackers to bypass intended access restrictions via a TCP session, as demonstrated by a session that uses the telnet program.

2. The number of vulnerabilities published in the CVE list (Common Vulnerabilities and Exposures) by regulators, various CERT (computer emergency response teams) and vendors does not always accurately reflect the situation. Not all of the data from the original advisory is published, and unpublished vulnerabilities might be fixed.

For example, the ICS-CERT news on fixing vulnerabilities by Honeywell contains description and references to 5 different CVE articles, while OSVDB (osvdb.org) contains a list of 24 vulnerabilities[6].

In the worst case scenario, a vendor does not consider a detected error as a vulnerability. In some cases, vendors refuse to adopt recommendations not to use standard hardcoded passwords that cannot be changed by users, or not to use remote OS commanding, or refuse to admit other errors that allow a system to be compromised and are classified by WASC (webappsec.org), OWASP (owasp.org), or CWE (cwe.mitre.org).

We assess the severity of vulnerabilities in ICS components risk levels based on the Common Vulnerability Scoring System version 2 (first.org/cvss). Qualitative assessment of a risk level is based on a type-based approach:

- 0.0 < CVSS ≤ 3.9 — low;
- 4.0 ≤ CVSS ≤ 6.9 — medium;
- 7.0 ≤ CVSS ≤ 10.0 — high.

2.2. Methods used to determine the occurrence of ICS components on the internet

To collect information on the online availability of ICS components, researchers used a passive approach only. Researchers scanned internet-accessible ports using publicly available search engines: Google, Shodan (shodan.io, icsmap.shodan.io), and Censys (scans.io, censys.io).

Once collected, the data was subjected to additional analysis to determine a relationship to ICS equipment. Positive Technologies specialists created a database of ICS identifiers, consisting of approximately 800 entries that allow interference with the product and vendors from the banner. In most cases, the protocols SNMP and HTTP/HTTPS were used because many ICS provide

[6] ics-cert.us-cert.gov/advisories/ICSA-14-352-01

convenient and easy access to HMI via HTTP/HTTPS as well as access to most network devices via SNMP. Additionally, there were a lot of identifiers for analyzing industrial protocols, such as Modbus TCP, S7, DNP3 over TCP/IP, BACnet IP, FINS.

While using passive gathering of data on the internet-availability of ICS components some limits were revealed:

- Shodan uses only a limited number of ports and it scans the internet from certain IP addresses that are sometimes added to a block list by administrators and vendors of firewalls. That is why in order to widen the analysis scope, Positive Technologies specialists used data obtained by Google and Censys.
- In some cases, it was impossible to identify a product version because the banner did not include information about software versions in use.

So the obtained information does not have the completeness that can be achieved by active scanning; however, the results are reliable and clearly show the availability of ICS components in the internet.

In order to avoid confusion, international terminology was used during the analysis of components.

3. Analysis of Vulnerabilities in ICS Components

3.1. Dynamics of detection of vulnerabilities

In total, vulnerabilities in components from approximately 500 ICS vendors were analyzed, and 743 vulnerabilities were found in all. In 2015 experts at Positive Technologies independently discovered 7 new vulnerabilities[7] (2 of them high-risk) and notified the relevant vendors.

The number of vulnerabilities detected every year between 2012[8] and 2015 remained virtually unchanged. This is the result of increased interest by vendors in addressing vulnerabilities and interacting with the security community.

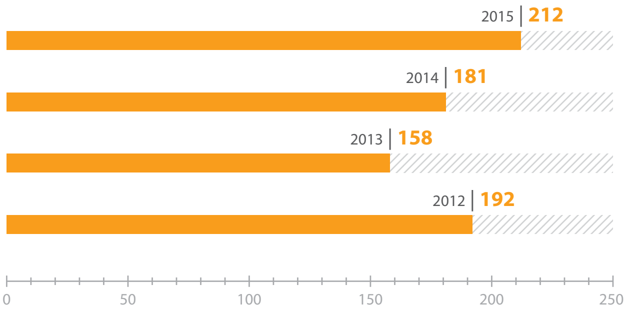

Figure 1. Total number of vulnerabilities discovered in ICS components

[7] ptsecurity.com/research/threatscape/
[8] The number of vulnerabilities presented in the 2012 report differs from the data provided now because some vulnerabilities of 2012 were published later.

3.2. The number of vulnerabilities in ICS components (by vendor)

As in 2012, vendors of the most vulnerable ICS components, in terms of the number of vulnerabilities found, are Siemens, Schneider Electric, and Advantech. The number of vulnerabilities in ICS components by vendor is presented in figure 2. The category "Other" includes 81 vendors: their products contain less than 5 vulnerabilities.

These numbers paint only a partial picture: they depend on the prevalence of the product and on whether the vendor practices responsible disclosure. Therefore these figures cannot be used to judge the degree of security of particular solutions from any particular vendor.

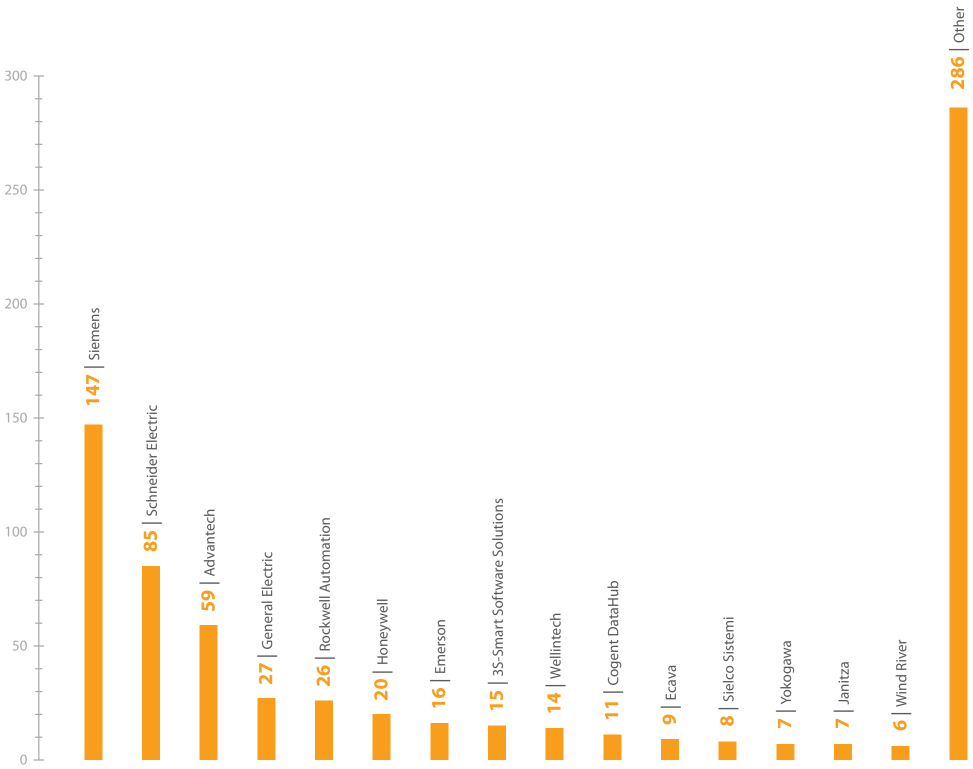

Figure 2. Number of vulnerabilities in ICS components (by vendor)

3.3. Vulnerabilities in various ICS components

Classification of ICS components is not a trivial issue. In this research, we merged types of components; however, you can get detailed classification in specialized resources, such as Control[9].

Most vulnerabilities were found in SCADA, HMI and PLC/RTU components, industrial network devices, and engineering software, which shows little change from 2012.

[9] www2.emersonprocess.com/siteadmincenter/PM%20Articles/ControlReadersChoice2014.pdf, textlab.io/doc/3540422/controlreaderschoice2015

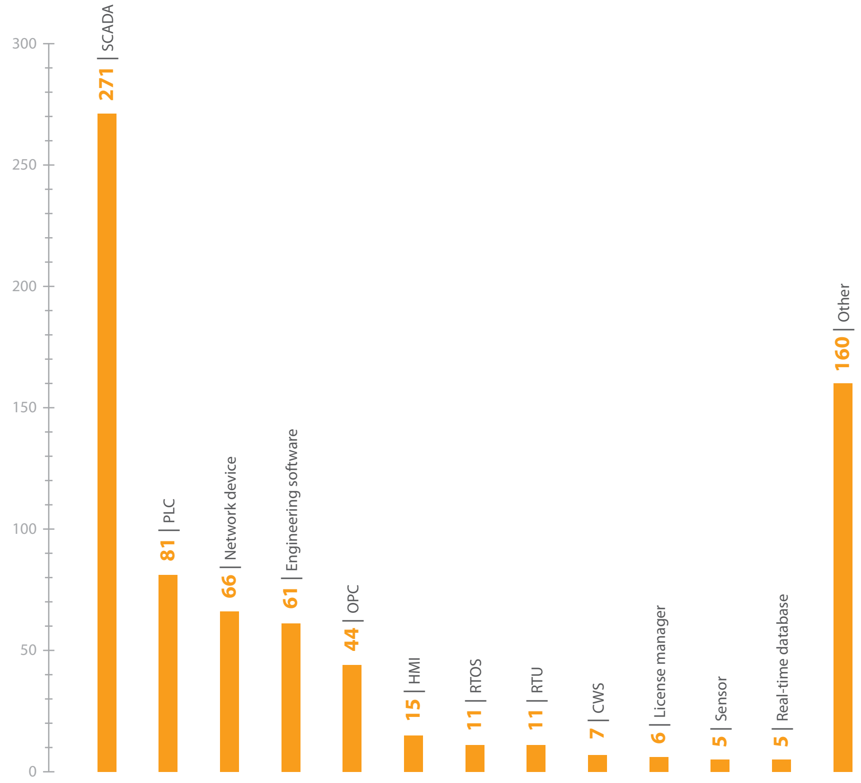

Figure 3. Vulnerabilities in various ICS components

3.4. The risk level of detected vulnerabilities

Nearly one half of detected vulnerabilities (47%) were high-risk.

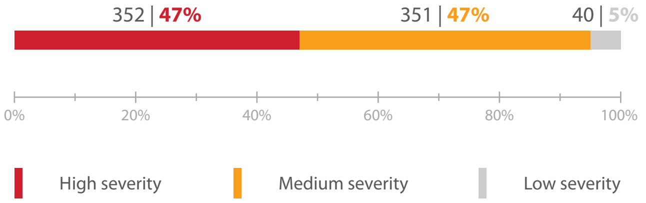

Figure 4. Distribution of vulnerabilities (by risk)

Figure 5 shows vulnerabilities in ICS component of different vendors by severity. The category "Other" includes vendors that provide products that are not commonly used and that contain an insignificant number of vulnerabilities.

The CVSS vector implies assessment of a risk level considering the likelihood that a main security threat could be implemented (breach of confidentiality, integrity, and availability) as a result of vulnerability exploitation and also considers complexity and conditions of exploitation. More than one half of vulnerabilities have the high metric of availability breach (figure 6).

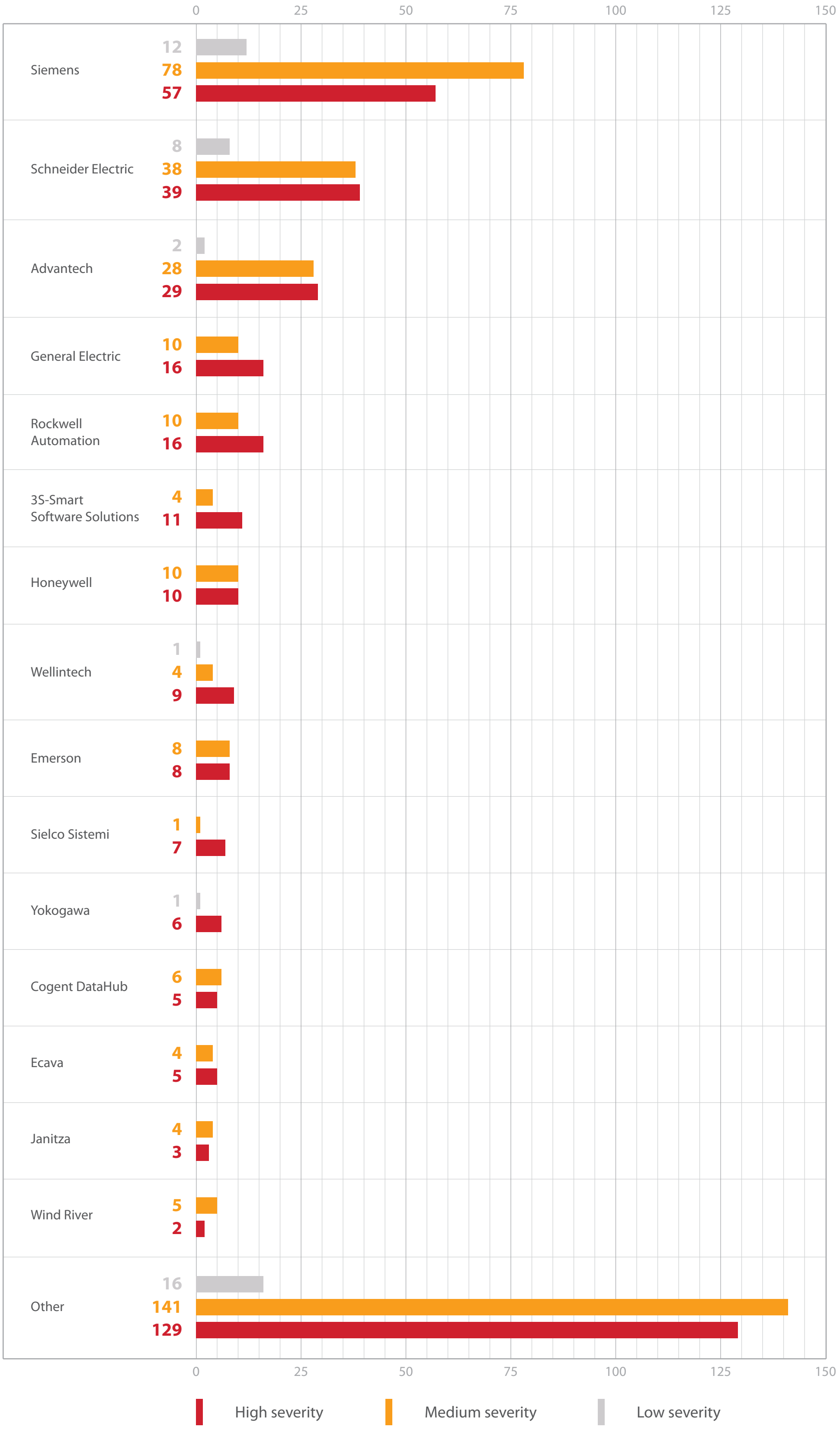

Figure 5. ICS component vulnerabilities (by severity)

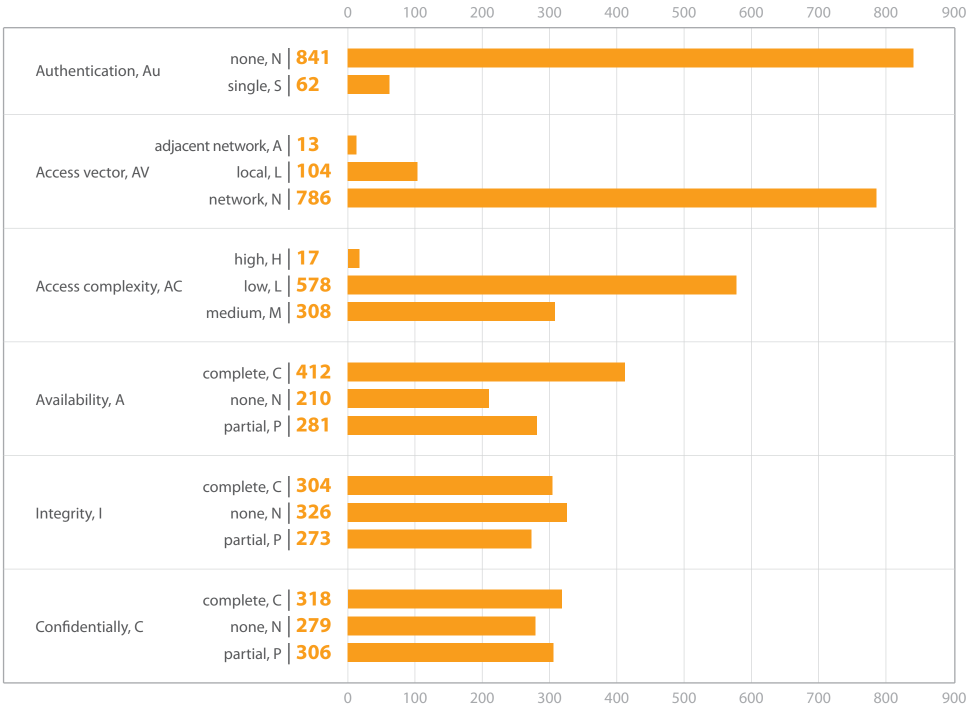

Figure 6. Number of vulnerabilities with various CVSS metric values

3.5. The fraction of fixed vulnerabilities in ICS components and possibilities for an attack

Since data on vulnerability fixes is not published, Positive Technologies researchers included in this section information provided by vendors themselves. Detailed information on the vulnerabilities already fixed by vendors is provided on the Positive Technologies website[10].

2015 data shows that only 14% of vulnerabilities were resolved within three months, while 34% waited over three months and the remaining 52% either were never repaired, or the date of repair was not given by the vendor.

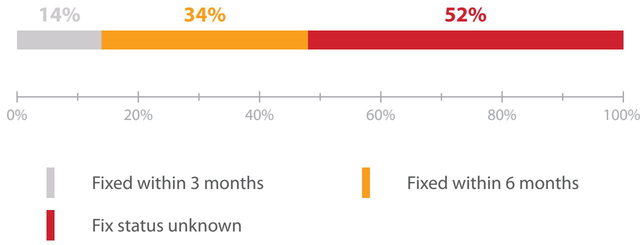

Figure 7. Repair timeline for vulnerabilities identified in ICS components

However, published exploits are available for only 5% of known vulnerabilities.

[10] ptsecurity.com/research/threatscape/

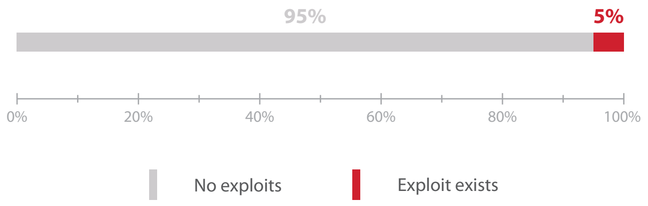

Figure 8. Vulnerabilities that have known exploits

These figures are an improvement over 2012. This, as well as virtually constant number of vulnerabilities found during a year, is due to the fact that at present equipment vendors are interested in eliminating vulnerabilities and they interact with security researchers in order to proactively detect vulnerabilities based on a responsible disclosure policy. However, we should bear in mind that such a low figure is not indicative of a reliable security system since there may be unpublished exploits.

3.6. Vulnerabilities by types

Most vulnerabilities fall into the categories of Denial of Service (DoS), Remote Code Execution, and Buffer Overflow. The proportions of the most common vulnerability types are shown in figure 9 (other types are not widely spread, less than 4%, and are not presented).

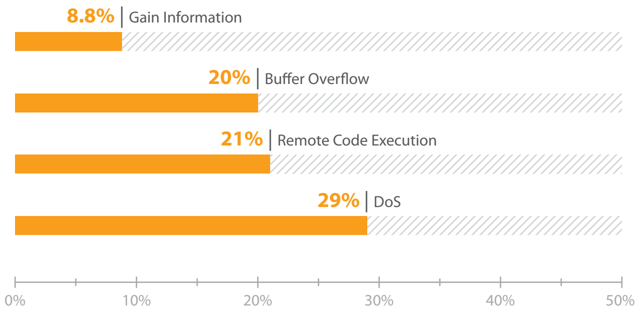

Figure 9. Common types of vulnerabilities in ICS components

Exploitation of such vulnerabilities by an intruder causes equipment failure or unsanctioned operation of equipment, which is equally undesirable given the reliability requirements and sensitivity of ICS components.

4. Internet Availability of ICS Components

4.1. The occurrence of ICS components

The research revealed that 158,087 ICS components are available online. Considering available components depending on protocols, the highest number of ICS components is available via the HTTP protocol.

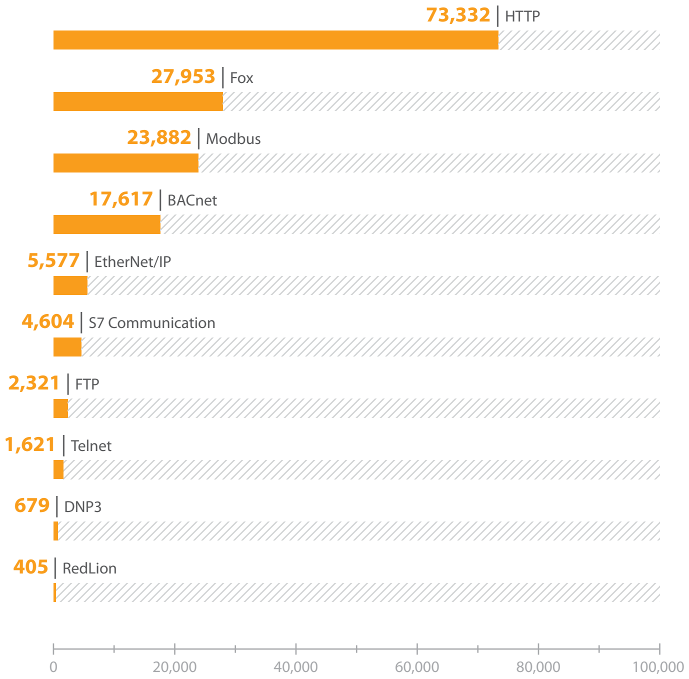

Figure 10. Protocols in use (the number of ICS components)

4.2. Territorial distribution of ICS components

The leader in the number of components found is the United States (39%) by a wide margin, Germany is second (12%) followed by France, Italy, and Canada (about 5% each). This, among other things, is due to the widespread occurrence of BACS that are popular in markets with a high level of automation.

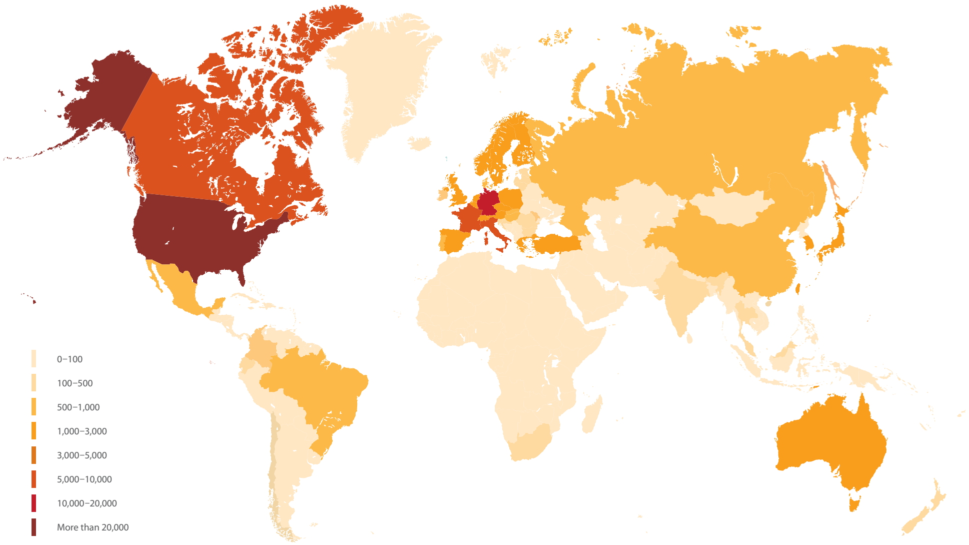

Figure 11. Number of internet-available ICS components

Table 1 shows countries with the most ICS components detected. Seven out of ten countries in this list are in Europe. The low number of ICS components found in Asia is due to the use of local solutions that are little known outside of their home markets. Russia placed 31st, with 600 available components (less than 1% of the total).

ICS components detected in the European internet segment represent about half of the total number of detected components. About 40% of components are concentrated in the Americas, the U.S. and Canada leading by a wide margin. Countries considered technology leaders unsurprisingly have a high concentration of ICS components on the internet.

Table 1. Top 10 countries considering the occurrence of ICS on the internet

Country	Available components	Share in the total number of available components
USA	61,413	38.85%
Germany	19,419	12.28%
France	8,577	5.43%
Italy	8,141	5.15%
Canada	7,801	4.93%
Spain	4,627	2.93%
Australia	3,233	2.05%
Sweden	2,897	1.83%
The Netherlands	2,790	1.76%
The United Kingdom	2,679	1.69%

Figure 12 shows the distribution of ICS components available via the internet by country. The category "Other" includes countries with a share of less than 1%. When compared with the results of the research of 2012, it is interesting to highlight that the U.S. remains the leader, but followed by Germany by a wide margin (not Italy as the previous report indicated).

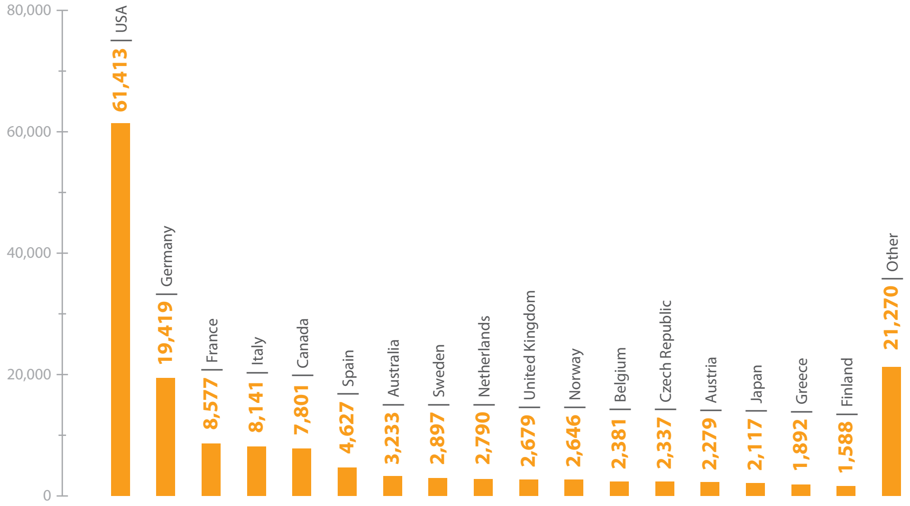

Figure 12. Number of internet-available ICS components

4.3. Occurrence of ICS components (by vendor and product)

The largest vendors of ICS components are Honeywell, SMA Solar Technology, Beck IPC, Siemens, and Bosch Security Systems.

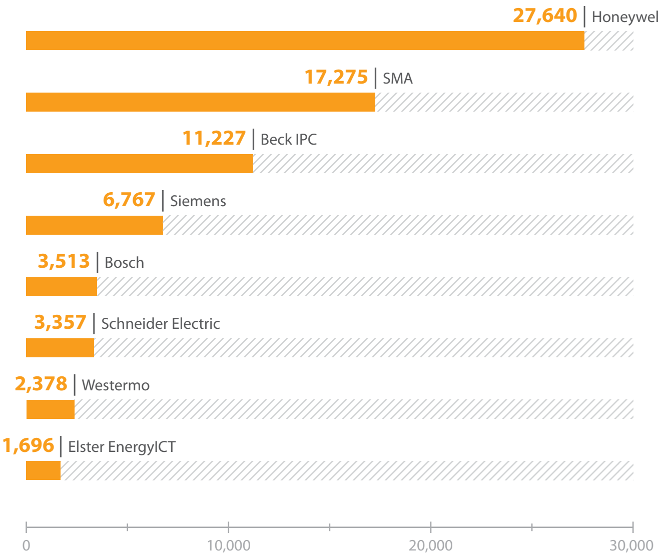

Figure 13. Internet-available ICS components (by vendor)

Niagara Framework developed by Honeywell has the largest number of internet-available equipment. 27,640 of devices were detected (17% of the total). Moreover, 700 various BACS from Honeywell and 1,696 devices from Elster EnergyICT (Honeywell) WebRTU were detected.

SMA Solar Technology and its Sunny WebBox is the second most common vendor. The company provides systems for building automation and power monitoring. 17,300 of its devices were detected via the internet (11%).

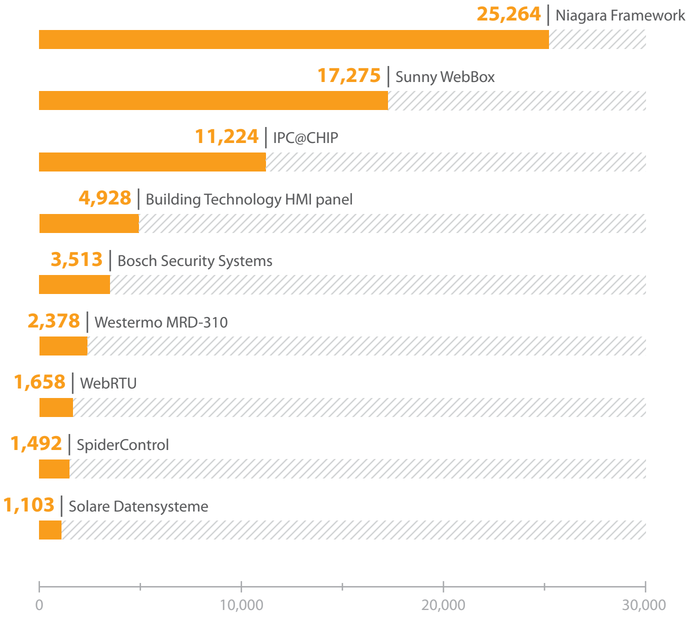

Figure 14. Number of internet-available ICS components

This is followed by the German company Beck IPC and its IPC@CHIP (7%).

Siemens was fourth with 4,930 BACS developed by Siemens Building Technologies were detected along with 1,840 other pieces of equipment from the company (PLC, DCS).

Bosch (3,513 components), Schneider Electric (3,360), and Westermo (2,378) were fifth, sixth, and seventh. We should note that Schneider Electric has a great diversity of equipment available in the global network, including 900 PLC Modicon M340, 650 PLC TWDLCAE40DRF, and 360 ION6800 meters. We should highlight that Bosch Security Systems (a division of Bosh) products are used at Madrid–Barajas Airport in Spain in particular.

Our analysis has also identified about 1,000 SpiderControl devices, Sofrel Lacroix S500, and Solare Datensysteme systems. Vendors and products with a share of less than 1% as well as equipment from unidentified vendors were also detected.

According to a report published by ICS-CERT[11], the highest number of incidents in the United States in 2015 were found in critical infrastructure, including in the energy sector. It should be noted that the analysis of information about the availability of internet-accessible ICS components, Positive Technologies experts determined that 4,893 of such components are used in the energy sector and 51,425 are used in building automation. If in order to compare this data with the ICS-CERT study we do not consider data about the building automation area, the proportion of components that are used in the field of energy and are available via the internet is almost 20% of the total number. This reveals the vulnerability of one of the leading areas of the economy, disruption of which may lead to serious consequences.

The highest number of internet-available components for power management are as follows: Honeywell (2,168), Schneider Electric (933), Solare Datensysteme (820), SenecIES (256), Nordex (239), Echelon (227), and Electro Industries/GaugeTech (138). The distribution of ICS components among vendors is represented in figure 15. The category "Other" includes companies with an insignificant number of detected components.

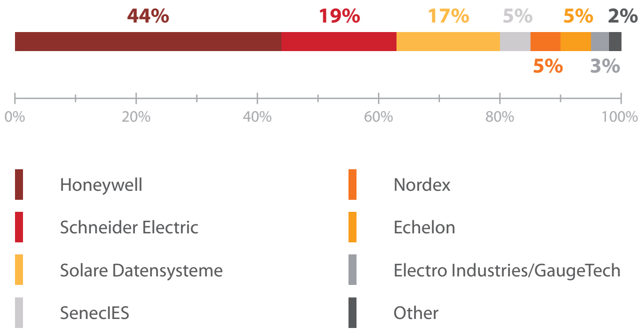

Figure 15. Components of ICS for power management (by vendor)

Schneider Electric is the second most common vendor in the field of power management components. Positive Technologies specialists have found a large number of different versions of PowerLogic and other electronic devices. The most commonly occurring products were WebRTU (2,130) and Solar-Log (820) from Solare Datensysteme. The number of detected power management system components are shown in figure 16 (the category "Other" contains less common components, including some products from Schneider Electric).

[11] ics-cert.us-cert.gov/Year-Review-2015

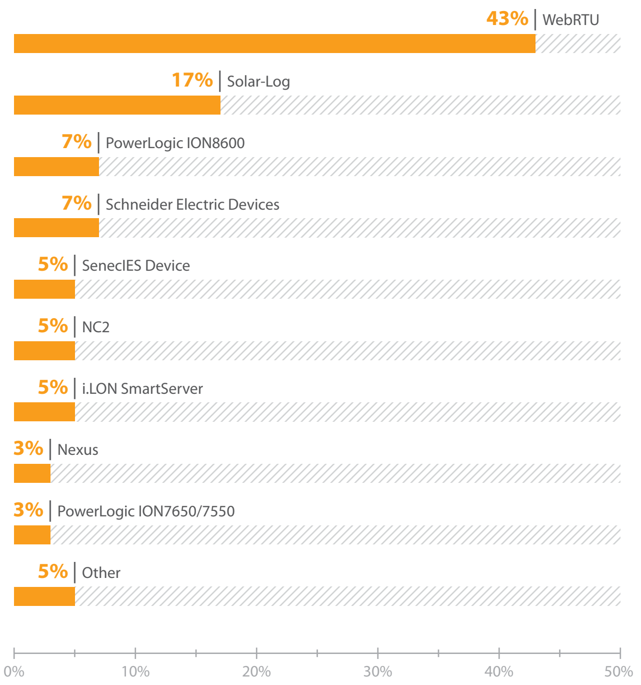

Figure 16. Fraction of various components of ICS for power management

4.4. Types of ICS components

When compiling a database of identifiers, specialists added information on types of ICS components, see below:

Table 2. Number of internet-available ICS components

ICS component	Number of detected components
HMI/SCADA + PLC/RTU	25,264
RTU/PLC	18,233
Electrical instrument	17,979
HMI/SCADA	13,485
Network device	5,016
Sensor	907
Interface converter	408
Circuit breaker	361
Electronic device	179
Power inverter	17
PSP	9
Other	76,229

The majority of internet-available products are devices that function as SCADA/HMI and PLC/RTU (25,250 units), which is due to the prevalence of the multifunctional Niagara Framework from Honeywell.

In terms of the prevalence, PLC/RTU components and remote terminals are second most common and 18,233 such devices were detected.

Devices such as interface converters, circuit breakers, electronic devices, inverters, and PSP are used to control processes associated with power production and transmission. Compromise of such devices (PSP, for example) may lead to power loss or even serious accidents. Given the increasing spread of digital relay protection and availability of such devices on the internet, the likelihood of attacks on them is quite high.

4.5. The number of vulnerable ICS components

Of the ICS components detected on the internet, only half of them can be considered secure. By gathering information with passive methods, it is not always possible to determine an ICS product's version, so it is not always possible to reliably determine whether the component under analysis contains known vulnerabilities. It is also important to consider that the absence of known vulnerabilities does not mean that the system is protected if there is no necessary protection measures and especially if the system can be accessed via the global network.

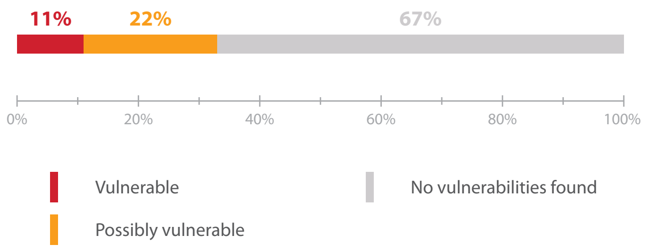

Figure 17. Fractions of vulnerable and secure internet-available ICS components

Summary

The study shows that the number of vulnerable ICS components is not reducing from year to year. Nearly half of identified vulnerabilities are high-risk. The majority of vulnerabilities are found in products from the most well-known vendors. SCADA systems are most vulnerable and at the same time are very common. The highest number of components available on the internet was found in countries where automation systems are most common.

The majority of internet-available components are multifunctional devices. Dictionary and default passwords are often used in ICS; this provides access to such systems and allows taking control over them with little effort.

Data obtained reveals the absence of adequate protection of ICS components. Even minimal preventive measures, such as using complex passwords and disabling ICS components from the internet, will greatly reduce the likelihood of attacks that have significant impact.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com