ICS SECURITY: 2016 YEAR IN REVIEW

POSITIVE TECHNOLOGIES

These days, industrial control systems are found in places quite different from traditional industrial settings. ICS components are integrated into everything from nuclear power plants, to smart home systems. With rapid growth in ICS integrators and a limited number of major vendors to supply them, the same products may be used both at critical infrastructure facilities and run-of-the-mill private companies. An intruder who finds an ICS vulnerability at one company can use the same vulnerability against targets all over the world. Even worse, vendors and users often neglect ICS security. Because of the need for uninterrupted uptime of critical systems (such as industrial protocols, operating systems, and database management systems), ICS software often goes years without updates. The combination of these factors has created a dangerous situation with an evolving threat landscape.

Based on our data, over 100 vulnerabilities in 2016 were detected in ICS components from leading manufacturers, primarily Siemens, Advantech, Schneider Electric, and Moxa. Most of these vulnerabilities were of critical and high risk (60%), typically involving Remote Code Execution, Denial of Service, and/or Information Disclosure. The majority of vulnerabilities are found in dispatch and monitoring systems (HMI/SCADA).

As of early 2017, over 160,000 ICS components could be accessed over the Internet. The largest numbers were found in the USA (31%), Germany (8%), and China (5%). As in previous years, the most commonly encountered Internet-accessible components were Tridium building automation systems, SMA Solar Technology power monitoring and management systems, and IPC@CHIP by Beck IPC.

Detailed results of our analysis of vulnerabilities and Internet-accessible ICS components are given below.

VULNERABILITY ANALYSIS

Materials and methods

Information was drawn from publicly available sources, such as vulnerability knowledge bases, vendor advisories, exploit databases and packs, scientific papers, and posts on security websites and blogs.[1]

The following vulnerability knowledge bases were used:

- 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)
- Schneider Electric Cybersecurity Support Portal (schneider-electric.com/b2b/en/support/cybersecurity/security-notifications.jsp)

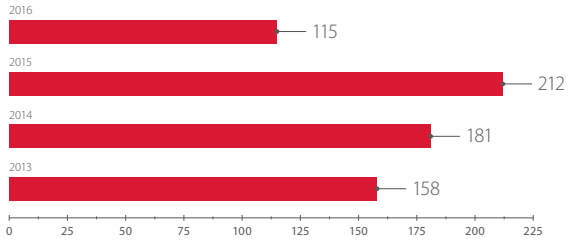
The severity of vulnerabilities in ICS components was assessed based on the Common Vulnerability Scoring System (CVSS) version 3 (first.org/cvss).

Vulnerability analysis included the hardware and software of leading ICS vendors. However, our results do not cover vulnerabilities in any public-domain software (such as OpenSSL or GNU) that may have been used in the development of ICS applications.

Trends

Compared to the previous year, the number of vulnerabilities found in the products of leading manufacturers decreased to 115 in 2016. However, this is not a complete list of vulnerabilities, since some of them can be made public only after the corresponding patches have been released. Positive Technologies experts have informed ICS vendors (Siemens, Schneider Electric, and others) about 13 additional vulnerabilities that have not yet been published as of when this article was written.

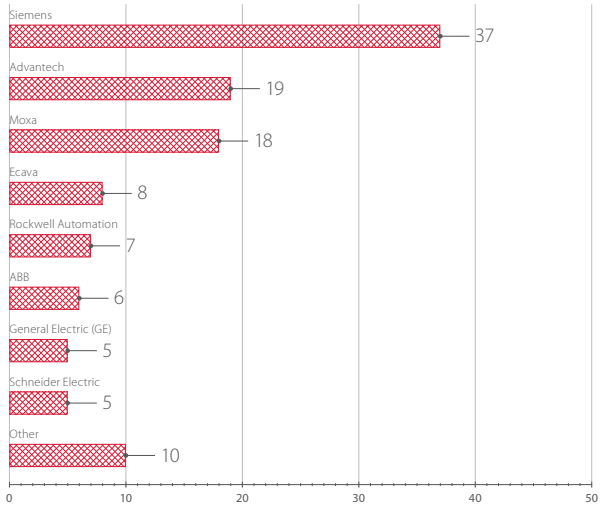
1 digitalbond.com, scadahacker.com, immunityinc.com/products/canvas, exploit-db.com, rapid7.com/db



Total number of ICS vulnerabilities found

Vulnerabilities by vendor

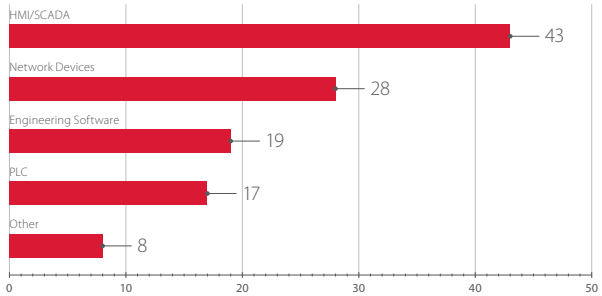
As in 2015, Siemens, Advantech, Schneider Electric, and industrial network equipment manufacturer Moxa are the leaders in reported ICS vulnerabilities. Keep in mind that this number (published vulnerabilities) depends on the prevalence of a vendor's products and on whether the vendor practices responsible disclosure. Therefore, these figures cannot be used to judge the degree of security of solutions from any particular vendor. On the contrary, products from vendors that do not publish information on detected and remediated vulnerabilities are likely to be more vulnerable.



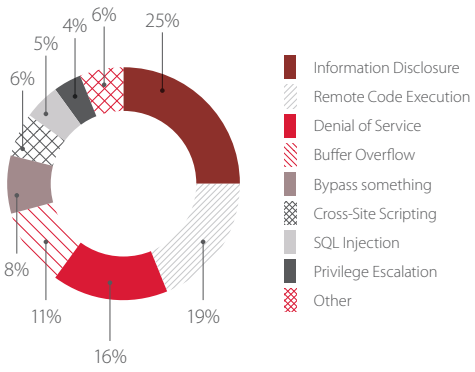
Vulnerabilities among major ICS component vendors

Vulnerabilities by component

The majority of vulnerabilities published in 2016 were detected in dispatch and monitoring systems (HMI/SCADA). Remote Code Execution, Denial of Service, and Information Disclosure vulnerabilities were the most frequent types.

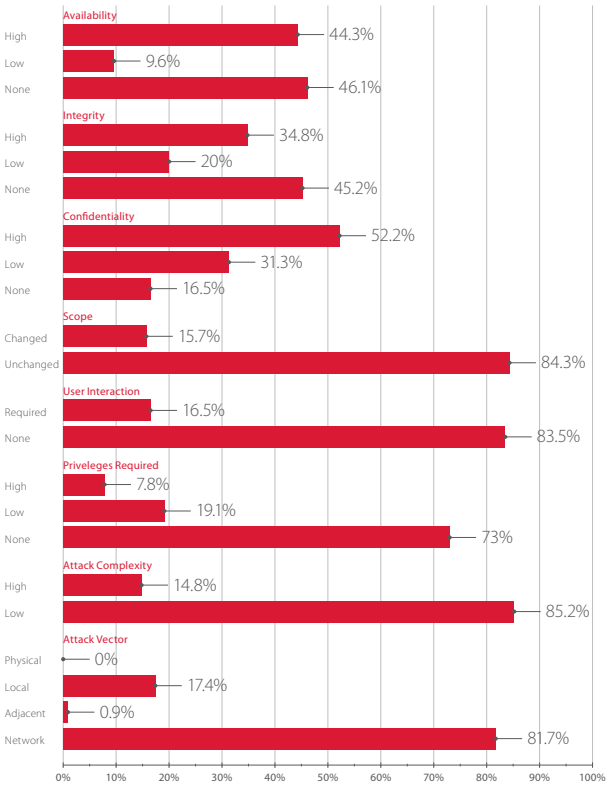


Number of vulnerabilities in various ICS components



Common types of vulnerabilities in ICS components

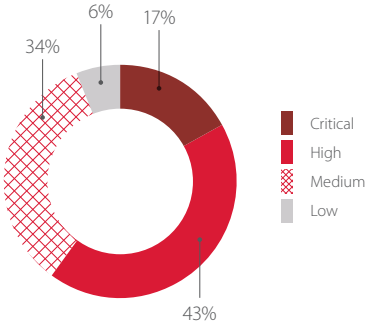
According to CVSSv3, most of the vulnerabilities can be exploited remotely, without obtaining any privileges.



Breakdown of vulnerabilities by CVSS criteria

Risk level

More than half of detected vulnerabilities are of critical and high severity, based on CVSSv3 scoring.



Distribution of vulnerabilities by risk

Vulnerabilities detected by Positive Technologies

In 2016, vendors confirmed and remediated 11 new vulnerabilities detected by our company in ICS components manufactured by Siemens, Advantech, Schneider Electric, General Electric, and Rockwell Automation. Two of the detected vulnerabilities were critical; two were of high severity.

Table 1. Examples of detected vulnerabilities

	ICSA-16-336-01 (CVE-2016-8567)	SEVD-2016-343-01	ICSA-16-336-05A (CVE-2016-9360)
Vendor	**Siemens**	**Schneider Electric**	**General Electric**
Brief description	Vulnerability in Siemens SICAM Power Automation System software involving insecure password storage and disclosure of sensitive information. An intruder can remotely gain privileged access to the SICAM PAS database by exploiting standard support for remote configuration via TCP port 2638 and hard-coded passwords of default user accounts.	Vulnerability in StruxureWare Data Center Expert 7.3.1.114 and 7.2.4 and earlier versions involving insecure storage of some passwords in RAM.	Vulnerability in Proficy HMI/SCADA iFIX 5.8 SIM 13, Proficy HMI/SCADA CIMPLICITY 9.0, Proficy Historian 6.0, and earlier versions allows an intruder to locally intercept user passwords if possessing access to an authorized session.
CVSS score	**9.8** Critical severity	**7.6** High severity	**6.4** Medium severity
CVSS vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:N	AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:L/A:L
Recommendations for remediation	Update SICAM PAS to version 8.0.	Update to version 7.4.0 or later.	Update Proficy HMI/SCADA iFIX to version 5.8 SIM 14, Proficy HMI/SCADA CIMPLICITY to version 9.5, and Proficy Historian to version 7.0.
Link	ics-cert.us-cert.gov/advisories/ICSA-16-336-01	schneider-electric.com/en/download/document/SEVD-2016-343-01	ics-cert.us-cert.gov/advisories/ICSA-16-336-05A

AVAILABILITY OF ICS COMPONENTS ON THE INTERNET

Materials and methods

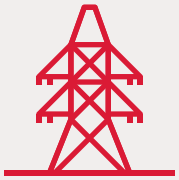
Researchers used only passive methods to collect information on the online availability of ICS components. This meant scanning Internet-accessible ports using publicly available search engines: Google, Shodan (shodan.io), and Censys (censys.io).

This data was then analyzed to determine a relationship to ICS equipment. Positive Technologies experts created a database of ICS identifiers, consisting of approximately 800 entries, for determining the product and relevant vendor from the device's banner.

Prevalence

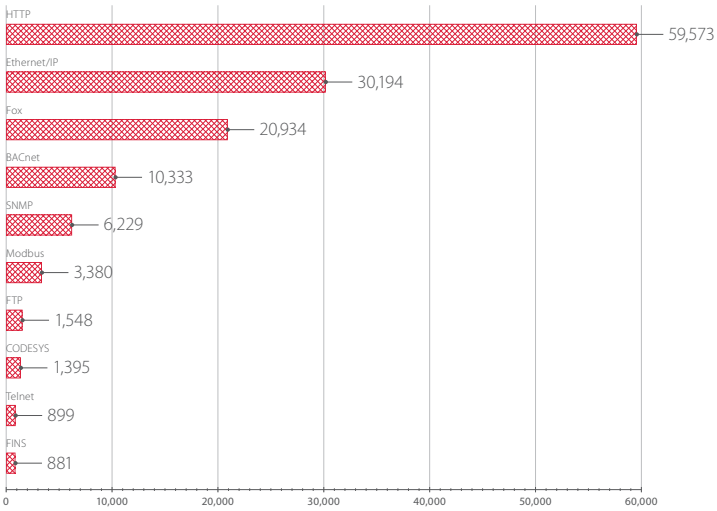
The research revealed 162,039 ICS components available online. Of these, 4,515 components (3%) are used in the energy sector and 38,580 (24%) are used in building automation.

Looking at the protocols used by the detected ICS components, the largest single protocol was HTTP, which is consistent with recent years.



Importance of encryption

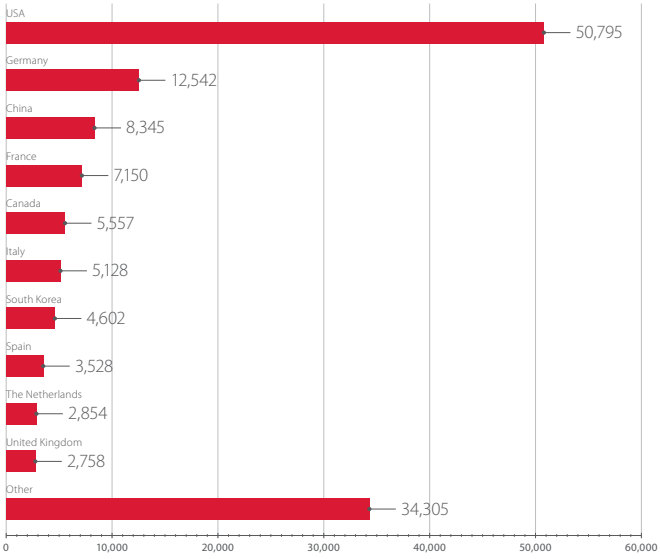
Unencrypted storage of passwords can result in an attacker gaining control of an ICS/SCADA system. The attacker can log in like any other user and start affecting operations—leading to economic losses, equipment failure, or even serious accidents. By gaining passwords to databases, an attacker is able to illegitimately modify information and create the preconditions for malfunction and/or physical harm.



Number of Internet-accessible ICS components (by protocol)

Geographic distribution

Also consistent with recent years, the leader in the number of components found is the United States (31% of the total) by a wide margin. Germany is second (8%), followed by China (5%), which was not even in the top 10 countries the previous year. One likely reason for the large number of ICS components found in these countries is the popularity of building automation systems.

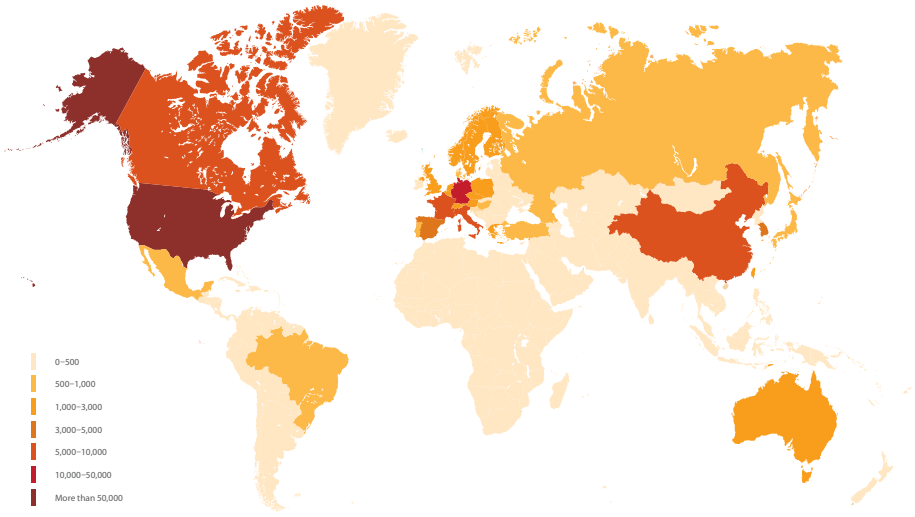


Top 10 countries by number of Internet-accessible ICS components

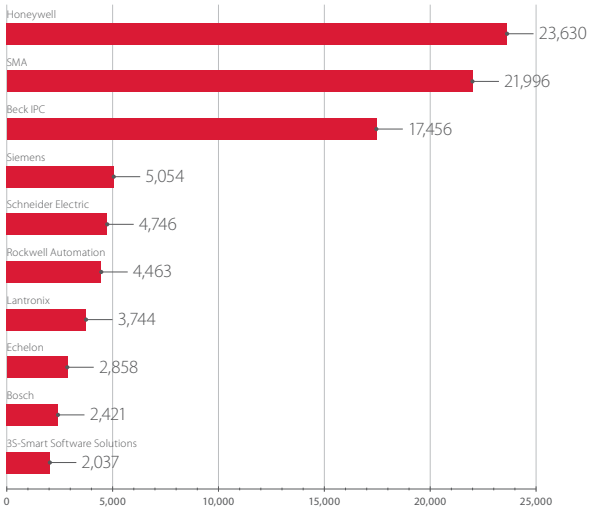
Prevalence of ICS components (by vendor)

Honeywell's Niagara Framework is still the software most commonly found on Internet-accessible equipment. Sunny WebBox by SMA Solar Technology is close behind in second place, with German company Beck IPC and its IPC@CHIP in third place.

Niagara Framework by Tridium, a Honeywell company, is one of the most popular systems for smart home automation. Sunny WebBox solar power monitoring and management systems by SMA Solar Technology are particularly popular in European countries. IPC@CHIP by Beck IPC is popular thanks to its relatively low price, multifunctionality, embedded Ethernet controller with TCP/IP stack support, and built-in web server.



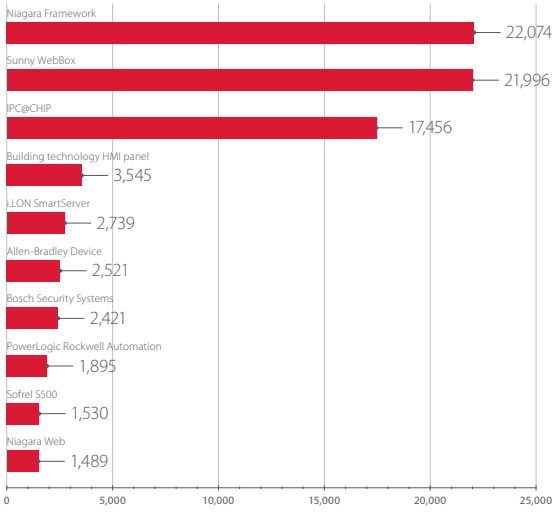
Number of Internet-accessible ICS components (by country)



Number of Internet-available ICS components (by vendor)

Interesting fact

Interface converters and network devices are of major interest to intruders. Attacks on these devices do not require in-depth knowledge of target processes, but have the potential to cause breakdowns and serious accidents.



Number of Internet-accessible ICS components (distribution by product)

Types of ICS components found

We classified ICS components by type based on their entries in the identification database.

Table 2. Share of Internet-accessible ICS components

ICS component	Share in 2016	Share in 2015
SCADA/DCS/HMI+PLC/RTU	13.62% ↓	15.98%
RTU/PLC	12.86% ↑	11.53%
SCADA/DCS/HMI	7.80% ↓	8.53%
Electrical measuring equipment	5.18% ↓	11.37%
Network device	5.06% ↑	3.17%
Interface converter	1.31% ↑	0.26%
Circuit breaker	0.15% ↓	0.23%
Power inverter	0.15% ↑	0.01%
Sensor	0.13% ↓	0.57%
Power system protection	0.01%	0.01%
Other	53.72% ↑	48.33%

SUMMARY

The number of vulnerabilities made public by the major ICS vendors significantly decreased in the last year, since many vulnerabilities had been remediated already in previous years. However, over half of the detected vulnerabilities were of critical and high risk, and these vulnerabilities are the ones that vendors attempt to remediate first. Leading vendors have already started paying more attention to detection and remediation of vulnerabilities during both the development and operation stages. Active cooperation between vendors and security researchers is critical for ensuring greater security for ICS overall.

At the same time, the number of Internet-accessible ICS components is growing. The majority of them were detected in the countries with the highest levels of automation (USA, Germany, China, France, and Canada). Most Internet-accessible ICS components are multifunctional and used for automation of a number of systems. Dictionary or default passwords are often used for remote access to ICS components, making it trivially easy for an intruder to take control. The most basic preventive measures—such as disconnecting ICS components from the Internet and using strong passwords—help to significantly decrease the likelihood of attacks.

We urge regular ICS security audits to identify possible attack vectors and develop an effective security strategy. In addition, vendors should be informed in a timely manner about new vulnerabilities and undeclared features of ICS components as they are discovered during ICS operation.

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