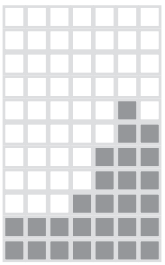
SCADA



SCADA SAFETY IN NUMBERS

POSITIVE TECHNOLOGIES

Table of Contents

1. Introduction

Modern civilization is largely dependent on ICS/SCADA industrial process automation systems. Computer technology now controls the operation of nuclear power plants, hydroelectricity plants, oil and gas pipelines as well as transport systems at national and global levels. Both corporate profits and national security depend on these control systems operating safely and reliably.

The security of such systems has become a hot topic in recent years following a series of incidents involving particular computer viruses such as Flame and Stuxnet. These attacks showed how easy it is for cyber-terrorists, competitor companies or the secret services of other nations to profit when ICS/SCADA/PLC information security is not given high priority.

Threat-modeling and simulated attacks are an essential part of the deployment process for critical systems. For these to be of use, it is important to understand what skills the potential attacker might possess and what method of attack they may choose. In order to answer these questions, the experts from Positive Research conducted a thorough security review of ICS/SCADA systems.

This report details the findings of the study which looked at the vulnerabilities that were discovered during the period from 2005 to October 1, 2012. It consists of 3 sections:

- An executive summary of the study's findings
- Statistical analysis for vulnerabilities found in ICS systems
- An assessment of the availability of ICS systems from the Internet

2.Executive Summary

1. The history of industrial system security can be considered as two distinct halves — the period prior to Stuxnet and the time after it was discovered. Since 2010, the number of vulnerabilities detected has been 20 times higher than in the preceding five years collectively.

HIGHLIGHTS:

- ***The number of vulnerabilities detected has increased by 20 times (since 2010).***
- ***One in five vulnerabilities is not fixed within a month of detection.***
- ***50% of vulnerabilities allow a hacker to execute code.***
- ***There are known exploits for 35% of vulnerabilities.***
- ***41% of vulnerabilities are classified as "critical".***
- ***Amateur hackers can access more than 40% of the ICS systems available on the Internet.***
- ***A third of all systems available over the Internet are located in the USA.***
- ***A quarter of all vulnerabilities are caused by failure to install the necessary security updates. 54% of Internet-available systems in Europe are vulnerable. In North America that figure is 39%.***

2. The number of vulnerabilities uncovered continued to grow rapidly in 2012. More security flaws were found in the first 10 months of 2012 than in the entire preceding five years.

3. Vulnerabilities are most likely to be found in the most commonly-used products, and in most cases the vendors are able to eliminate them relatively quickly. However, one in five vulnerabilities remained unresolved for more than 30 days after its detection.

4. About 65% of vulnerabilities are rated as of high or critical severity. This figure significantly exceeds a similar index for IT systems in general, demonstrating that overall information security levels in ICS systems are poor.

5. Half of the vulnerabilities detected would allow a hacker to execute arbitrary code in the target ICS system.

6. More than 40% of the SCADA systems available via the Internet are vulnerable and can be hacked by malware users with only limited skills.

7. Of all the regions analyzed, the USA and Europe have the most ICS systems available via the Internet and yet they also demonstrate the least apparent concern for ICS security.

8. More than a third of the security flaws detected in Internet-available ICS systems were caused by errors in system configurations, including the use of default passwords.

9. A quarter of the vulnerabilities detected in Internet-available ICS systems were caused, at least in part, by a failure to install the recommended security updates.

3. Detailed Statistics on Vulnerabilities Found in ICS Systems

3.1. Research Methodology

This report is the result of detailed analysis of data from a variety of sources including vulnerability databases, vendors' alerts, exploit packs, science conference reports and articles published on specialized sites and blogs. It was necessary to analyze this broad spectrum of data to gain an accurate picture of the state of the industry; since cooperation between the information security research community and vendors of ICS systems is still in its infancy. In fact, details of many vulnerabilities are still being published without the knowledge of the applicable vendor.

The main sources used in the research

Vulnerability databases:

- ICS-CERT
- NVD
- CVE
- Bugtraq
- OSVDB
- Mitre Oval Repositories
- exploit-db
- Siemens Product CERT

Exploit packs:

- SAINTexploit
- Metasploit Framework
- Immunity Canvas
  - Agora Pack
  - Agora SCADA+
  - D2 Exploit Pack
  - White Phosphorus exploit pack
  - VulnDisco Exploit Pack

For each vulnerability discovered, the Positive Research team searched for any methods that were generally available which would allow a hacker to exploit the weakness. They then provided their expert evaluation of the related risks.

3.2. Dynamics of Vulnerability Discovery

Information security specialists discovered only nine vulnerabilities during the period from January 2005 to early 2010. But since the computer worm Stuxnet was discovered in 2010, both information security experts and hackers have shown a much greater level of interest in this area. As a result, 64 ICS vulnerabilities were discovered in 2011 and 98 additional ones were announced in the first eight months of 2012 alone, — more than the total number for the preceding seven years combined.

The path from the discovery of a vulnerability in SCADA systems to a fix is sometimes a frustrating one. During the investigation of the Stuxnet incident, it was found that one of the exploited vulnerabilities — a default password for MS SQL Server — was known long before the attack. It was first mentioned on support forums in May 2005 and the default passwords were published in April 2008. The issue was fixed only after the Stuxnet attack in 2010.

Table 1. The Number of Vulnerabilities Discovered

Year	Vulnerability total
2005	1
2007	3
2008	5
2010	11
2011	64
2012	98

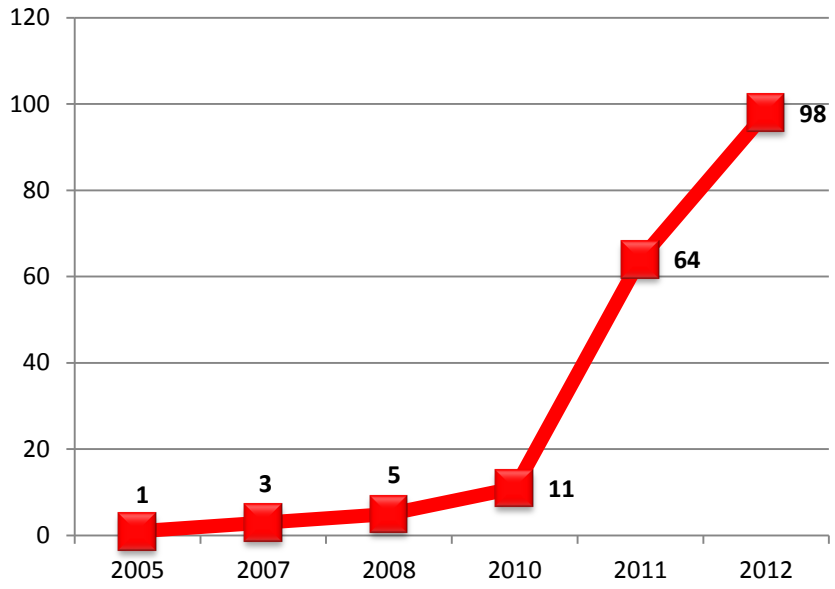


Figure 1. Number of ICS Vulnerabilities Reported

3.3. The Number of Vulnerabilities in ICS systems of Various Vendors

The vendor with the highest number (42) of vulnerabilities found during the reporting period was Siemens (when all the various components of its ICS are considered together). Second place went to Schneider Electric with 30 vulnerabilities, followed by Broadwin/Advantech with 22 vulnerabilities.

Table 2. The Number of Vulnerabilities in the ICS Systems of Various Vendors

Vendor	Vulnerability Total	Vendor	Vulnerability Total
Automated Solutions	2		
Schweitzer Engineering Laboratories	2	WellinTech	9
RuggedCom	2	General Electric	15
Lantronix	3	Invensys Wonderware	15
Progea	3	Schneider Electric	30
ABB	3	Advantech/Broadwin	22
Sielco Sistemi	3	Siemens	42
Iconics	5	Emerson	6
Measuresoft	6	Rockwell Automation	9
Ecava	5		
Emerson	6		

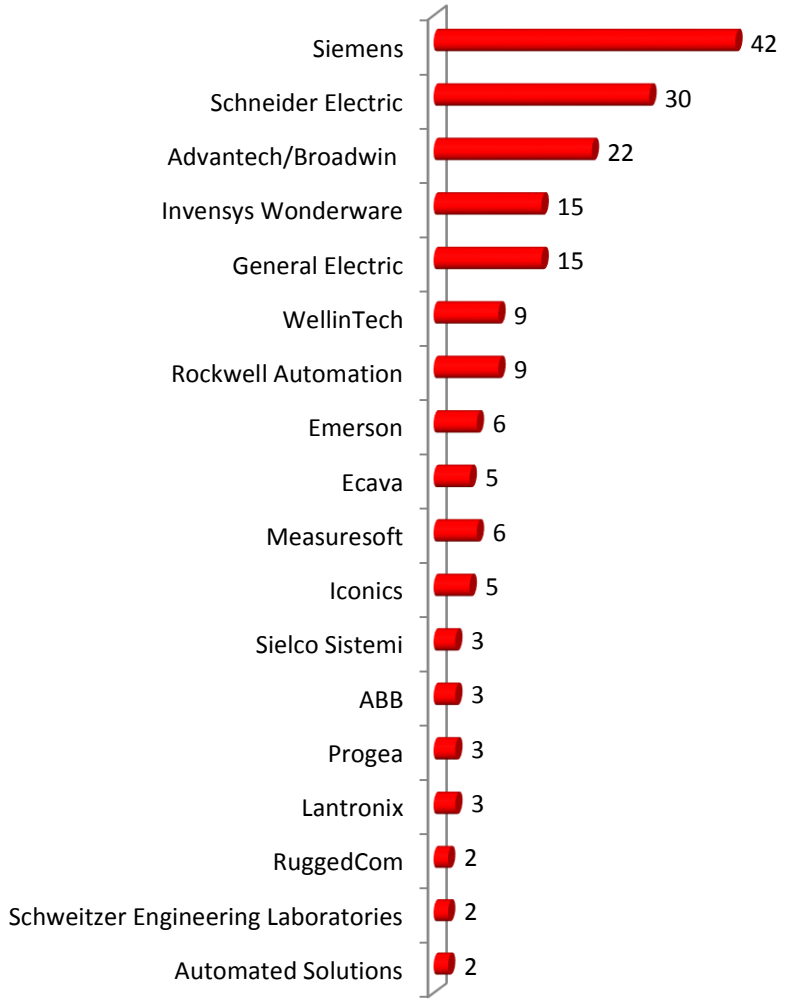


Figure 2. The Number of Vulnerabilities in the ICS Systems of Various Vendors

As with other IT systems, the highest number of vulnerabilities in ICS are found in the most commonly-used components. Moreover, during the period under consideration a number of vendors changed their approach to ICS security from reactive to proactive and took significant steps to find and fix vulnerabilities in their products. For instance, Siemens created a specific department, Siemens ProductCERT (http://www.siemens.com/corporate-technology/en/research-areas/siemens-cert-security-advisories.htm), whose main goal is to discover and resolve security issues in the company's products. The vulnerabilities discovered by the ProductCERT team are also included in the general statistics; which in part explains the sharp increase in the number of issues found and fixed.

3.4. Vulnerabilities Relating to ICS Hardware and Software Components

ICS components such as SCADA systems and human machine interfaces (HMI) present a significant lure for attackers: these systems yielded 87 and 49 vulnerabilities respectively. During the study, researchers found 20 vulnerabilities in the programmable logic controllers of systems from the various vendors.

Table 3. The Number of Vulnerabilities in Different Types of the ICS Components

System Type	Vulnerability Total
SCADA	87
HMI	49
PLC	20
Hardware	11
Software	7
Interface/Protocol	1

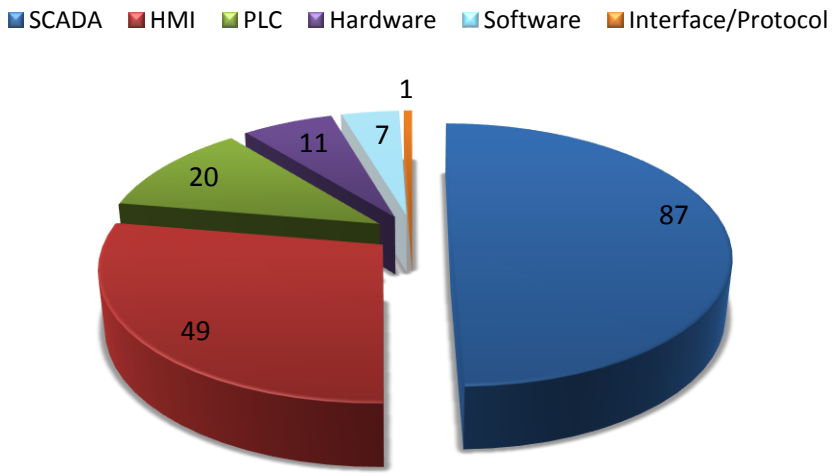


Figure 3. The Number of Vulnerabilities in Different Types of ICS Component

3.5. Classification of Vulnerabilities According to Their Types and Possible Consequences

Over a third (36%) of vulnerabilities found were associated with Buffer Overflow — an anomaly where a program overruns the buffer's boundary while writing data. This defect in security allows the attacker not only to cause the program to end prematurely or freeze

(leading to a denial of service), but also to execute arbitrary code in the target system. Vulnerabilities which allow the attacker to execute code, including Buffer Overflow and Remote Code Execution, make up 50% of all the detected flaws – an extremely high figure.

The recent rapid growth of vulnerability detection in ICS is the result of ethical hackers getting involved. Positive Research discovered more than 50 vulnerabilities in different ICS products in 2012, most of which have now been fixed by the vendors. A lot of work to coordinate the process of vulnerability remediation is being done by ICS CERT.

Also worthy of note is the large number of issues surrounding Authentication and Key Management — almost 23% of the vulnerabilities found fell into this classification.

Table 4. Classification of Vulnerabilities in ICS According to Type

Vulnerability Type	Vulnerability Percentage, %
Buffer Overflow	36
Remote Code Execution	13
Web (client-side)	9
Web (server-side)	11
Local Privilege Escalation	2
DoS/Data Integrity	6
Authentication / Key Management	23

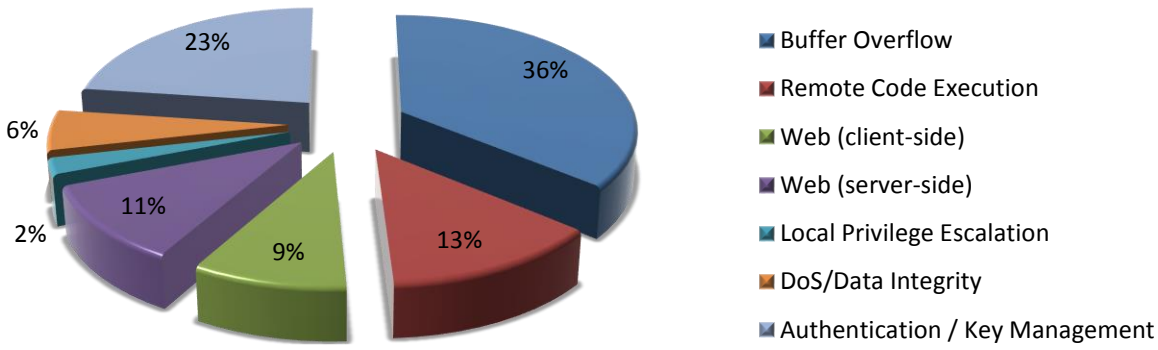


Figure 4. Classification of Vulnerabilities in ICS According to Type

3.6. Percentage of Fixed Vulnerabilities in ICS

The figures for the percentage of vulnerabilities fixed by each ICS vendor gives a clear demonstration of how seriously they take information security. For instance, Siemens fixed and released patches for 88% of vulnerabilities found in its products, while ABB fixed only 67% of security defects.

Table 5. Percentage of Vulnerabilities Fixed in ICS

Vendor	Fixed, %
Schneider Electric	93
Advantech/Broadwin	91
WellinTech	89
Siemens	88
General Electric	80
Rockwell Automation	78
ABB	67
Lantronix	—
Schweitzer Engineering Laboratories	—
Total	**84**

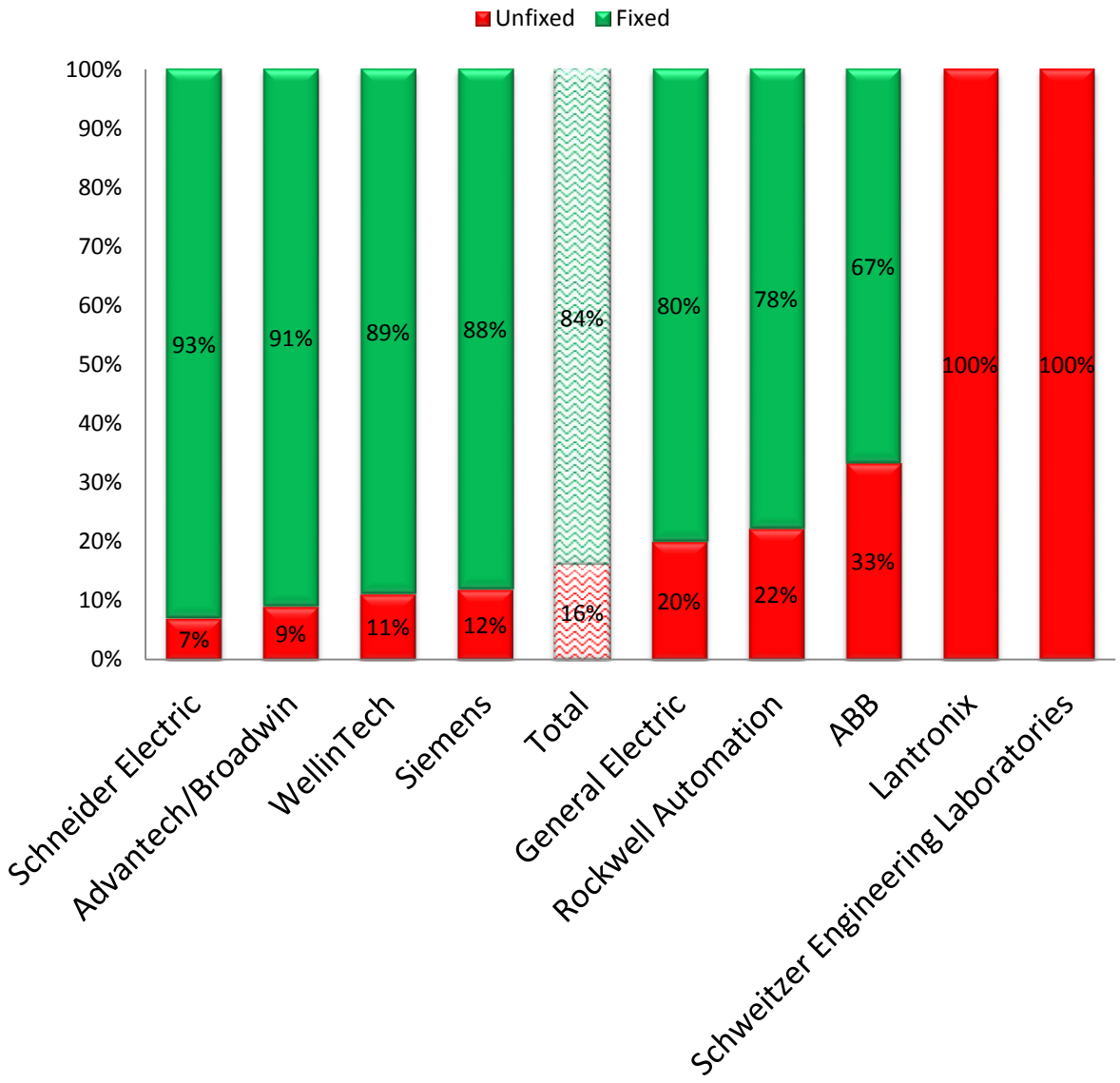


Figure 5. Percentage of Vulnerabilities Fixed in ICS

3.7. Percentage of Vulnerabilities Fixed Promptly

The majority (81%) of the security defects found were fixed promptly by ICS component vendors – typically before the flaws became widely known or within 30 days of uncoordinated disclosure. Approximately one in five vulnerabilities was only fixed after a

significant delay, or was not fixed at all.

In August 2010, US-CERT VU#362332 was published. It reported a dangerous vulnerability in VxWorks, a real-time OS, used in industrial systems. According to HD Moore, he discovered more than 250,000 vulnerable systems which were accessible through the Internet.

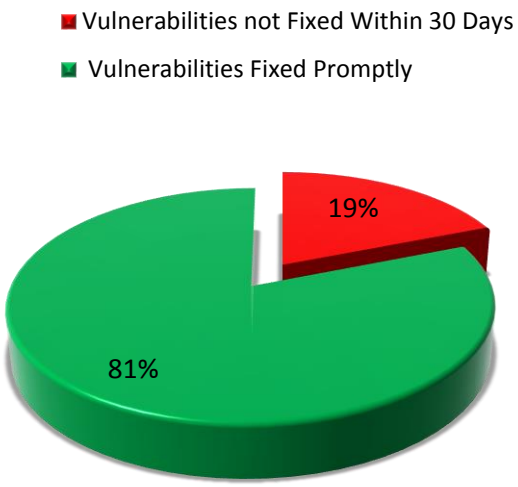


Figure 6. Percentage of Vulnerabilities Fixed Promptly

3.8. Availability of information and software to conduct attacks

If there are ready-to-use tools to exploit a vulnerability that are already in the public domain, it is much more likely that an attack will be conducted successfully. Positive Research found widely-available information that would allow hackers to take advantage of 35% of all known SCADA vulnerabilities. The exploits had either been issued as single utilities, as part of penetration testing software or had been described in security bulletins. This rate of 35% is several times higher than the corresponding rate for IT systems as a whole.

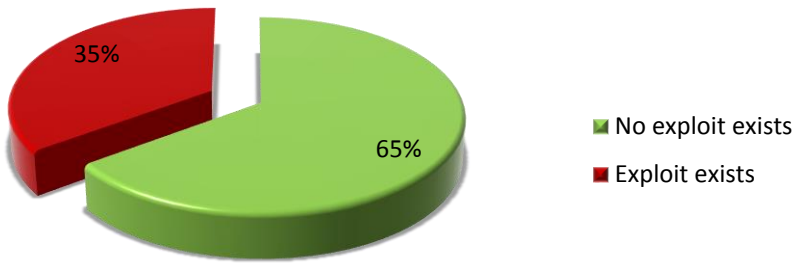


Figure 7. Percentage of vulnerabilities that have known exploits

3.9. Number of published exploits

As a general rule, the number of detected vulnerabilities correlates with the number of published exploits. From 2011 to the end of September 2012, 50 exploits were published - six times greater than the corresponding rate for the period from 2005 - 2010.

Table 6. Number of published exploits

Year	Number of exploits
2008	2
2010	6
2011	30
2012	20

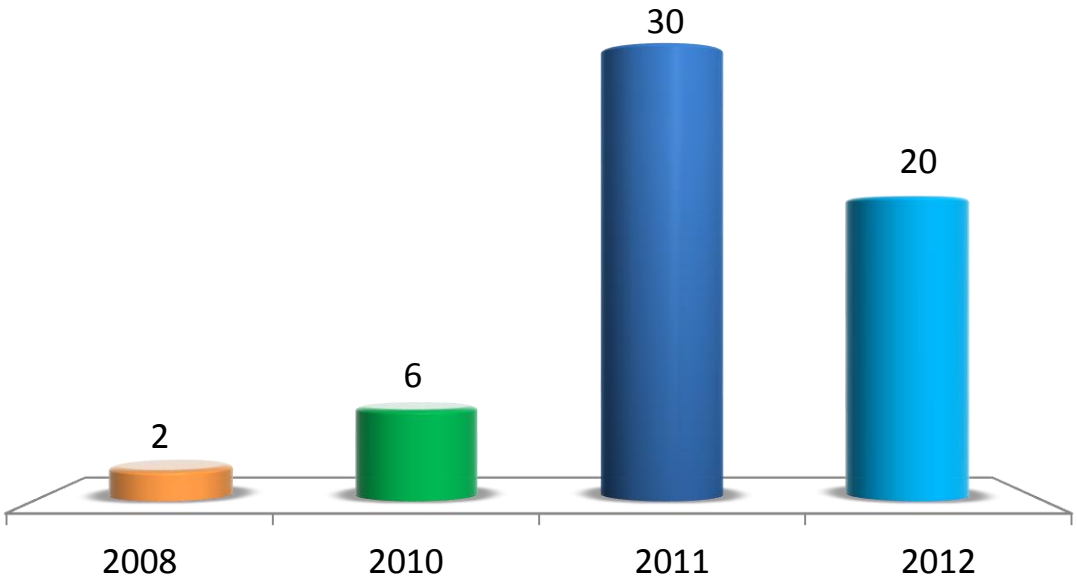


Figure 8. Number of published exploits

There are two plausible reasons why the number of exploits published in 2012 were less than those in 2011:

- Relationships between SCADA vendors and information security researchers have been formalized and responsible disclosure policies are being used
- There is a clear lag between the publication of vulnerability details and the publication of exploits (certain costs are incurred to develop exploitation tools).

3.10. Risk levels of detected vulnerabilities

A great number (66%) of the vulnerabilities detected are of high or critical level[1].

The most dangerous are critical vulnerabilities (with published exploits).

[1] Vulnerabilities of high-level have a CVSS v2 Base Score value > 6.5. Vulnerabilities of critical-level are high-level with known exploits.

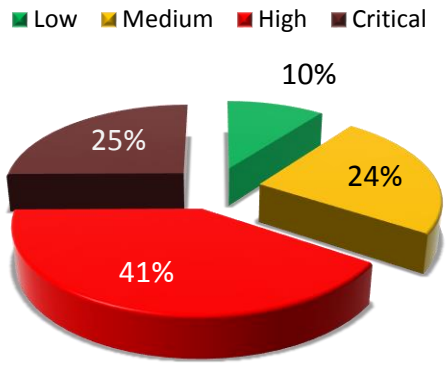


Figure 9. Vulnerabilities by risk level

Table 7. ICS vulnerabilties by risk level

	Critical, %	High, %	Medium, %	Low, %
SEL	—	50	50	—
Lantronix	—	33	33	33
Emerson	—	40	40	20
Invensys Wonderware	—	47	40	13
Rockwell Automation	11	56	33	—
Siemens	14	42	31	14
General Electric	20	67	7	7
Advantech/Broadwin	23	45	23	9
ABB	33	67	—	—
Ecava	33	17	33	17
Schneider Electric	40	20	27	13
Measuresoft	40	40	20	—
Iconics	40	40	—	20
Automated Solutions	50	50	—	—
WellinTech	56	33	11	—
Progea	67	33	—	—
Sielco Sistemi	67	33	—	—
RuggedCom	100	—	—	—

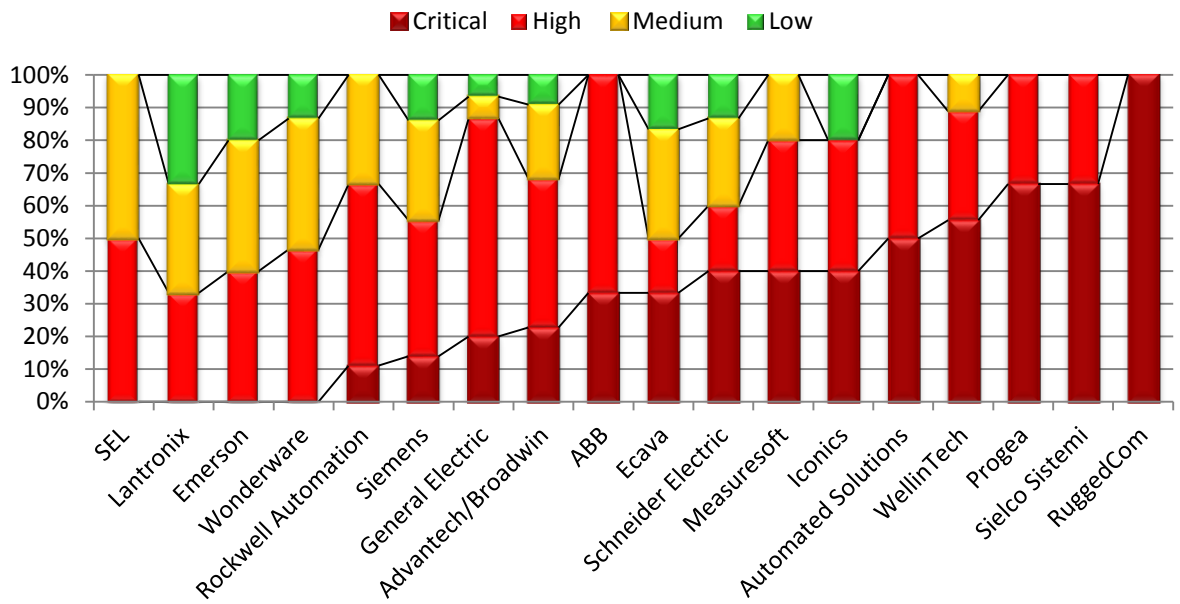


Figure 10. ICS vulnerabilties by risk level

The lack of critical vulnerabilities in the SCADA components produced by SEL, Lantronix, Emerson and Invensys indicates that there are no relevant published exploits. This reduces the chance that systems from these vendors will be attacked, but does not rule it out completely. As a rule, an attack against an industrial enterprise can be considered as a kind of multi-move game played by experienced experts who do not need the assistance of "exploit packs" and other such tools intended for "ordinary" hackers.

Information about the ICS systems accessible over the Internet is being published constantly on Twitter through accounts such as @ntisec. More than 2,000 SCADA IP addresses located in different regions of the world have been posted on Pastebin.com

3.11. Unresolved ICS Vulnerabilities

The greatest risk to a system comes from vulnerabilities for which there is a known means of attack, but no means of defense. If there is an exploitable vulnerability for which a fix has not yet been issued, the risk of compromise to the system is high, because an attacker does not need significant knowledge or an extended period to prepare for the attack. Moreover, the attack can be conducted by hooligans who may have little other intent than to cause maximum chaos. The systems with the highest incidence of these unresolved vulnerabilities were the General Electric SCADA components, where three vulnerabilities were detected for which no fix was available. Schneider Electric's system was the second most vulnerable with two unresolved flaws. Third and fourth places were shared between Advantech/Broadwin and Rockwell Automation, with one open vulnerability in each of their systems.

Table 8. Number of SCADA System Vulnerabilities with Exploits but No Fix

Vendor	Number of vulnerabilities
Advantech/Broadwin	1
Rockwell Automation	1
Schneider Electric	2
General Electric	3

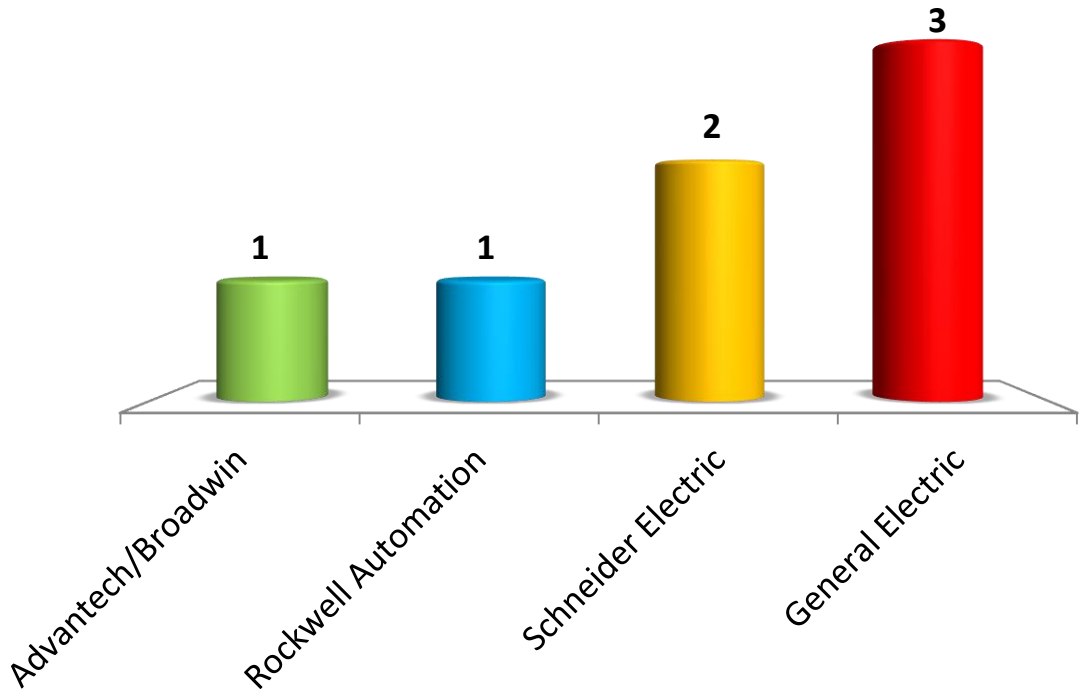


Figure 11. Number of SCADA System Vulnerabilities with Exploits but No Fix

4. Popularity of ICS on the Internet

To understand to what extent the vulnerabilities described above can be used by an attacker, Positive Research carried out an assessment to establish the level of information available in relation to vulnerable ICS systems. Passive analysis was carried out together with investigation of search engines (Google, Yahoo, and Bing) and specialized databases such as ShodanHQ. The Every Routable IP Project was also employed to search and check system versions. The information obtained from these sources was analyzed to detect vulnerabilities related to configuration-management and the installation of updates.

Unfortunately, the passive technique is not a reliable way of identifying all detected vulnerabilities. For this reason, the majority of the information in this section should be considered as a positive script: where detailed analysis occurs, the number of detected vulnerabilities will certainly increase.

4.1. Frequency of ICS Systems

Almost a third (31.3%) of all the ICS systems which have elements that are accessible via the Internet are located in the USA. Italy follows far behind with 6.8%, with South Korea lying third in the table at 6.2%. Russia holds 12th place with 2.3%, and only 1.1% of ICS systems available from the global network are located in China.

Table 9. ICS Allocation by Country

Country	ICS, %	Country	ICS, %
USA	31.3	Netherlands	2.5
Italy	6.8	Russian Federation	2.3
South Korea	6.2	Spain	2.3
Canada	5.6	Austria	1.7
India	4.8	Finland	1.7
Czech Republic	3.9	Sweden	1.7
France	3.9	Switzerland	1.7
Poland	3.1	Great Britain	1.4
Germany	2.8	China	1.1
Taiwan	2.8	Other countries	12.4

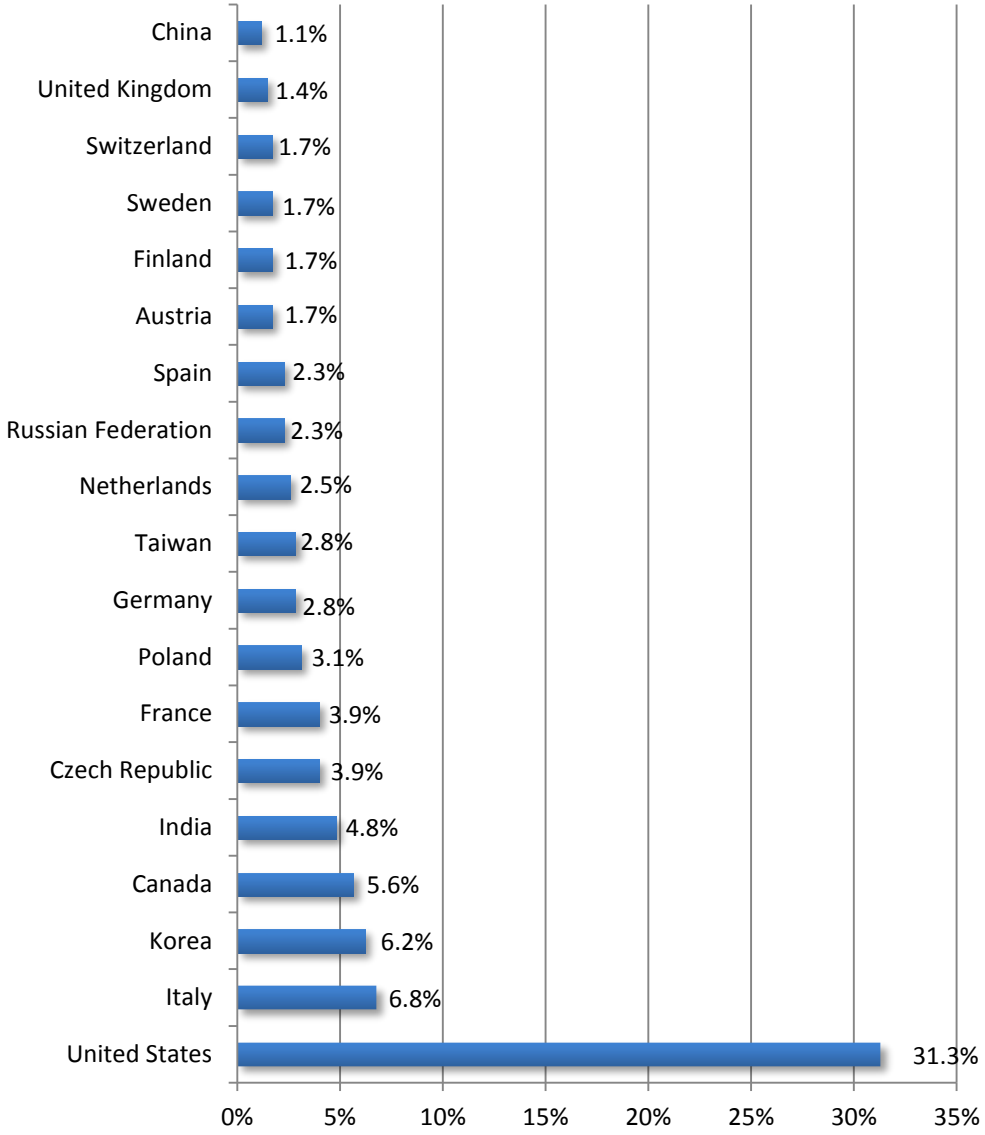


Fig. 12. ICS Allocation by Country

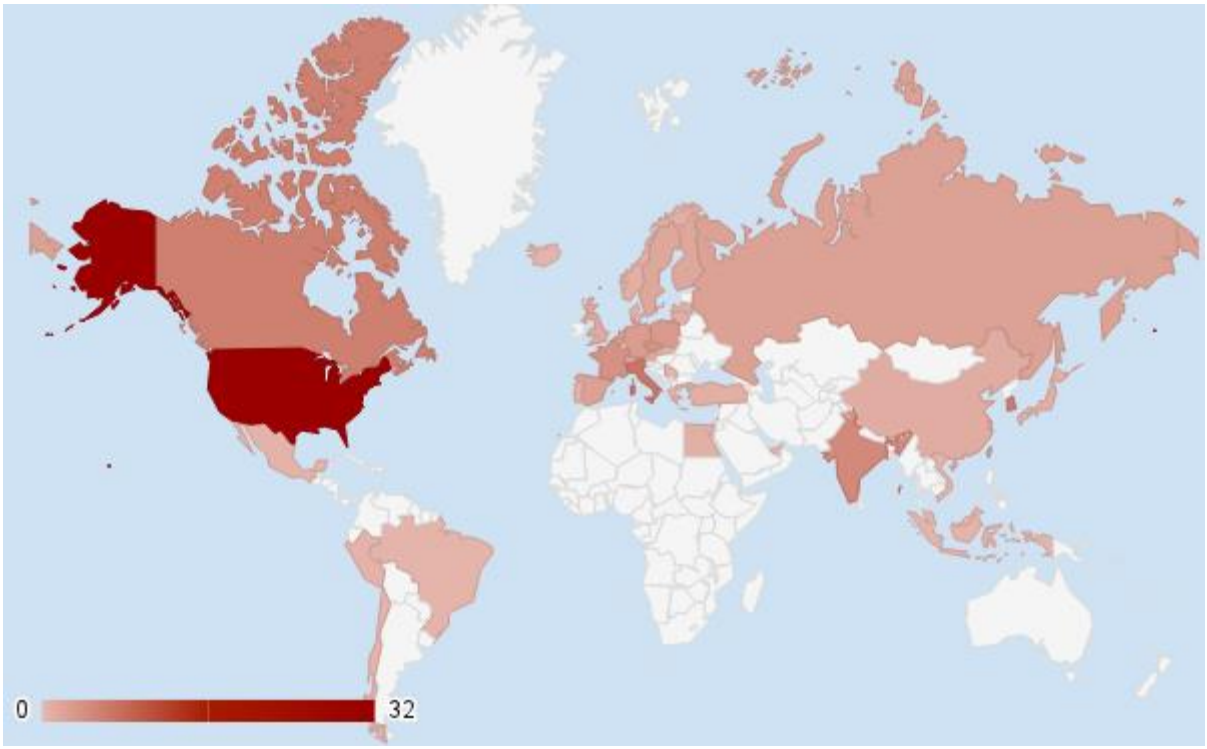


Fig. 13. ICS Allocation by Country

It is also interesting to consider the allocation of ICS systems by region as well as on the basis of individual countries. The highest concentration of ICS components available via the Internet is in Europe (41.41%), despite the modest numbers found in individual European countries. North America (37.46%) is second and Asia (12.39%) is in third place. These results are perhaps not surprising as the number of available systems directly depends on the degree of infrastructure automation.

Table 10. ICS Allocation by Region

Region	ICS, %
Europe	41.41
North America	37.46
Asia	12.39
India	4.79
MEA[2]	2.82
South America	1.13

[2] Middle East and Africa

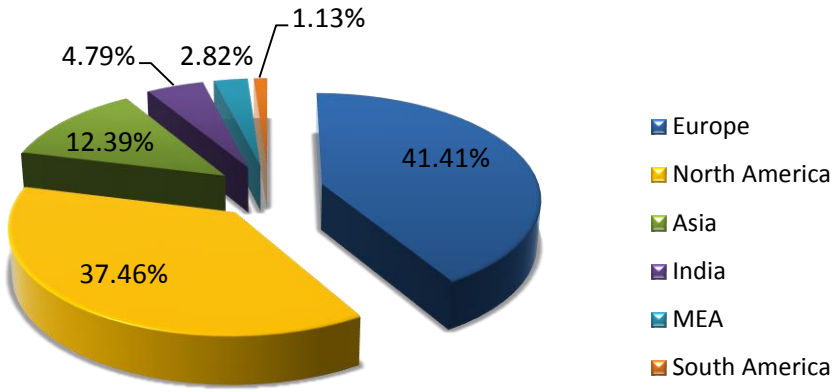


Fig. 14. ICS Allocation by Region

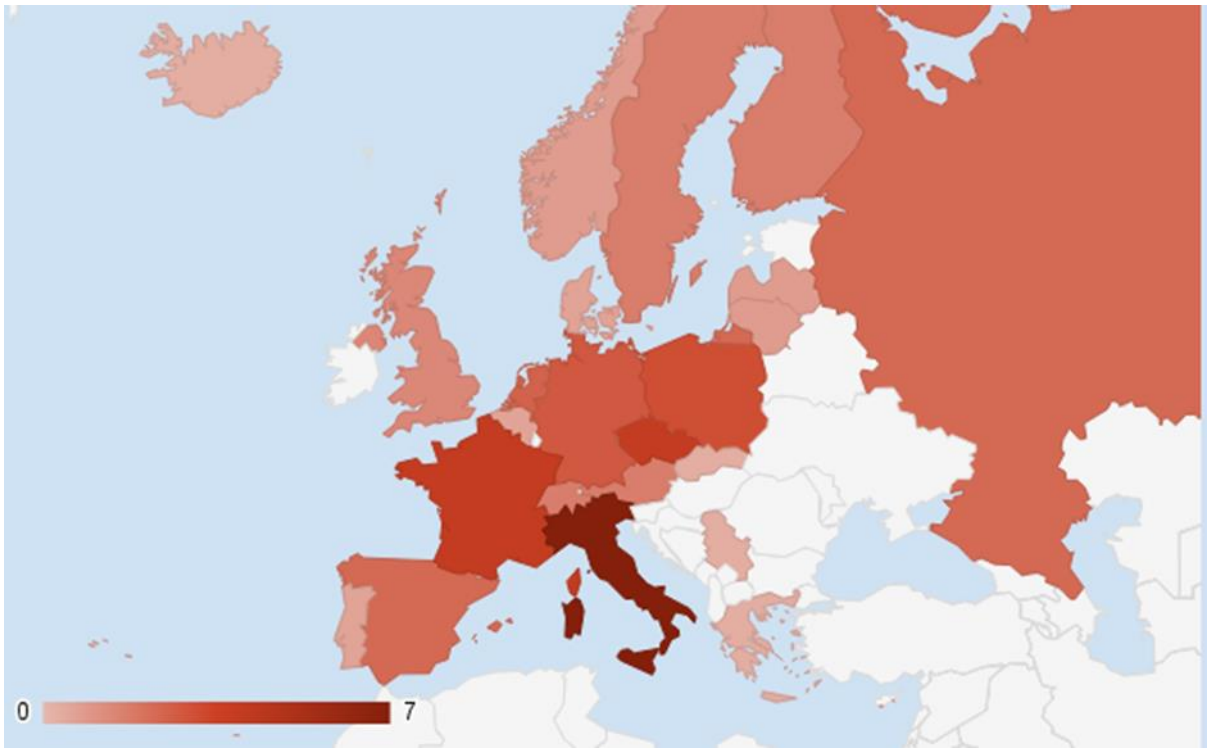


Fig. 15. ICS Allocation in Europe

4.2. Types of ICS Systems

The most common ICS elements accessible via the Internet are various SCADA components including HMI. These account for 70% of all ICS objects detected in our research. Another 27% of the ICS components are programmable logic controllers. Various

network devices used in ICS networks (referred to as “Hardware” in the following table) were detected in 3% of cases.

Table 11. ICS Component Types Detected via the Internet

Type	World Percentage, %
Hardware	3
HMI	27
PLC	27
SCADA	12
SCADA/HMI	31

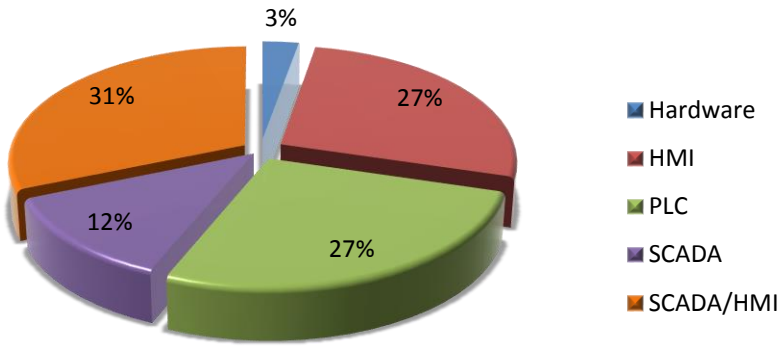


Fig. 16. ICS Component Types Detected via the Internet

4.3. Percentage of Vulnerable and Secure ICS Systems

At least 42% of ICS systems available from the Internet contain vulnerabilities which can be easily exploited by an attacker. Almost the same proportion (41%) of accessible systems are exposed to risk but, as noted above, passive analysis is not a reliable way of identifying vulnerabilities in these systems. Therefore, a significant portion of vulnerable ICS systems may be hidden in this unreachable area. In the course of our research we found only 17% of ICS systems to exhibit suitable levels of security.

Table 12. Percentage of Vulnerable and Secure ICS Systems

System Status	World Percentage, %
Secure	17
Unknown status	41
Vulnerable	42

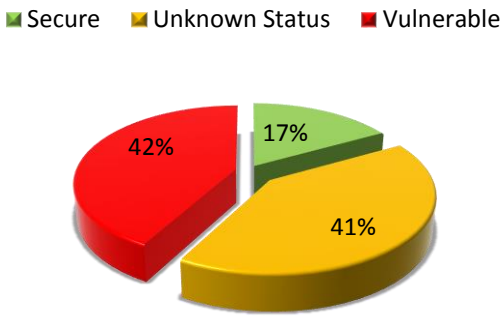


Fig. 17. Percentage of Vulnerable and Secure ICS Systems

4.4. Vulnerability Types

Security flaws related to configuration errors were the most common vulnerabilities, making up 36% of the detected cases. They include flawed password policies (as well as the use of default passwords), access to sensitive information and mistakes in the assignment of user rights. A quarter (25.35%) of all vulnerabilities were connected to failures to install the necessary security updates on the ICS system.

Table 13. Vulnerability Types

Vulnerability Type	World Percentage, %
Complex	41.97
Configuration Errors	36.06
Patch Management	25.35

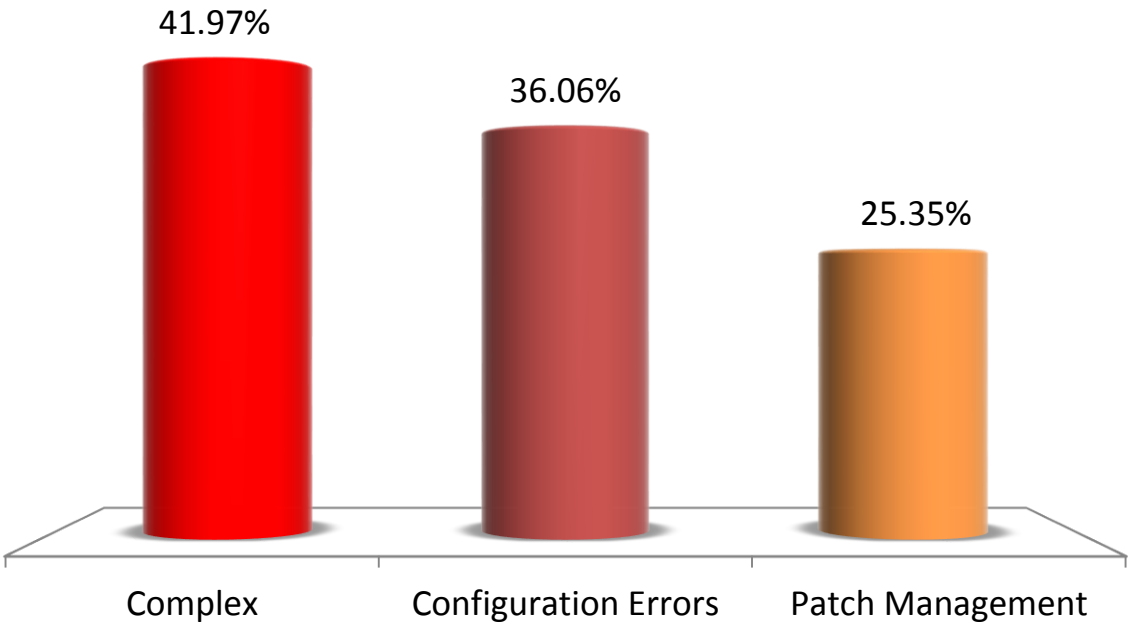


Fig. 18. Vulnerability Types

4.5. Percentage of Vulnerable ICS Systems by Country

Switzerland contains the highest percentage of vulnerable ICS systems available from the Internet – every single one of the country's ICS systems was found to be vulnerable. Second place belongs to the Czech Republic (86%) with Sweden in third (67%)[3]. In Russia, exactly half (50%) of ICS systems available from the Internet are vulnerable.

Table 14. Percentage of Vulnerable ICS Systems by Country

Country	Vulnerable ICS, %
Switzerland	100
Czech Republic	86
Sweden	67
Spain	63
Taiwan	60
United Kingdom	60
Russian Federation	50
Finland	50

[3] Table 14 and figure 19 show countries with a considerable number of SCADA systems available from the Internet.

Italy	42
United States	41
Poland	36
France	36
Netherlands	33
Austria	33
Korea	32
Canada	25
Germany	20
India	—
China	—

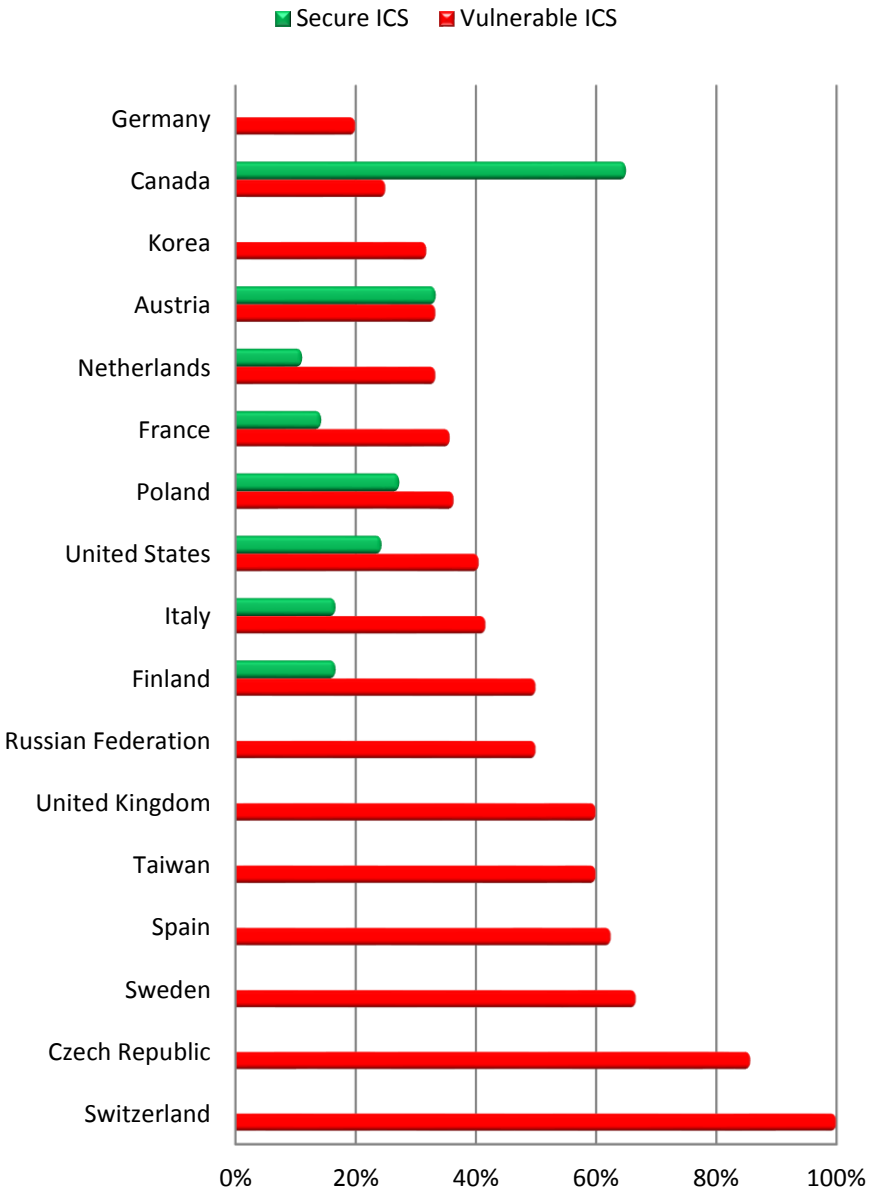


Fig. 19. Percentage of Vulnerable ICS Systems by Country

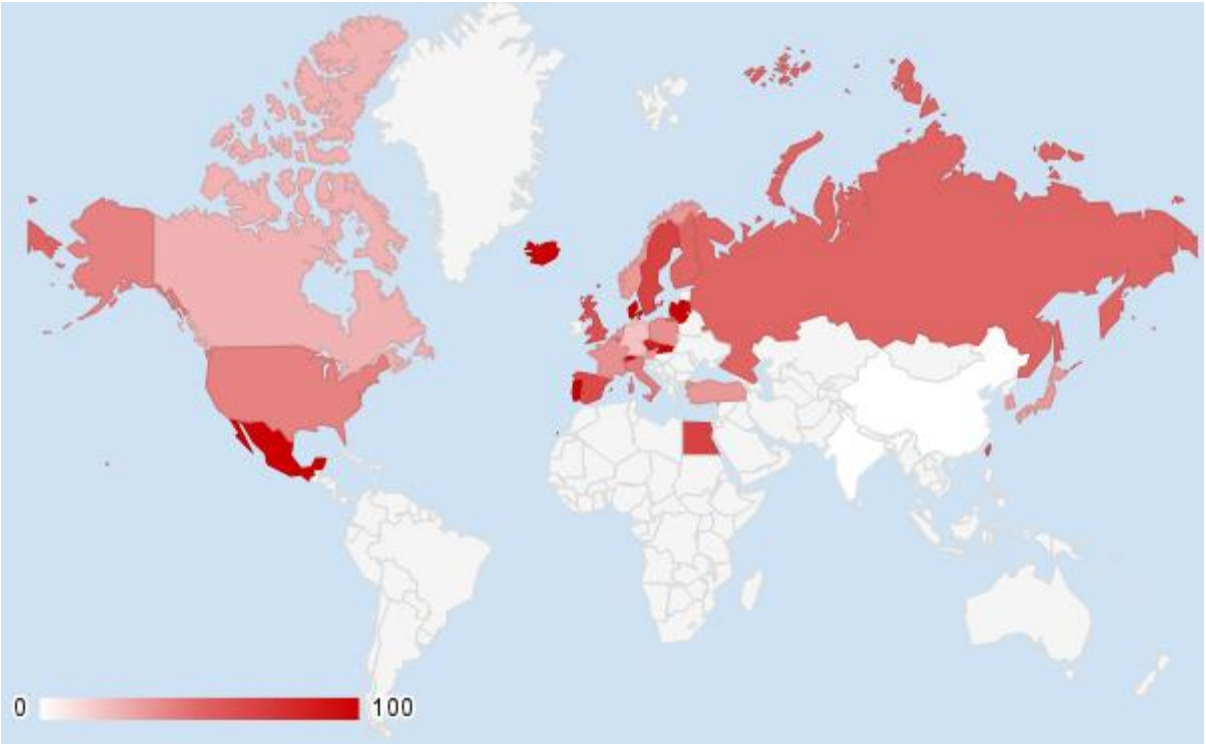


Fig. 20. Percentage of Vulnerable ICS Systems by Country

4.6. Percentage of Vulnerable ICS Systems by Region

Our research suggests Europe pays the least attention to ICS information security — 54% of industrial automation systems located in this region are vulnerable and can be attacked remotely. South America has the second highest level (39%) of vulnerability. Third place goes to Asia where, as is clear from the previous section, the main concentration of insecure systems fall in Taiwan and South Korea.

Table 15. Percentage of Vulnerable ICS Systems by Region

Region	Vulnerable ICS, %
Europe	54
North America	39
Asia	32
MEA	30
India	—
South America	—

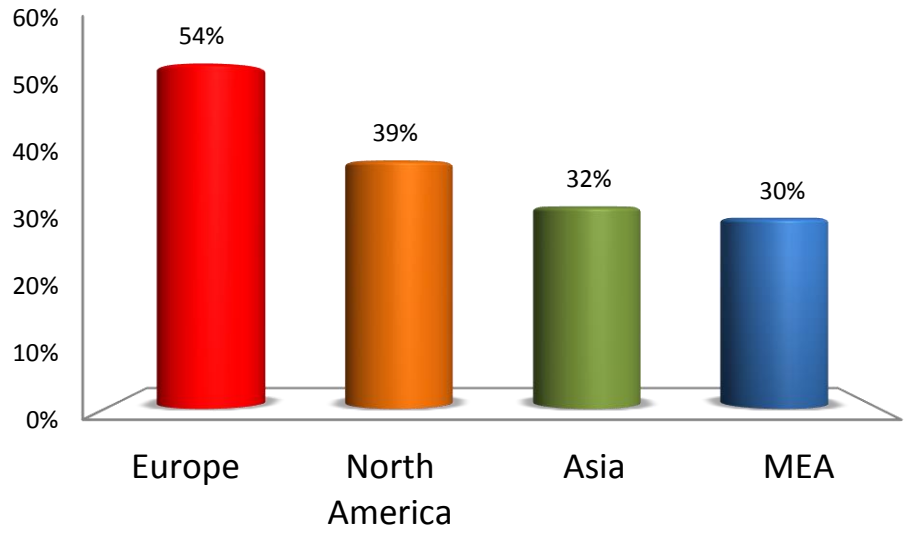


Fig. 21. Percentage of Vulnerable ICS Systems by Region

5. About Positive Technologies

Positive Technologies is a leading provider of vulnerability assessment, compliance management and threat analysis solutions to more than 1,000 global enterprise clients. We are among the world's most advanced specialist researchers, renowned security experts and highly-skilled programmers.

With one of the largest and most dynamic research facilities in the world, Positive Technologies carries out research, penetration testing and threat and vulnerability analysis on dozens of large-scale networks each year. As a result we have developed a unique understanding of how security should work, across a wide range of geographies and systems. We earned our reputation as one of the foremost authorities on SCADA, Banking, Telecom, Web Application and ERP security, anywhere.

Our solutions work seamlessly across your entire business: securing applications in development; assessing your network and application vulnerabilities; assuring your company's compliance with regulatory requirements and corporate standards; and blocking real-time attacks. Positive Technologies will give you complete confidence in the security of your network, its associated policies and its related applications.

Hands-on experience, underscored by a decade of service to clients worldwide, has enabled Positive Technologies to develop a thorough knowledge and understanding of vulnerability and compliance management that is unmatched. Our commitment to clients and track record of research excellence has earned Positive Technologies distinction as the #1 fastest growing Security and Vulnerability Management firm in 2012, as shown in an IDC report. We are not simply IT specialists. We are security experts.*

To learn more about Positive Technologies please visit www.ptsecurity.com

*Source: IDC Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares, doc #242465, August 2013. *Based on year-over-year revenue growth in 2012* for vendors with revenues of $20M+