POSITIVE TECHNOLOGIES

SCADA SAFETY IN NUMBERS

Gleb Gritsai

Alexander Timorin

Yury Goltsev

Roman Ilin

Sergey Gordeychik

Anton Karpin

2012

CONTENT

1. Introduction 3

2. Conclusions 4

3. Analysis of the Vulnerabilities in the ICS Systems 5

3.1. Analysis of the Vulnerabilities in the ICS Systems 5

3.2. Dynamics of Vulnerability Discovery 6

3.3. The Number of Vulnerabilities in the ICS systems of Various Vendors 7

3.4. Vulnerabilities Relating to ICS Hardware and Software Components 9

3.5. Classification of Vulnerabilities According to Their Types and Possible Consequences 10

3.6. Percentage of Fixed Vulnerabilities in ICS 11

3.7. Percentage of Vulnerabilities Fixed Promptly 13

3.8. Availability of information and software to conduct attacks 14

3.9. Number of exploits 14

3.10. Risk levels of detected vulnerabilities 15

3.11. SCADA non-fixed vulnerabilities 18

4. Popularity of ICS in the Internet 19

4.1. Frequency of ICS Systems 19

4.2. Types of ICS Systems 23

4.3. Percentage of Vulnerable and Secure ICS Systems 24

4.4. Vulnerability Types 24

4.5. Percentage of Vulnerable ICS Systems in Different Countries 25

4.6. Percentage of Vulnerable ICS Systems in Different Regions 28

5. About Positive Technologies 30

1. Introduction

Modern civilization is largely dependent on ICS/SCADA industrial process automation systems. The operation of nuclear power plants, hydroelectricity plants, oil and gas pipelines, and transport systems at national and world level are based on computer technology. Both the profit of a company and national security depend on control systems safety.

Industry systems security gained great interest not very long ago — after a series of incidents involving particular computer viruses, Flame and Stuxnet. It was then found that special services of foreign countries, competitive companies or cyber-terrorists are able to profit from the lack of attention paid to ICS/SCADA/PLC information security.

Threat modeling and imitating a potential attacker are essential in building a security system. It is necessary to understand what skills the attacker possesses and what scheme of attack may be chosen. In order to answer these questions, the experts of Positive Technologies explored ICS systems security. This report consists of 2 sections:

- Statistics on Vulnerabilities in the ICS Systems;
- Assessment of the Popularity of ICS on the Internet.

The subject of the investigation comprises the vulnerabilities that were discovered for the period from 2005 to October 1, 2012.

2. Conclusions

1. The history of industrial system security is divided into two parts — prior to Stuxnet and afterwards. 20 times more vulnerabilities have been detected since 2010 comparing with the previous five years.

<u>ICS in Figures:</u>

The number of detected vulnerabilities has increased by 20 times (since 2010). It takes more than a month to fix each fifth vulnerability.

50% of vulnerabilities allow a hacker to execute code.

There are exploits for 35% of vulnerabilities.

41% of vulnerabilities are critical. More than 40% of systems available from the Internet can be hacked by unprofessional users.

The third part of systems available from the Internet is located in the USA.

The fourth part of vulnerabilities is related to the lack of necessary security updates.

54% and 39% of systems available from the Internet in Europe and North America respectively are vulnerable.

2. The number of vulnerabilities keeps on growing rapidly in 2012. The number of security flaws found within ten months is far bigger than the number of flaws found during the whole previous period starting from 2005.

3. Vulnerabilities are primarily detected in the most common products, and the major part of vendors eliminate them quite quickly. However, each fifth vulnerability wasn't fixed within 30 days from the moment of its detection.

4. About 65% of vulnerabilities are rated as of high and critical severity. This figure significantly exceeds a similar index in IT systems, which proves a low information security level of ICS systems.

5. Exploitation of each second vulnerability allows an attacker to execute arbitrary code in the target ICS system.

6. More than 40% of SCADA systems available from the Internet are vulnerable and can be hacked by poorly trained malware users.

7. The USA and Europe lead in the number of ICS systems published in the Internet and demonstrate the most thoughtless attitude towards their security comparing with other regions.

8. More than a third of security flaws of available ICS systems are caused by configuration errors, including the use of default passwords.

9. The fourth part of vulnerabilities of available ICS systems is related to the lack of necessary security updates.

3. Analysis of the Vulnerabilities in the ICS Systems

3.1. Research Methodology

Information from different sources (e.g. vulnerability databases, vendors' notices, exploit packs, science conference reports, articles published on specialized sites and blogs) served as a basis for the research. It was necessary to analyze this broad spectrum of sources since cooperation between the community of information security researchers and the ICS vendors is just getting started and a lot of vulnerabilities are published without the developers' approval.

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:

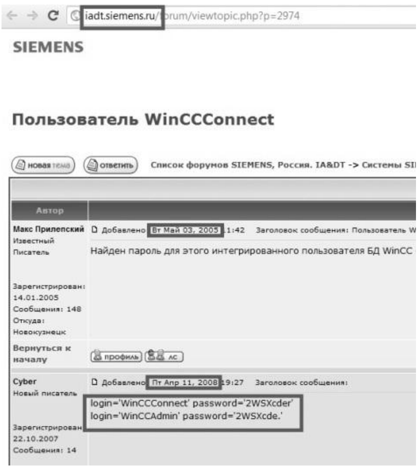
- SAINTexploit,
- Metasploit Framework,
- Immunity Canvas,
  - Agora Pack,
  - Agora SCADA+,
  - D2 Exploit Pack,
  - White Phosphorus exploit pack,
  - VulnDisco Exploit Pack.

For each vulnerability discovered, the experts searched for generally available methods of exploiting the vulnerability and provided an expert evaluation of the related risks.

3.2. Dynamics of Vulnerability Discovery

The specialists in information security discovered only 9 vulnerabilities for the period from 2005 to early 2010. Since the computer worm Stuxnet was discovered, both information security experts and hackers have showed deep interest in the subject. As a result, 64 vulnerabilities in ICS systems were discovered by the end of 2011. Moreover, for the first 8 month of 2012, 98 vulnerabilities were announced — more than in the previous years since 2005.

> ***A path from the discovery of vulnerabilities in SCADA to fixing them sometimes has to be a twisted 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 ago. It was first mentioned during the support forums in May, 2005. The passwords were published in April, 2008. The issue was fixed after the attack, in 2010.***



iadt.siemens.ru/forum/viewtopic.php?p=2974

Пользователь WinCCConnect

Список форумов SIEMENS, Россия. IA&DT -> Системы SI

Автор

Макс Прилепский
Известный Писатель
Зарегистрирован: 14.01.2005
Сообщения: 148
Откуда: Новокузнецк

Добавлено: Вт Май 03, 2005 1:42 Заголовок сообщения: Пользователь W

Найден пароль для этого интегрированного пользователя БД WinCC

Вернуться к началу

Cyber
Новый писатель
Зарегистрирован: 22.10.2007
Сообщения: 14

Добавлено: Пт Апр 11, 2008 19:27 Заголовок сообщения:

login='WinCCConnect' password='2WSXcder'
login='WinCCAdmin' password='2WSXcde.'

Tab. 1. The Number of Vulnerabilities Discovered

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

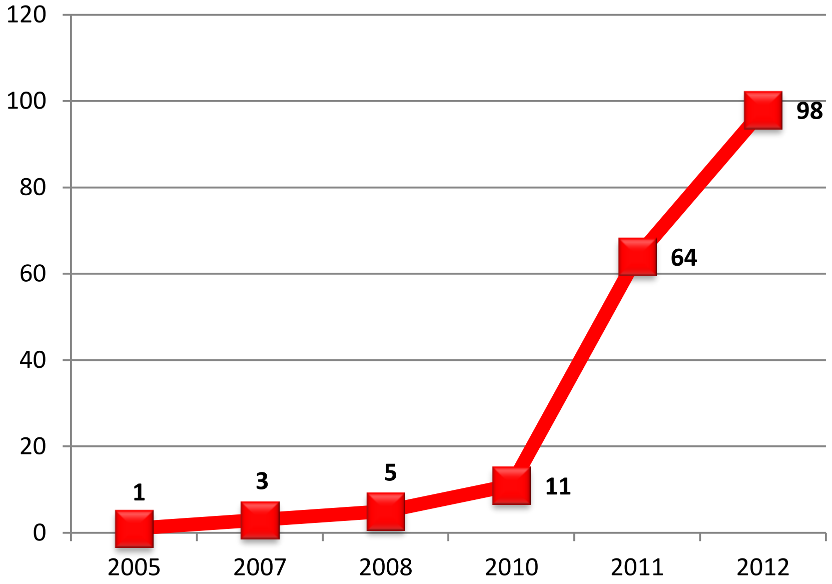


Figure 1. Dynamics of the Number of Vulnerabilities

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

The highest number of vulnerabilities for the reporting period (42) was discovered in the components of the ICS developed by Siemens. The second place goes to Broadwin/Advantech (22 vulnerabilities); the third, to Schneider Electric (18 vulnerabilities).

Tab. 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	7-Technologies	12
Lantronix	3	General Electric	15
Progea	3	Invensys Wonderware	15
ABB	3	Schneider Electric	18
Sielco Sistemi	3	Advantech/Broadwin	22
Iconics	5	Siemens	42
Measuresoft	6	Emerson	6
Ecava	5	Rockwell Automation	9
Emerson	6		

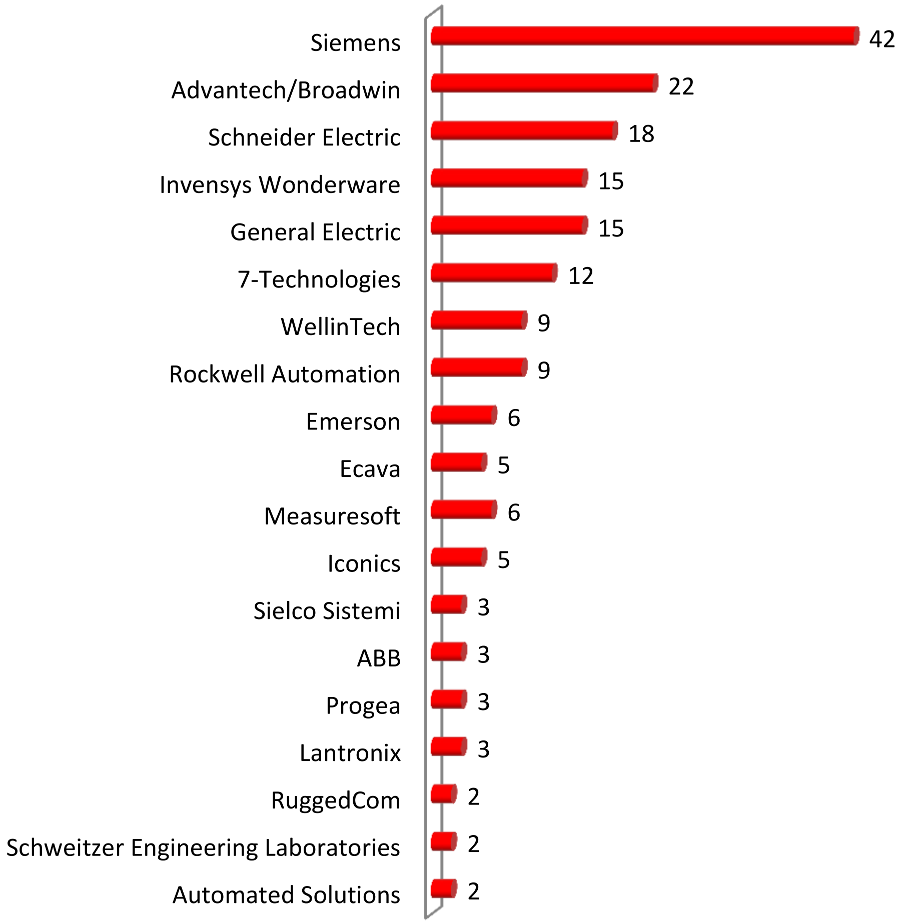


Figure 2. The Number of Vulnerabilities in the ICS Systems of Various Vendors

The highest number of vulnerabilities in ICS (also true for other systems) was discovered in the most common components. Moreover, a number of vendors changed their approach from reactive to proactive and took resolute measures to find and fix vulnerabilities in their products. For instance, Siemens organized a specialized department, Siemens ProductCERT (http://www.siemens.com/corporate-technology/en/research-areas/siemens-cert-security-advisories.htm), whose main goal is to discover and fix security issues in the company's products. The vulnerabilities discovered by the team are also included in the general statistics; thus the number of discovered and fixed issues is increasing.

3.4. Vulnerabilities Relating to ICS Hardware and Software Components

Such ICS components as SCADA systems and human machine interface (HMI) are present a significant interest for attackers: 87 and 49 vulnerabilities were discovered, respectively, in these systems. For the reporting period, the experts discovered 20 vulnerabilities in the programmable logic controllers of different vendors.

Tab. 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

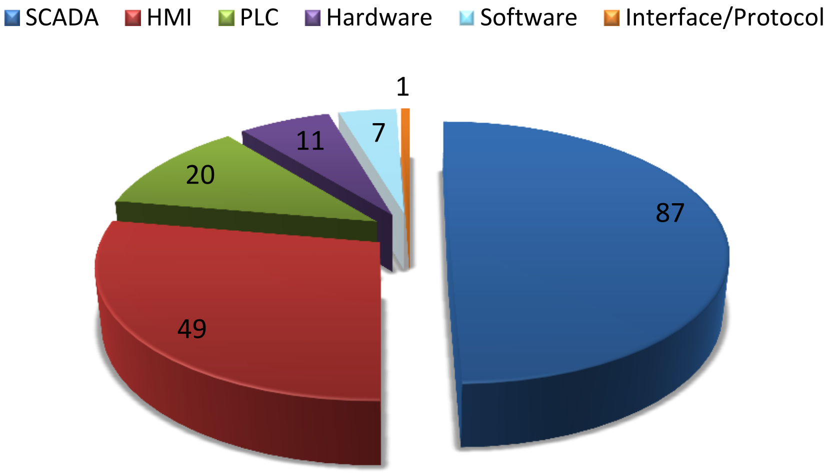


Figure 3. The Number of Vulnerabilities in Different Types of ICS Component

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

Over a third of vulnerabilities (36%) are associated with the 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 premature ending of a program or freeze (which leads to denial of service), but also to execute arbitrary code in the target system. The types of vulnerability which allow the attacker to execute code (Buffer Overflow, Remote Code Execution) make up 50% of all vulnerabilities (an extremely high figure!). We should also consider the large number of problems in Authentication and Key Management — almost 23%.

> ***The recent rapid growth of the vulnerabilities discovered in ICS is caused by the ethical hackers getting involved in the process. The Positive Research Center experts discovered more than 50 vulnerabilities in different products in 2012, the most part of which has already been fixed by the vendors. A lot of work in coordination of the vulnerability fixing process is carried out by ICS CERT.***

Tab. 4. Classification of Vulnerabilities in ICS According to Type

Vulnerability Type	Vulnerability Percentage, %
Buffer Overflow	36
Remote Code Execution	13,14
Web (client-side)	9,14
Web (server-side)	10,86
Local Privilege Escalation	2,29
DoS/Data Integrity	5,71
Authentication / Key Management	22,86

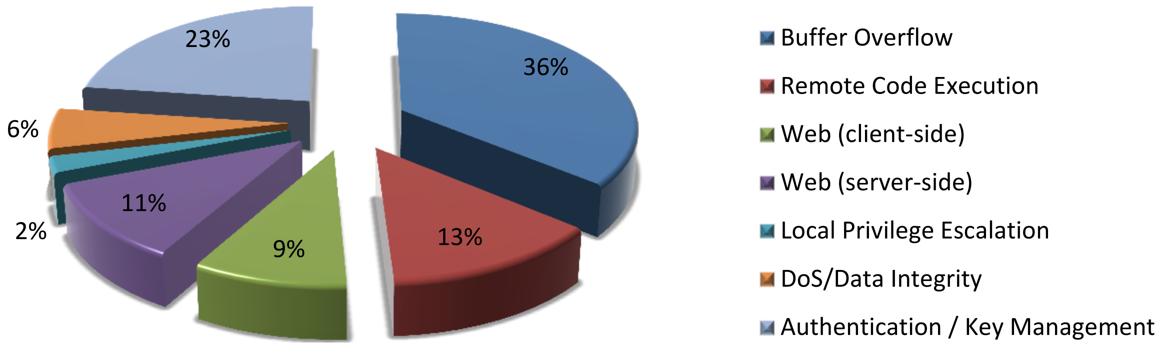


Figure 4. Classification of Vulnerabilities in ICS According to Type

3.6. Percentage of Fixed Vulnerabilities in ICS

A display of fixed vulnerabilities percentage gives a clear view on how serious ICS vendors are about information security issues. For instance, Siemens fixed and released patches for 88% of vulnerabilities, while Schneider Electric fixed only 56% of security defects.

Tab. 5. Percentage of Fixed Vulnerabilities in ICS

Vendor	**Fixed, %**
Advantech/Broadwin	91
WellinTech	89
Siemens	88
General Electric	80
Rockwell Automation	78
ABB	67
Schneider Electric	56
Lantronix	—
Schweitzer Engineering Laboratories	—
Total	**78**

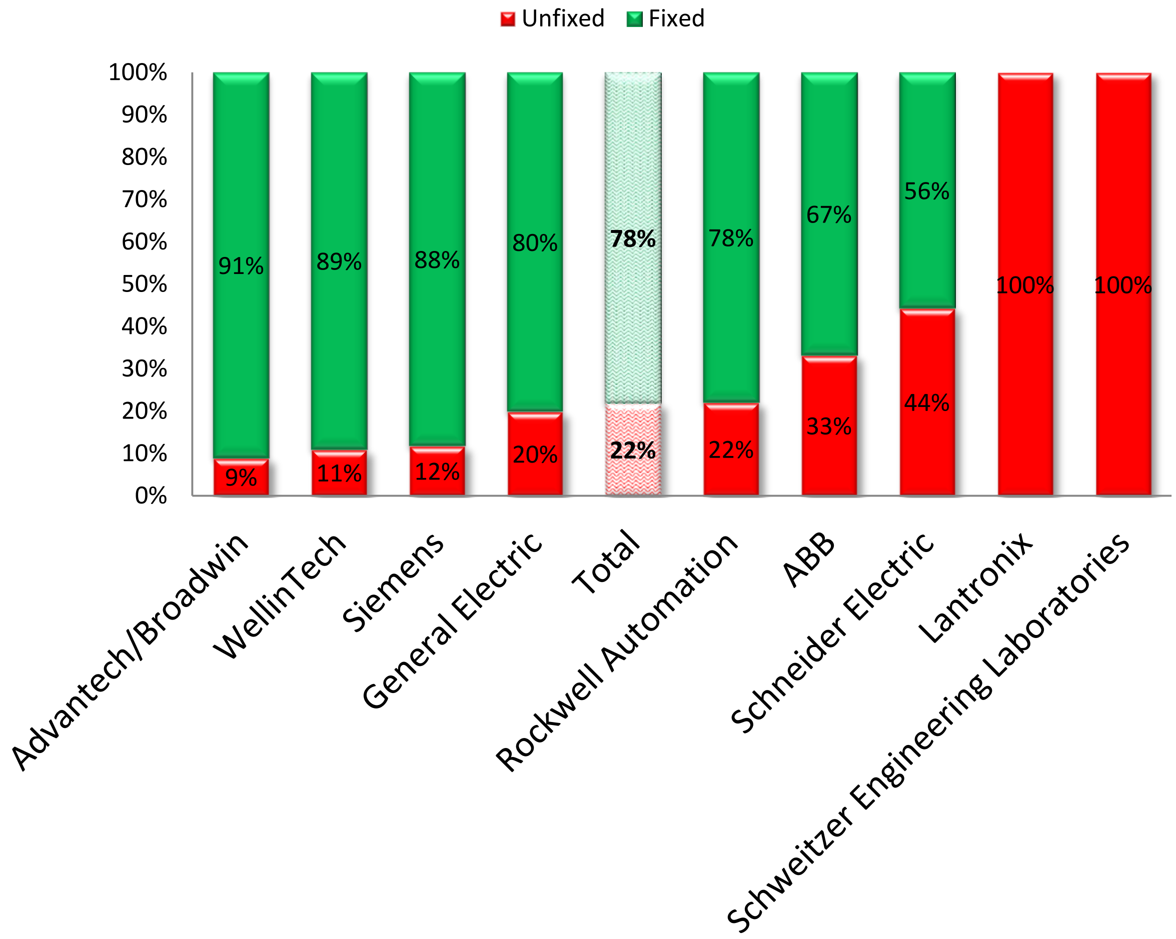
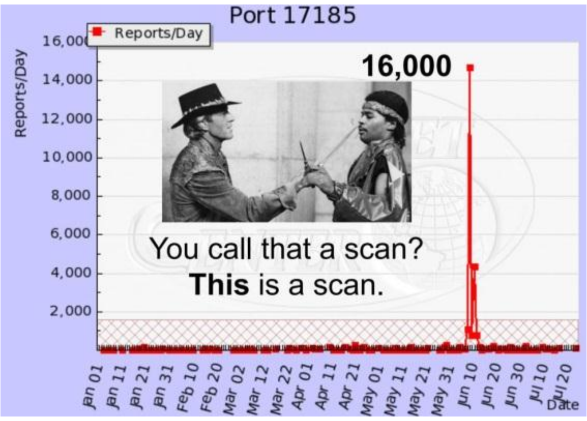


Figure 5. Percentage of Fixed Vulnerabilities in ICS

3.7. Percentage of Vulnerabilities Fixed Promptly

Most security defects (81%) have been fixed rather efficiently by ICS component vendors before they became widely known or within 30 days of uncoordinated disclosure. Approximately every fifth vulnerability was fixed with a significant delay, or was even not fixed in certain cases.

> ***August 2010 note US-CERT VU#362332 was published; it reported on a dangerous vulnerability in the real-time system VxWorks, which is used in industry systems. According to HD Moore, he discovered more than 250,000 vulnerable systems which were accessible through the Internet.***



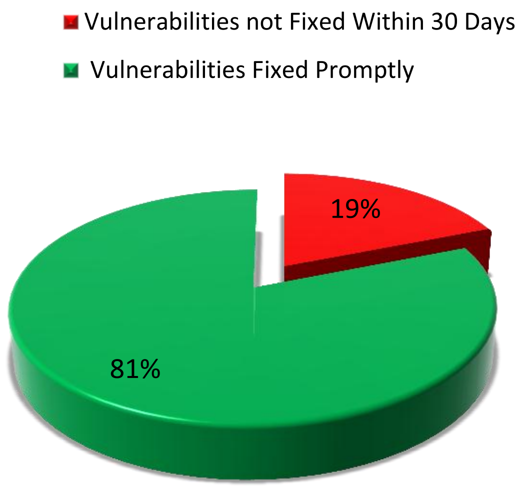


Figure 6. Percentage of Vulnerabilities Fixed Promptly

3.8. Availability of information and software to conduct attacks

If there are ready-to-use tools to exploit the vulnerability in the public domain, it is much more possible that the attack will be conducted successfully. Now for 35% of all known SCADA vulnerabilities exploits have been issued, which are available as single utilities, parts of penetration testing software or are described in security bulletins.

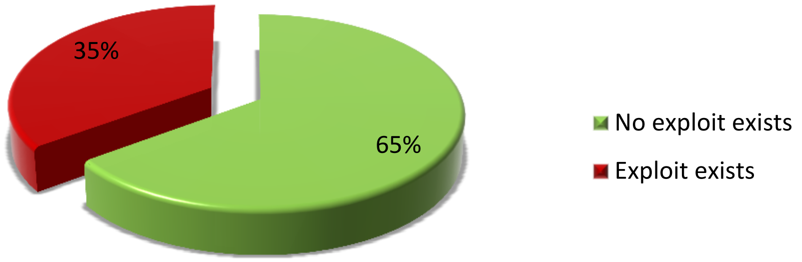


Figure 7. Part of vulnerabilities that have exploits

Please note that 35% is rather a high value for the number of available SCADA exploits: it is several times higher than the corresponding rate for IT systems as a whole.

3.9. Number of exploits

As a rule, the number of detected vulnerabilities correlates with the number of published exploits. 50 exploits were published starting in 2011 and up to September 2012: this is six times greater than the corresponding rate for the period 2005 - 2010.

Tab. 6. Number of published exploits

Year	Number of exploits
2008	2
2010	6
2011	30

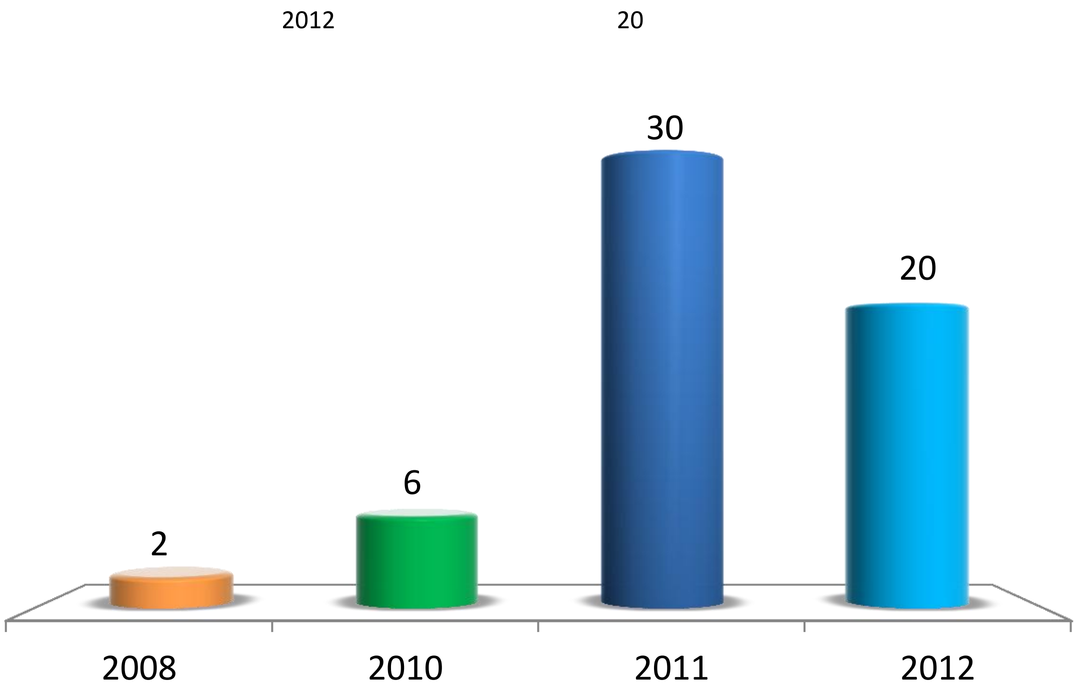


Figure 1. Number of published exploits

The number of exploits published in 2012 is rather small. There are two possible reasons:

- Relationships between SCADA vendors and explorers are put in order: responsible disclosure policy is 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 of vulnerabilities (about 65%) are of high or critical level[1].

[1] Vulnerabilities of high level have CVSS v2 Base Score value > 6,5. Vulnerabilities of critical level are vulnerabilities of high level with known exploits.

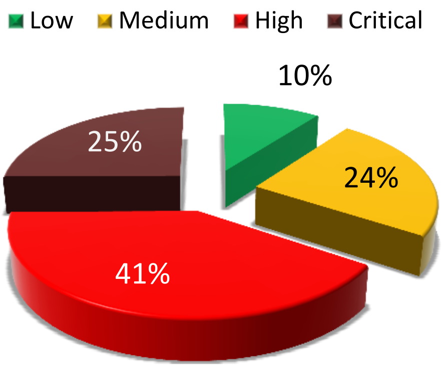


Figure 2. Vulnerabilities by risk level

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

Tab. 7. SCADA 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
Schneider Electric	28	11	39	22
ABB	33	67	—	—
Ecava	33	17	33	17
Measuresoft	40	40	20	—
Iconics	40	40	—	20
Automated Solutions	50	50	—	—
7-Technologies	50	42	8	—
WellinTech	56	33	11	—
Progea	67	33	—	—
Sielco Sistemi	67	33	—	—
RuggedCom	100	—	—	—

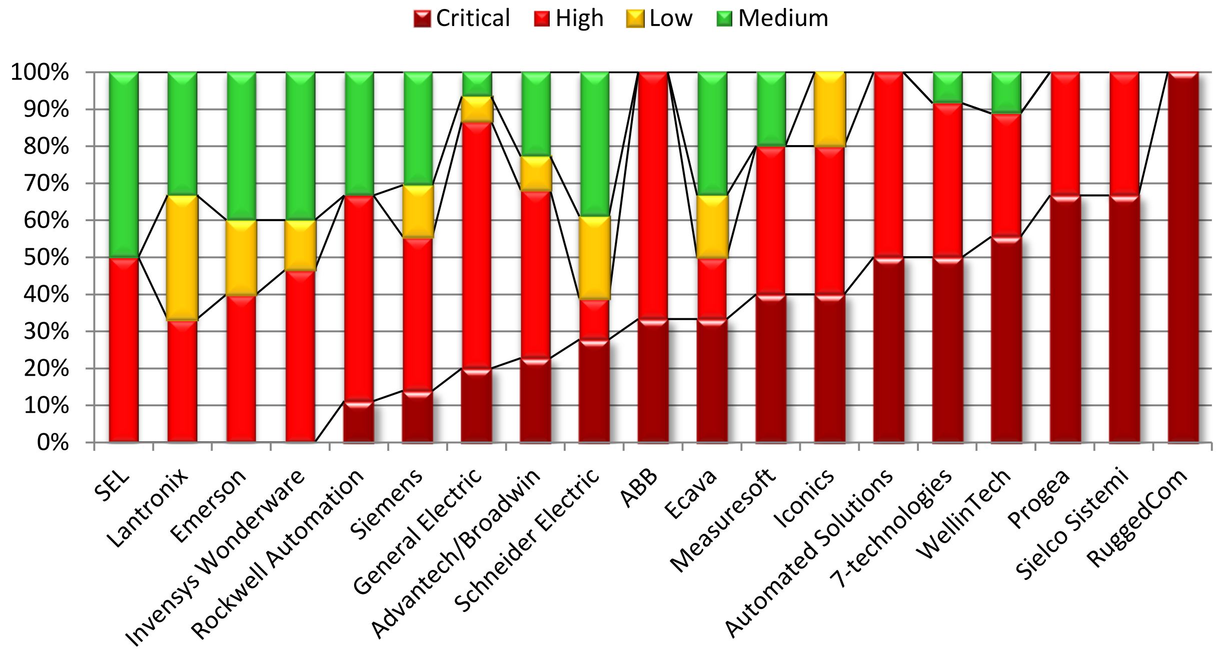
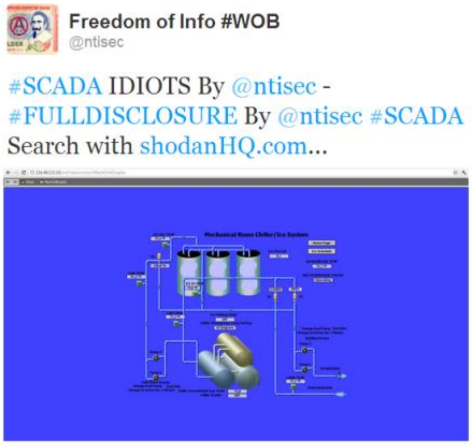


Figure 3. SCADA vulnerabilties by risk level

If there are no methods to conduct the attack, the possibility that SCADA components by SEL, Lantronix, Emerson and Invensys will be attacked is lower, but is not ruled out. As a rule, an attack against an industrial enterprise is a kind of multi-move game played by experienced experts who do not need “exploit packs” and other tools intended for “ordinary” hackers.

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



Freedom of Info #WOB
@ntisec

#SCADA IDIOTS By @ntisec - #FULLDISCLOSURE By @ntisec #SCADA Search with shodanHQ.com...

3.11. SCADA non-fixed vulnerabilities

Vulnerabilities for which there are already means of attack, but no means of resistance, provide the greatest risk. If there is a vulnerability and a fix has not been issued, the risk that the system can be compromised is rather high, as an attacker does not need deep knowledge and a protracted period to prepare for the attack. Moreover, the attack can be conducted by hooligans. The most grievous situation concerns Schneider Electric SCADA components, where six vulnerabilities were detected. The second place goes to General Electric (3 vulnerabilities); the third and fourth places are between Advantech/Broadwin and Rockwell Automation, with one open vulnerability.

Tab. 8. Number of SCADA non-fixed vulnerabilities with exploits

Vendor	Number of vulnerabilities
Advantech/Broadwin	1
Rockwell Automation	1
General Electric	3
Schneider Electric	6

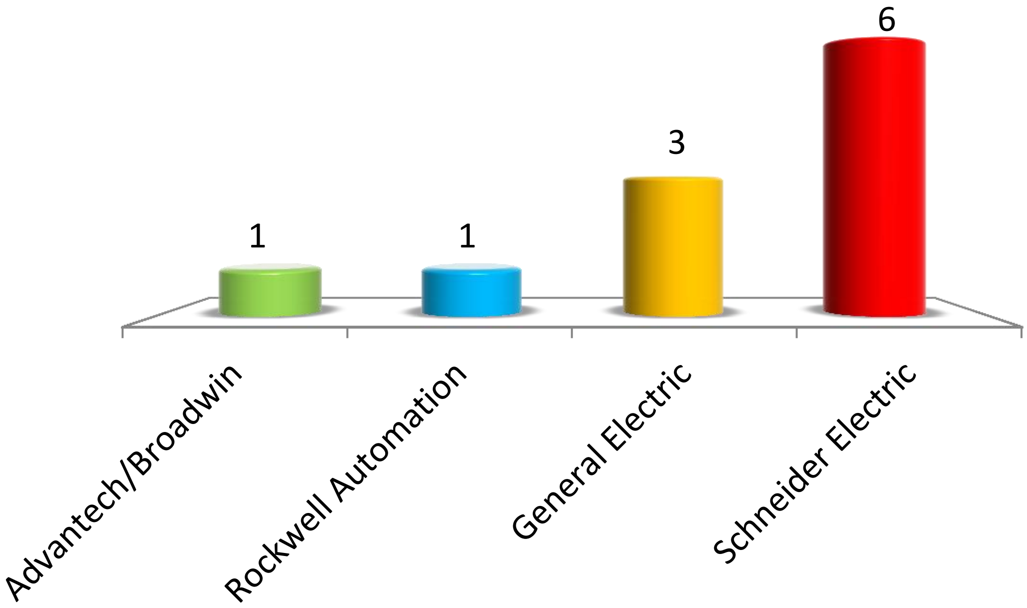


Figure 4. Number of SCADA non-fixed vulnerabilities with exploits

4. Popularity of ICS in the Internet

To understand to what extent the vulnerabilities described above can be used by an attacker, the Internet has been assessed in relation to vulnerable ICS. Passive analysis together with search engines (Google, Yahoo, Bing) and specialized databases such as ShodanHQ, Every Routable IP Project were employed to search and check system versions. The obtained information was analyzed from the point of view of vulnerabilities related to configuration management and updates installation.

Unfortunately, the passive technique cannot be reliable in identifying all detected vulnerabilities, that is why the major part of the information in this section should be considered as a positive script: in case of a detailed analysis, the number of detected vulnerabilities will certainly increase.

4.1. Frequency of ICS Systems

Almost the third part of the ICS systems, which elements can be accessed from the Internet, are located in the USA (31.3%). Italy follows far behind (6.8%), South Korea rounds out the top three (6.2%). Russia holds the 12th place with 2.3%, and only 1.1% of ICS systems available from the global network are located in China.

Table 12. ICS Allocation by Countries

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

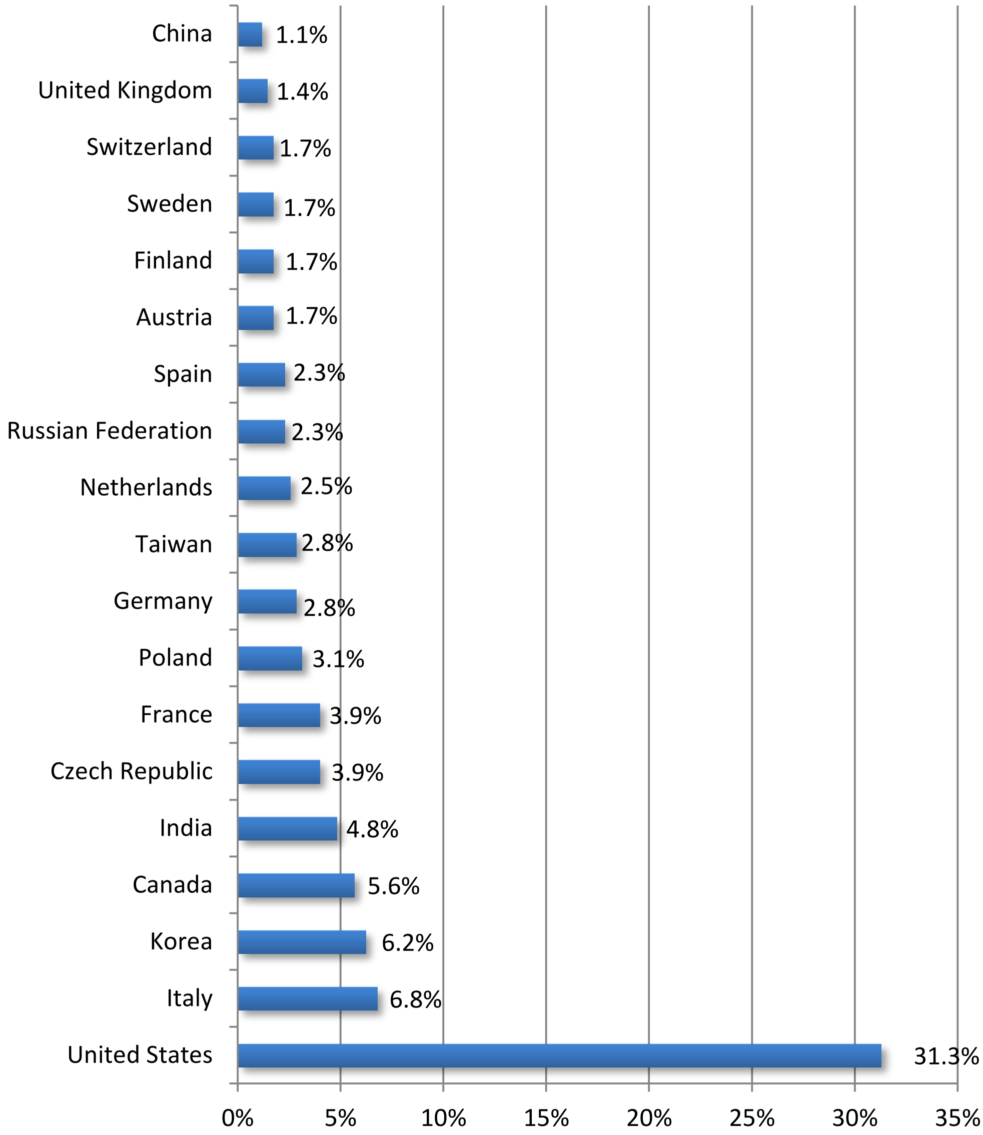


Fig. 12. ICS Allocation by Countries

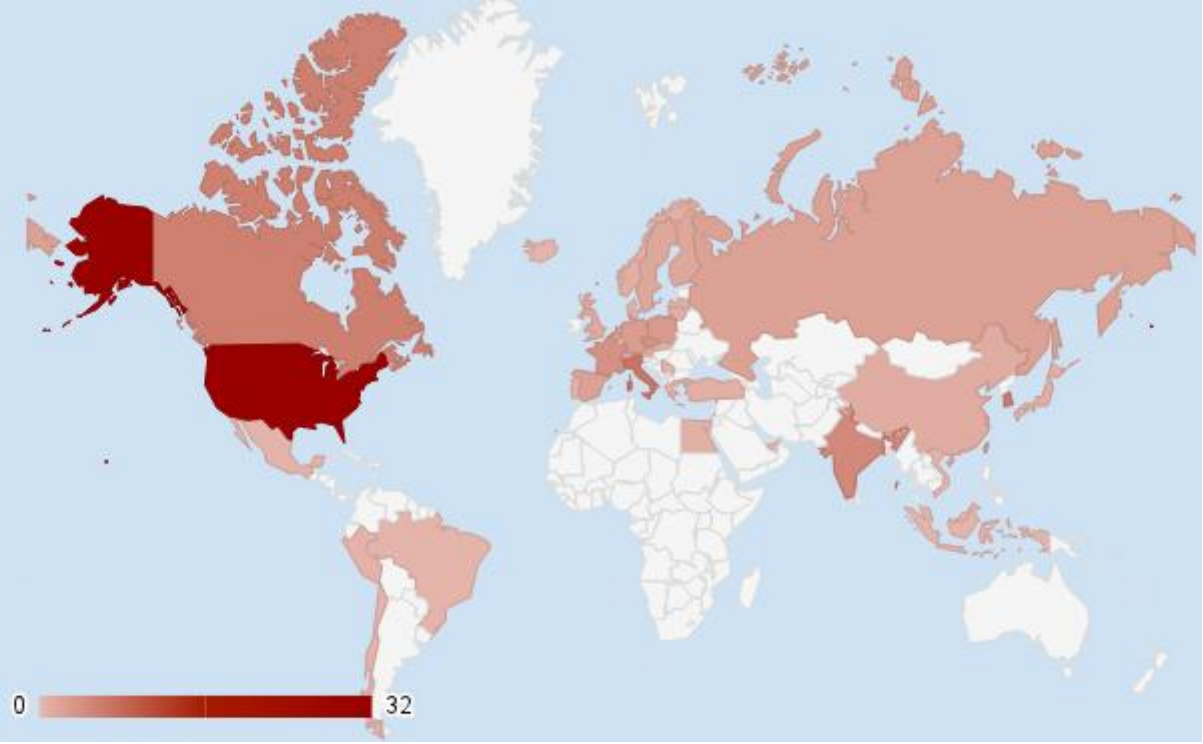


Fig. 13. ICS Allocation by Countries

The ICS components available from the Internet are concentrated in the European region (41.41%) despite the modest numbers in individual countries. South America lags behind the Old World (37.46%), Asia holds the third place (12.39%).

Table 13. ICS Allocation by Regions

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

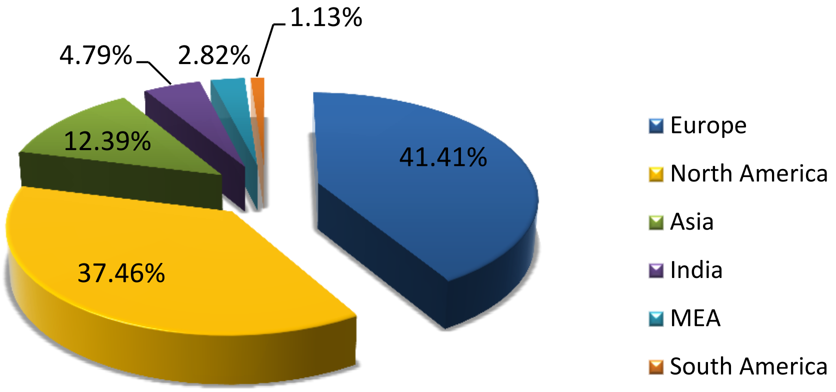


Fig. 14. ICS Allocation by Regions

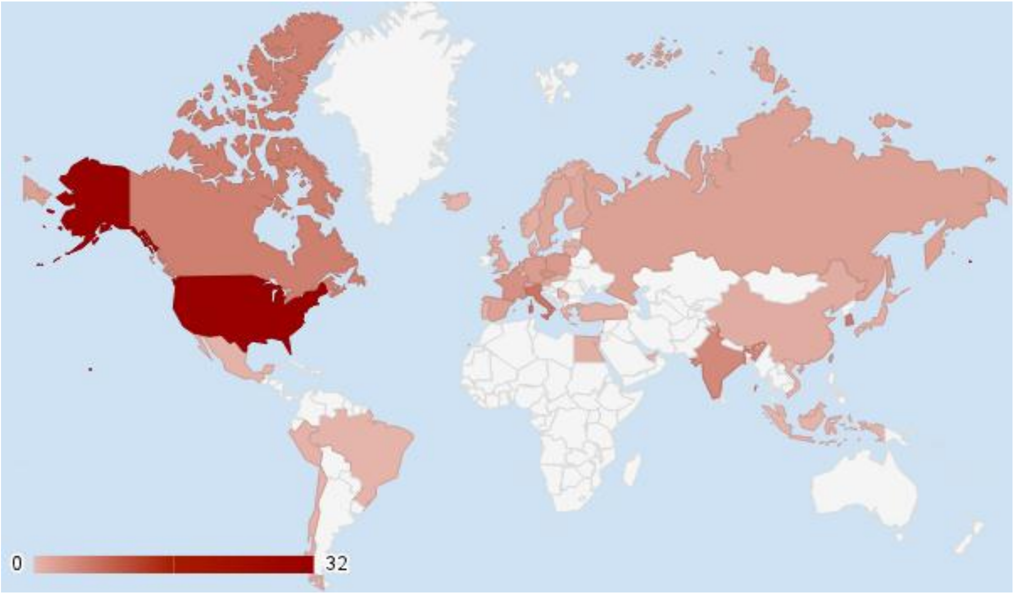


Fig. 15. ICS Allocation in Europe

These results can be anticipated, because the number of available systems directly depends on the degree of infrastructure automation.

4.2. Types of ICS Systems

Most often the global network contains various SCADA components including HMI. They account for 70% of all detected objects. Another 27% of the ICS components are programmable logic controllers. Various network devices used in ICS networks (referred to as the Hardware in the following table) were detected in 3% of cases.

Table 14. ICS Components

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

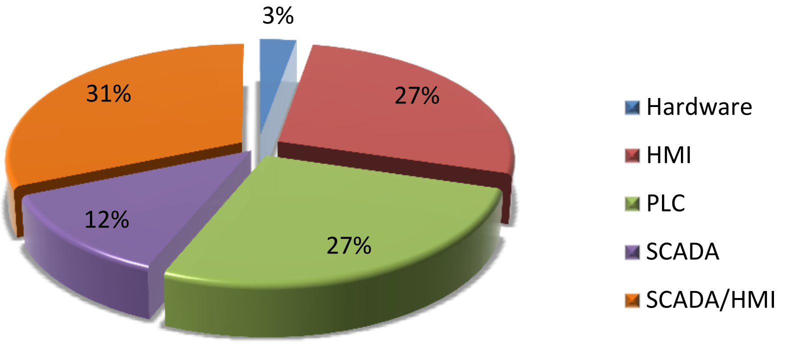


Fig. 16. Types of ICS Systems

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 number of systems (41%) are exposed to risk, but as it was mentioned above passive analysis is far from being reliable in identifying vulnerabilities detected in them. Therefore, a significant part of vulnerable ICS systems may hide in this unreachable area. The systems, which were proved secure in the course of the research, comprise only 17%.

Table 15. Percentage of Vulnerable and Secure ICS Systems

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

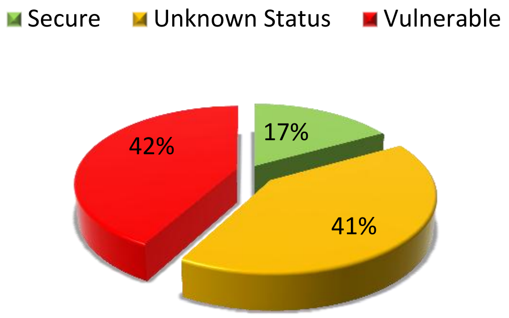


Fig. 17. Percentage of Vulnerable and Secure ICS Systems

4.4. Vulnerability Types

Security flaws related to configuration errors being the most common vulnerabilities were detected in 36% of cases. They include an incorrect password policy (as well as the use of default passwords), access to sensitive information, wrong restriction of user rights, and etc. The fourth part of vulnerabilities (25.35%) is connected with the lack of necessary security updates.

Table 16. Vulnerability Types

Vulnerability Type	World Percentage, %
Complex	41.97
Configuration errors	36.06
Patch management	25.35

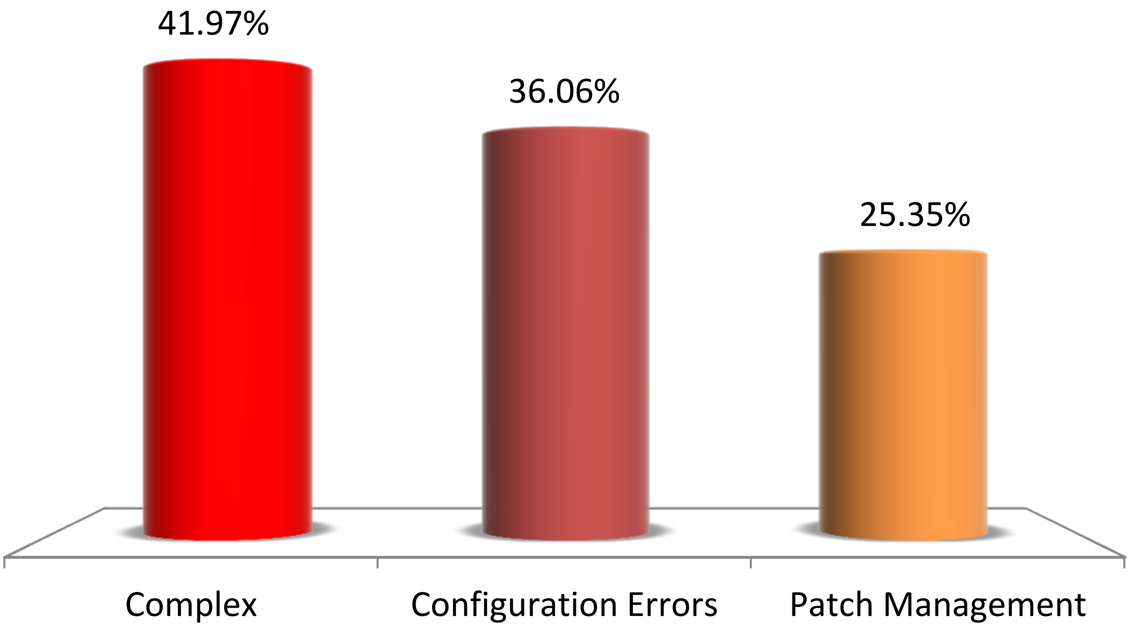


Fig. 18. Vulnerability Types

4.5. Percentage of Vulnerable ICS Systems in Different Countries

Switzerland contains the major part of vulnerable ICS systems available from the Internet. All similar systems are vulnerable in this country. The second place belongs to the Czech Republic (86%), the third — to Sweden (67%)[3]. Exactly the half (50%) of ICS systems available from the Internet are vulnerable in Russia.

[3] Table 17 and picture 19 shows countries with a considerable number of SCADA systems available from the Internet.

Table 17. Percentage of Vulnerable ICS Systems in Different Countries

Country	Vulnerable ICS, %
Switzerland	100
Czech Republic	86
Sweden	67
Spain	63
Taiwan	60
United Kingdom	60
Russian Federation	50
Finland	50
Italy	42
United States	41
Poland	36
France	36
Netherlands	33
Austria	33
Korea	32
Canada	25
Germany	20
India	—
China	—

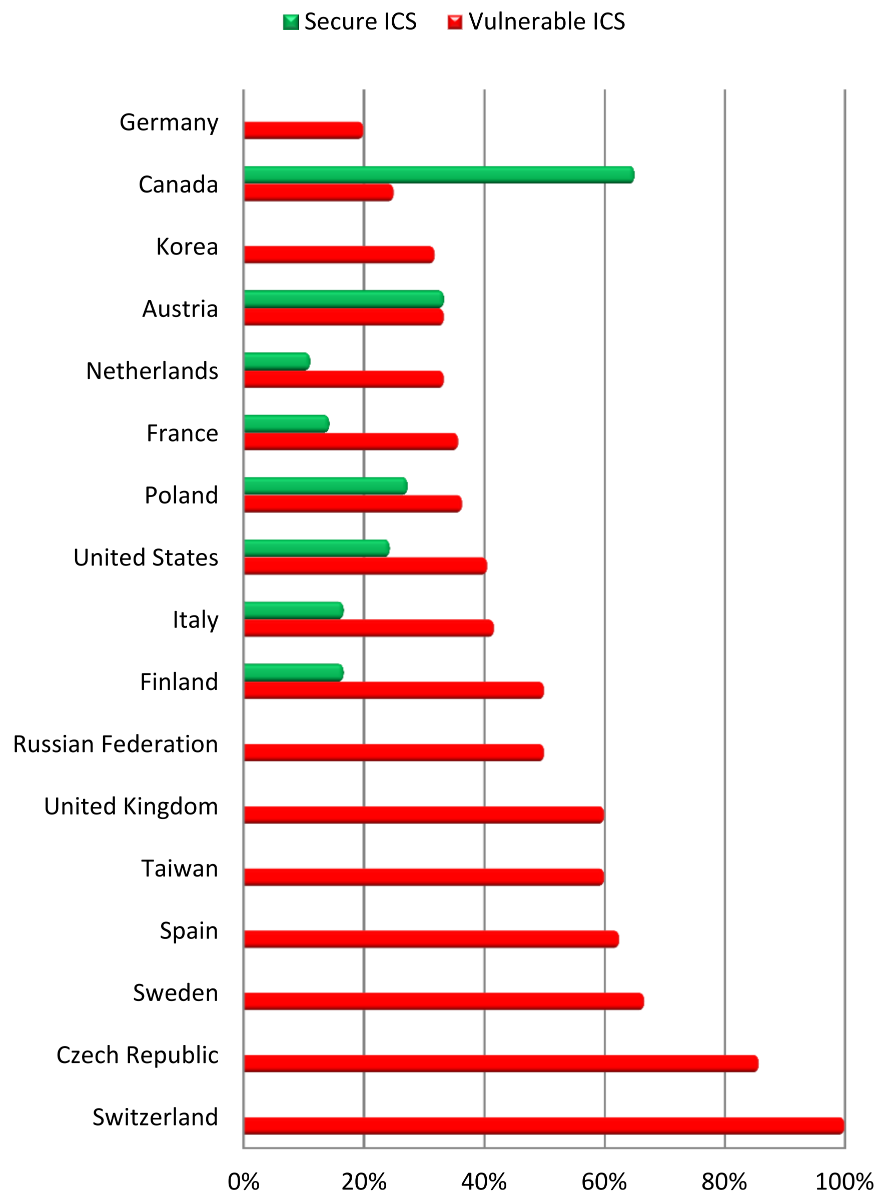


Fig. 19. Percentage of Vulnerable ICS Systems in Different Countries

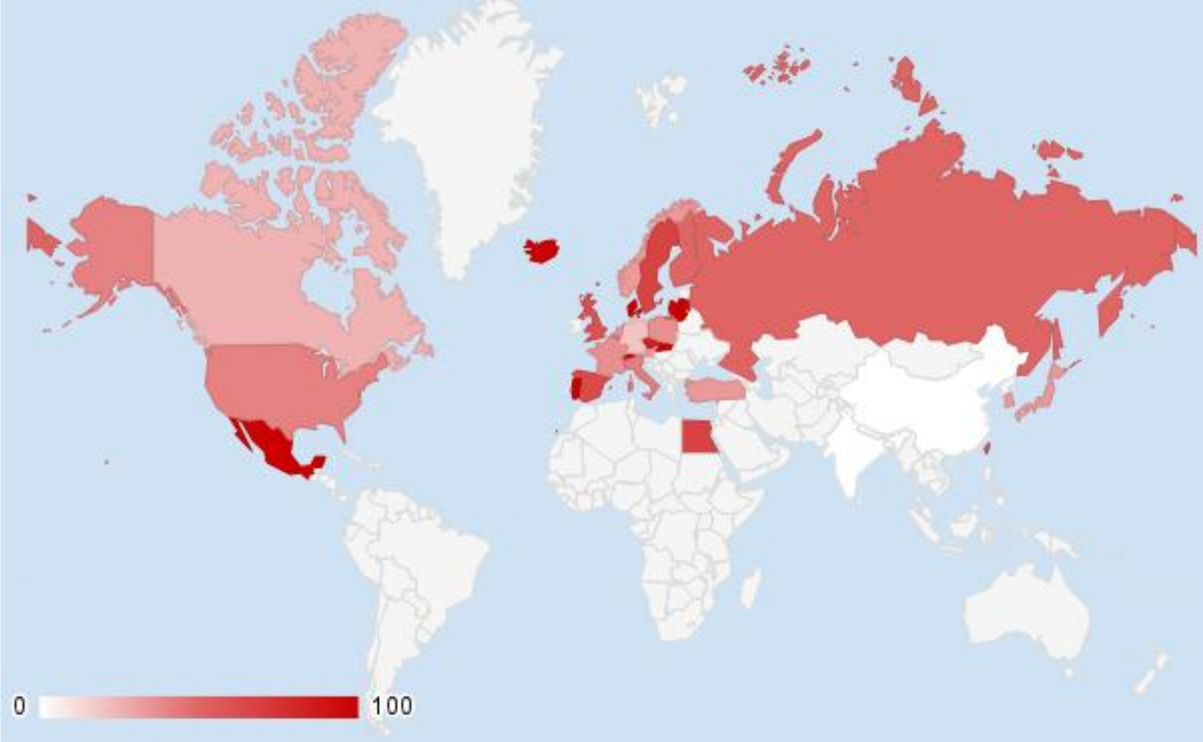


Fig. 20. Percentage of Vulnerable ICS Systems in Different Countries

4.6. Percentage of Vulnerable ICS Systems in Different Regions

Europe pays the least attention to the issues of the ICS information security — 54% of industrial automation systems located in this region are vulnerable and can be attacked remotely. South America is the second (39%), the third is Asia, where, as it is clear from the previous section, insecure objects in Taiwan and South Korea are of the essence.

Table 18. Percentage of Vulnerable ICS Systems in Different Regions

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

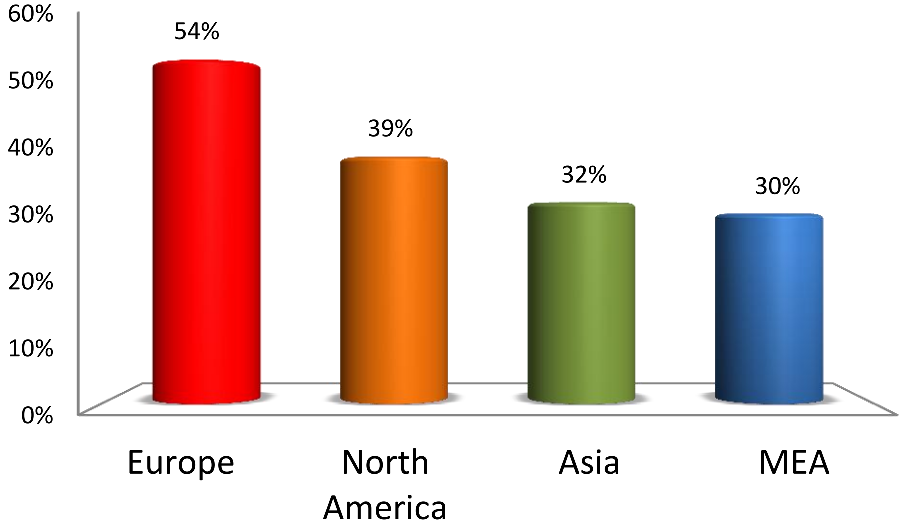


Fig. 21. Percentage of Vulnerable ICS Systems in Different Regions

5. About Positive Technologies

Positive Technologies is at the cutting edge of IT Security. A specialist developer of IT Security products, Positive Technologies has over a decade of experience in detecting and managing vulnerabilities in IT systems. The company has been named one of the top ten worldwide vendors of Vulnerability Assessment systems and is among the top five fastest-growing firms in Security & Vulnerability Management globally*

Positive Technologies has more than 300 employees at its offices and research centres in London, Rome, Moscow, Seoul and Tunis. Its technology partners include IBM, Oracle, Cisco, Microsoft and HP.

Positive Technologies' innovation division, **Positive Research**, is one of the largest security research facilities in Europe. Our experts work alongside industry bodies, regulators and universities to advance knowledge in the field of information security and to apply this analysis to improving the company's products and services. The centre carries out research, design and analytical works, threat and vulnerability analysis and error elimination.

Since 2004, Positive Research has helped global manufacturers including Microsoft, Cisco, Google, Avaya, Citrix, VMware and Trend Micro to eliminate hundreds of vulnerabilities and defects that threatened the safety of their systems.

*Source: Market intelligence firm IDC's report "Worldwide Security and Vulnerability Management Forecast for 2012-2016"

www.ptsecurity.com
pt@ptsecurity.com
+7 (495) 744 01 44