# Practical analysis of the cybersecurity of European smart grids

Gleb Gritsai, Alexander Timorin, Kirill Nesterov, Alexander Tlyapov, Sergey Gordeychik

## Abstract

This paper summarizes the experience gained during a series of practical cybersecurity assessments of various components of Europe's smart electrical grids.

## Keywords

Cybersecurity, SIL, industrial control system (ICS), IEC 61850, Smart Grid, smart grids, vulnerabilities, relay protection

## Introduction

Smart grid technologies are now being widely implemented across Europe. To a large extent this trend reflects a focus on energy efficiency and the mass adoption of mini- and microgeneration renewable electric power sources. The main regulatory guide in this field is Directive 2009/28/EC of the European Parliament and Council of 23 April 2009; this document sets the target of achieving 20% power generation from renewable sources by 2020, and 80% by 2050.

In this article, we summarize the experience gained during a number of practical security assessments of various components of Europe's smart grids.

## Scope of work

In this article, we define industrial control system (ICS) cybersecurity as the process of ensuring operation of a management object with no dangerous failures or inadmissible damage. It also implies the target level of economic efficiency and reliability being maintained under the conditions of a purposeful negative human-induced information impact.

This definition makes it possible to apply a mission-centric approach[1] to a security assessment and to use existing industrial and functional security, reliability theory for risk assessment and threat modeling. The findings of this analysis will be published in our subsequent papers.

The main objects of the research were determined based on NISTIR 7628 Guidelines for Smart Grid Cyber Security[2].

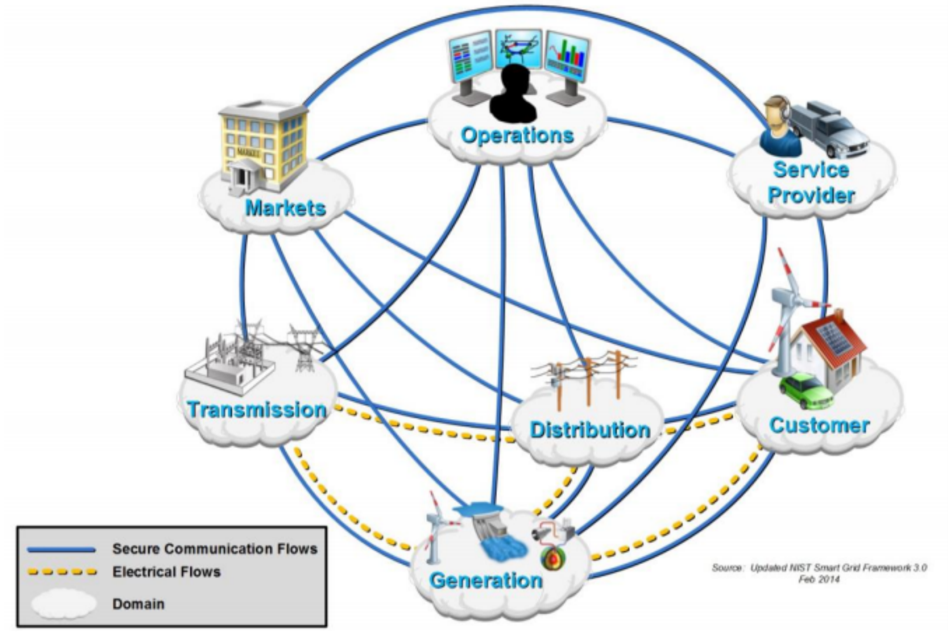


Figure 1. Electricity flows and communication lines in the NIST Smart Grid Framework model

For the purposes of this research, the basic model envisaged an anonymous intruder with average skills and acting over the Internet. This adequately models the capabilities of a motivated group of ‘hacktivists’ or of a medium-budget industrial espionage campaign or criminal operation. In our research we did not look at attack vectors associated with CVSS adjacent networks, including local radio networks. The results of our work showed that at the current time it is impractical to consider more complex intruder models or attack methods, since even an anonymous intruder acting from the Internet has sufficient opportunity to conduct a variety of attacks.

This article presents the findings of several independent projects aimed at assessing the security of different elements (network communications, elements of relay protection and automatic equipment, SCADA, application software, small-scale power generation systems). This research does not claim to be complete.

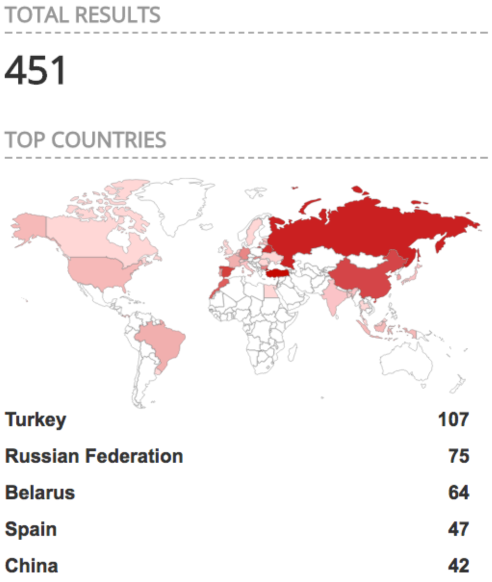
## Security of communication

As can be seen in the NIST Smart Grid Framework model, different data communication lines exist between all the subjects. Therefore, the communication lines and application protocols are a substantial element of the attack surface, and the degree to which they are protected largely determines the security status of the entire system.

Security audits at a number of power facilities in Europe have confirmed CIGRE's conclusions[3] that the IEC 61850 family of protocols currently in use have low tolerance to eavesdropping, session spoofing and man-in-the-middle attacks. However, despite the fact that IEC 61850 has been widely implemented, a practical assessment of security has demonstrated that standard ICS data communication protocols such as Modbus, S7, PROFINET, and IEC 60870-104, are widely used at power facilities.

During our analysis, we prepared a number of tools for the identification, modification and fuzzing of communication protocols; some of these were published as open-source tools[4] and presented at the Power of Community conference in Seoul, South Korea. The practical application of these tools enabled us to identify a number of unknown vulnerabilities in different systems, such as being able to disable a Siemens S7-1200 controller by sending Profinet packets[5].

The findings of this research were used in a number of projects, including CRISALIS[6], Shodan. At the 4SICS conference in Stockholm, Sweden, John Matherly presented his project ICS Map[7], which is based on the Shodan system core, but scans systems using industrial protocols. This project can be used to identify industrial systems connected to the Internet.



TOTAL RESULTS

451

TOP COUNTRIES

| | |
|---|---|
| Turkey | 107 |
| Russian Federation | 75 |
| Belarus | 64 |
| Spain | 47 |
| China | 42 |

Figure 2. A map of Shodan IEC 60870-104 systems on the Internet (June 2017)

However, the attack surface is not limited to ICS protocols. During a presentation at the Chaos Communication Congress 30 conference[8], it was demonstrated that ICS components make widespread use of standard application layer protocols for remote administration and communication of information. In fact, only 2% of all detected ICS systems on the Internet used industrial communication protocols.

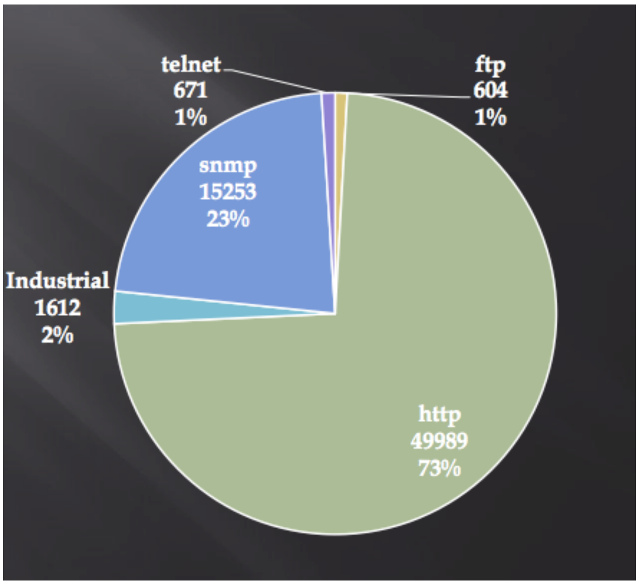


Figure 3. Protocols used by ICS components detected online (December 2013)

Further research has shown that many of the devices detected online are network hardware supporting internal or external communications of ICS systems. For example, it is stated in the 2016 Kaspersky Lab publication 'Industrial Control Systems and their online availability'[9] that around 28% of all ICS components detected on the Internet are network devices such as industrial grade routers, cellular modems, etc.

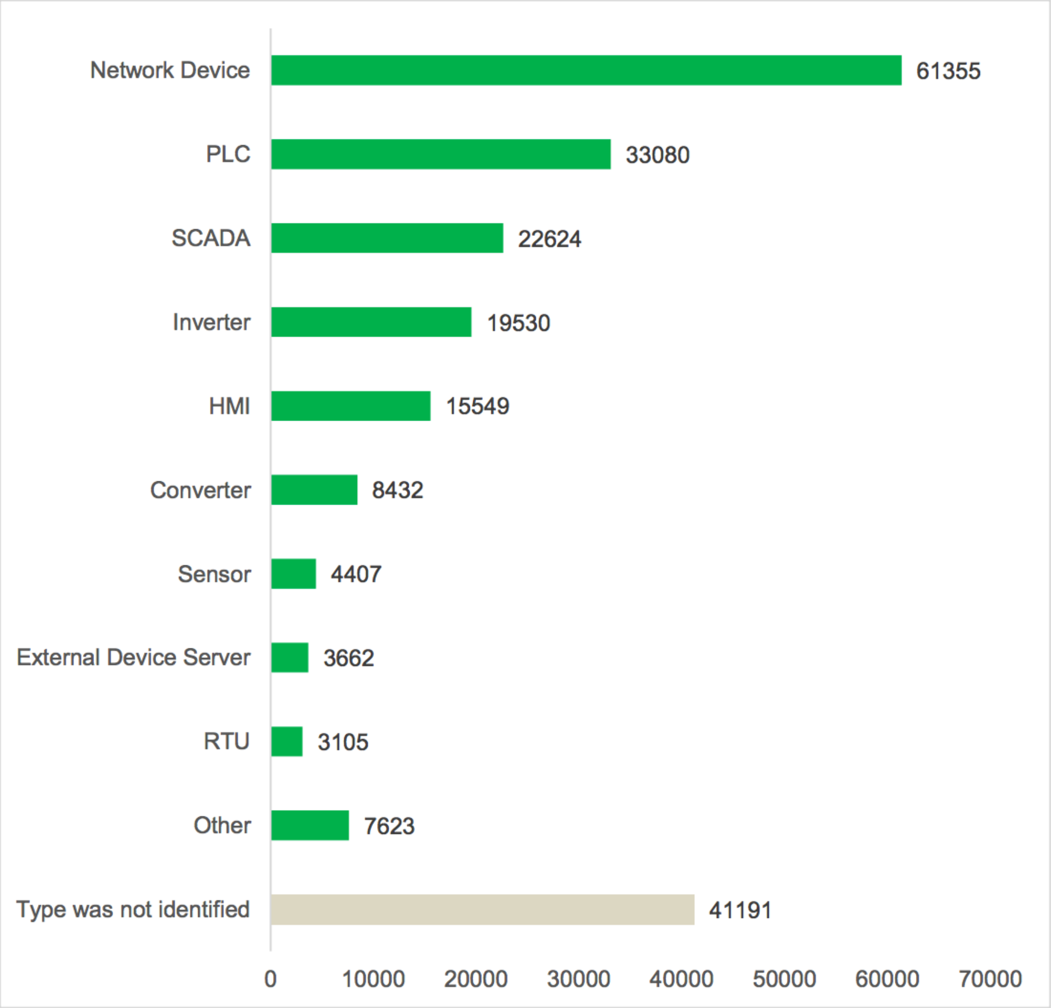


Figure 2. ICS components availability

Figure 4. Types of ICS components reachable from the Internet (2016)

To obtain a better understanding of possible attacks, a security assessment was carried out for network devices used in industrial systems such as Bintec, Digi, Moxa, Sierra Wireless. This analysis showed that such systems typically have low protection levels, and that there is an abundance of vulnerabilities that are easy to detect and exploit, such as hardcoded passwords, hardcoded SSH keys, weak mobile communications (2G/3G/4G), web management interface issues, and buffer overflows. If a potential intruder exploits one of these vulnerabilities, it enables them to modify network device configurations, monitor and redirect traffic, block network communications and/or gain unauthorized access to internal components of industrial systems.

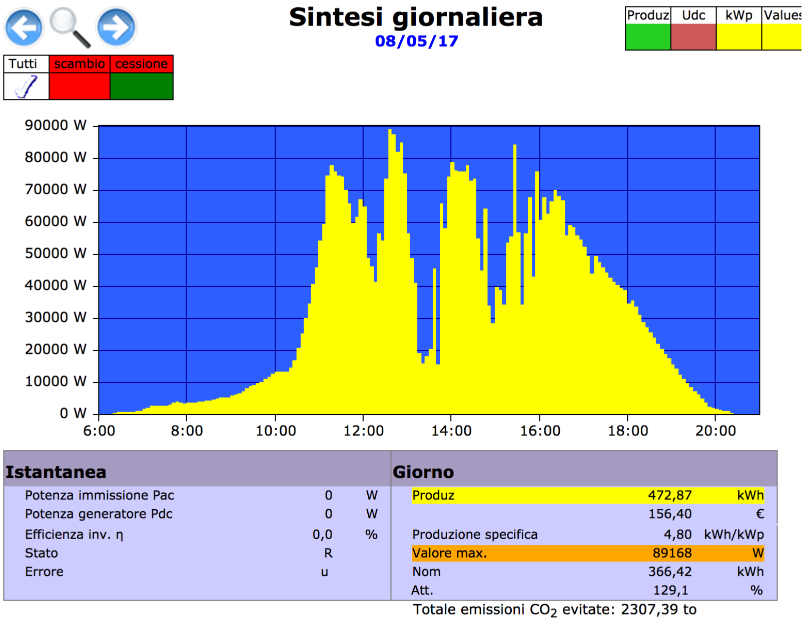
The findings were presented at the conference 32C3 in Germany[10]. The appropriate manufacturers have now fixed most of the detected vulnerabilities.

Special mention should be made of the widespread use of global wireless networks, such as 2G/3G/4G mobile networks in the energy sector. Our research, which was presented at the conference PacSec, Japan [11] , demonstrated how vulnerabilities in core mobile network components (SGSN/GGSN), mobile modems and SIM cards can be used to intercept network communications and introduce unauthorized modifications, modify firmware installed on devices, and gain unauthorized access. Many of these attacks can be implemented from an arbitrary location and do not require a physical location close to the target. In April 2017, security incidents in several German banks were identified where cybercriminals exploited vulnerabilities in signaling networks to intercept text messages [12] . This demonstrates that such methods are available to groups of cybercriminals.

## Microgeneration

For a fuller picture, it is necessary to look at the security risks around small-scale power generation from renewable sources.

During our research project, we analyzed attack surfaces and searched for vulnerabilities in four popular solar and wind-driven power generation platforms: Solar-Log and SMA SunnyWebbox facilities, and in the Nordex NC2 portal which is used as a SCADA system for Nordex wind-driven power plants. The analysis showed that over 80,000 such systems are accessible on the Internet. Many of them do not require authorization before they provide data on the amounts of electric power produced and other technical information, so it is possible to passively estimate the capacity of power generation through an analysis of OSINT sources, such as Google’s cache.



Sintesi giornaliera

08/05/17

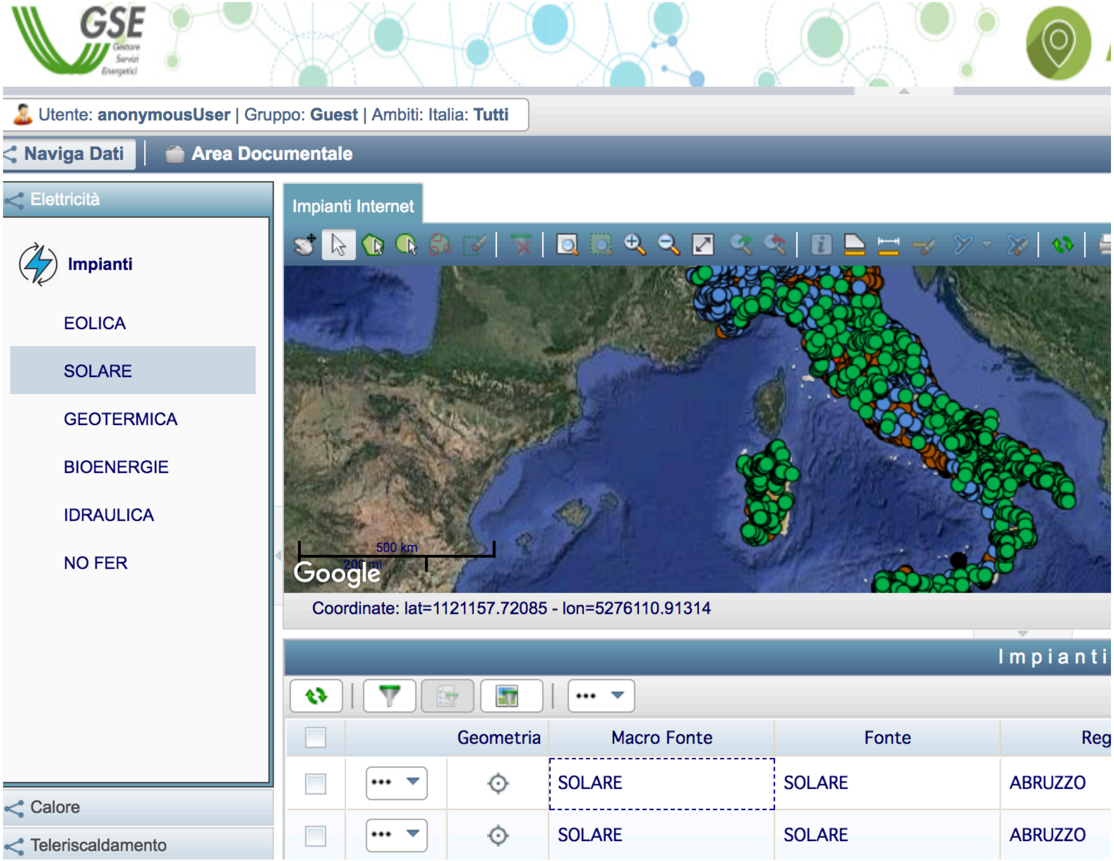
| Istantanea | | | Giorno | | |
|---|---|---|---|---|---|
| Potenza immissione Pac | 0 | W | Produz | 472,87 | kWh |
| Potenza generatore Pdc | 0 | W | | 156,40 | € |
| Efficienza inv. η | 0,0 | % | Produzione specifica | 4,80 | kWh/kWp |
| Stato | R | | Valore max. | 89168 | W |
| Errore | u | | Nom | 366,42 | kWh |
| | | | Att. | 129,1 | % |

Totale emissioni $CO_2$ evitate: 2307,39 to

Figure 5. Information on power generation from Solar Log

By averaging the obtained data, we found that the average instantaneous power output of those systems that can be reached via the Internet is about 8 GW, a large part of which is produced in Europe.

Another peculiarity of small generation facilities is that they make extensive use of cloud-based centralized management systems. With this approach, inverter management systems are connected to the centralized reporting system located at the site of the manufacturer or operator, and they send information there about the status of the systems, electrical power outputs, wind velocities, etc. In some cases, the centralized systems have certain control capabilities, e.g. they can update firmware of the inverter management systems. In that case, an attack on the management system can lead to mass unauthorized access to endpoint devices.



Utente: **anonymousUser** | Gruppo: **Guest** | Ambiti: Italia: **Tutti**

Coordinate: lat=1121157.72085 - lon=5276110.91314

| | | Geometria | Macro Fonte | Fonte | Reg |
|---|---|---|---|---|---|
| □ | ••• | ⊙ | SOLARE | SOLARE | ABRUZZO |
| □ | ••• | ⊙ | SOLARE | SOLARE | ABRUZZO |

Figure 6. The web interface of GSE SpA,
centralized power generation accounting system

A superficial analysis has shown that most of these cloud-based solutions do not meet basic security requirements, so an attacker may be able to find a vulnerability in them that allows unauthorized access to the system[13]. Therefore, management systems, including those that are cloud-based, must be taken into account when planning security upgrade programs.

If we look at how well protected endpoint devices are, we can see that they have a very low level of resistance to external attacks. During our analysis, we detected a number of 0-day vulnerabilities within the firmware of such systems[14], including fixed and master passwords, insufficient authentication/authorization, weak cryptography, various types of buffer overflow. In most cases, the potential risk associated with the detected vulnerabilities enabled a potential threat actor, whether directly or indirectly, to gain full access to the device by executing an arbitrary code or downloading modified software.

When combined with operational errors, such as the widespread use of default passwords, all of the above make these kinds of ‘home’ systems an attractive target for attacks. This is currently the case for home routers and other Internet of things (IoT) devices that may be used to manipulate gauge readings, penetrate information systems of connected municipal electric grids, and carry out a variety of specific attacks to disrupt power system stability.

Examples of such attacks are the sending of false information about power generation or consumption in an attempt to destabilize the power grid, or a new type of ransomware blocking the management systems of solar or wind-driven power generation. The current trend towards integration between microgeneration management systems and smart power meters only serves to provide cybercriminals with more opportunities.

The findings were reported to the appropriate authorities and agencies, such as IMPACT, ENISA, ICS CERT, hardware manufacturers and to regional CERT teams, so they could inform device owners and block remote access to ICS systems from the Internet. Thanks to this project, more than 60,000 ICS components associated with microgeneration were disconnected from the Internet[15].

## Digital substations

ICS systems used in industrial-scale power generation and distribution were also found to have low security levels. Here, the typical defects are the extensive use of obsolete or unsupported operating systems, weak protection tools, multiple vulnerabilities in SCADA and PLC, and unprotected network protocols. This, combined with low levels of network isolation and widespread use of under-protected radio communication channels, is the reason why a targeted or spontaneous cyberattack could easily be implemented.

Recent security incidents involving Ukraine’s energy systems[16] and the WannaCry case have demonstrated that standard attack methods, such as spear phishing or exploits for known vulnerabilities, are sufficient to penetrate internal ICS networks.

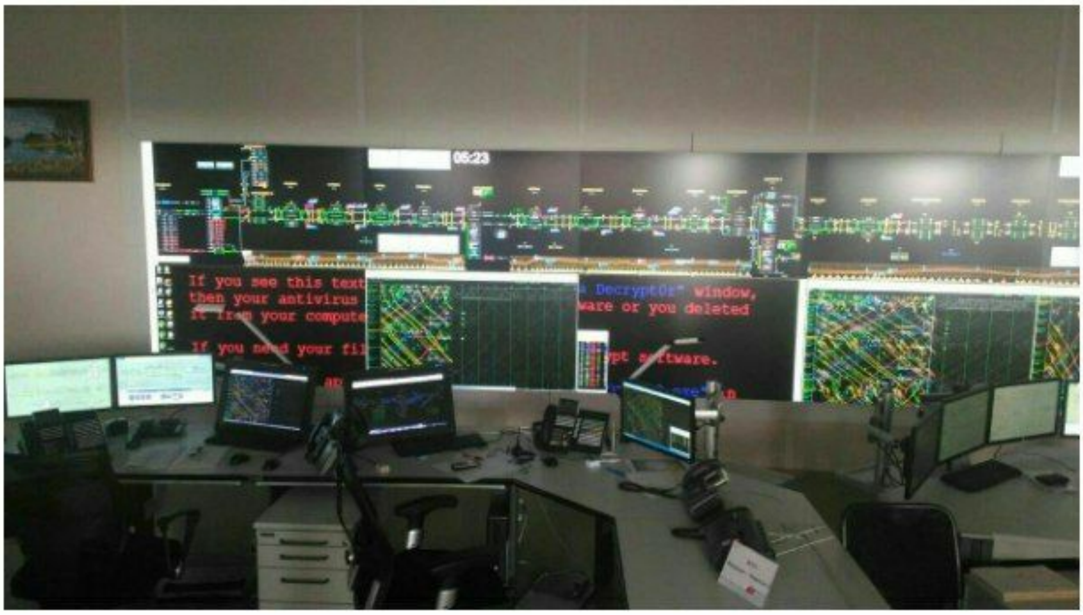


Figure 1. A centralized traffic control system blocked by the WannaCry worm

Digital protective relays are a key component of digital substations. They are designed to promptly identify damaged components in electrical power systems in emergencies and isolate them from the system to ensure normal operation. In other words, they are an element of accident prevention.

During our security assessment projects at power generation and distribution facilities, we analyzed digital protective relays of leading manufacturers, such as NARI Relays, Siemens, ABB, and General Electric. Different types of vulnerabilities were identified, including hardcoded management passwords, unpatched 61850 Stack, remote reboots, permanent DoS, and remote code execution.

By exploiting combinations of vulnerabilities, attackers can manipulate operating parameters for systems or facilities, remotely control circuit breakers, disconnect and grounding switches, disrupt the proper operation of terminals, and even use them as intermediate platforms for malware distribution.

The research findings were presented at the conferences Area 41 in Zurich [17] and RECON BRUSSELS [18] . Information about the detected vulnerabilities was reported to the appropriate manufacturers as part of a responsible disclosure policy. Some of the vulnerabilities have now been fixed by the vendors.

## Conclusions

The experience gained from cybersecurity analysis of Smart Grid technologies has demonstrated that electric grid systems are highly vulnerable to accidental or deliberate information impact.

Despite the obvious economic benefits, implementation of Smart Grid creates the following potential cybersecurity problems:

- widespread use of standard network technologies (TCP/IP, 3G/4G, WiFi), system and application technologies (OS, database management systems), and all their associated security problems;
- blurring the boundaries of power system protection and the system control role, with the transfer of a number of emergency prevention functions;
- blurring of the network perimeter and increased attack surfaces as a result of large numbers and various types of network devices with different owners, but that are connected in a single network;
- minimal attention to cybersecurity issues by the designers and integrators of ICS components, leading to the emergence of large numbers vulnerabilities that are cheap to exploit.

Consequently, modern Smart Grid implementations contain large numbers of system-wide and specific vulnerabilities both in individual components and in overall ICS systems and networks. Identifying and using these vulnerabilities requires an average level of expertise and a modest level of funds. The implications of such attacks vary from local fraud to negative physical impact on power substation components to large-scale network accidents.

[1] Signalling cyber security: the need for a mission-centric approach
Valentin Gapanovich, Efim Rozenberg and Sergey Gordeychik
http://www.railjournal.com/index.php/signalling/signalling-cyber-security-the-need-for-a-mission-centric-approach.html

[2] NISTIR 7628 Guidelines for Smart Grid Cyber Security Victoria Y. Pillitteri, Tanya L. Brewer, https://www.nist.gov/publications/guidelines-smart-grid-cybersecurity

[3] The Impact of Implementing Cyber Security Requirements using IEC 61850 CIGRE Working Group the B5.38, August 2010

[4] Alexander Timorin, Power of Community 2013 special release of ICS/SCADA toolkit, http://scadastrangelove.blogspot.com/2013/11/power-of-community-2013-special-release.html

[5] SSA-654382: Vulnerabilities in SIMATIC S7-1200 CPU, https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-654382.pdf

[6] Marco Caselli, Frank Kargl, Dina Hadziosmanovic, “Device fingerprinting preliminary results”, http://www.crisalis-project.eu/sites/crisalis-project.eu/files/crisalis_deliverable-D4.1.pdf

[7] Shodan, Industrial Control Systems https://www.shodan.io/explore/category/industrial-control-systems

[8] Sergey Gordeychik, Gleb Gritsai, “30C3 releases: all in one”, http://scadastrangelove.blogspot.com/2014/01/30c3-releases-all-in-one.html

[9] INDUSTRIAL CONTROL SYSTEMS AND THEIR ONLINE AVAILABILITY, Oxana Andreeva, Sergey Gordeychik, Gleb Gritsai, Olga Kochetova, Evgeniya Potseluevskaya, Sergey I. Sidorov, Alexander A. Timorin https://kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICS_Availability_Statistics.pdf

[10] The Great Train Cyber Robbery, Sergey Gordeychik, Alexander Timorin https://scadastrangelove.blogspot.com/2015/12/32c3-slides.html

[11] "Root via SMS: 4G access level security assessment”, Sergey Gordeychik, Alexander Zaytsev, https://pacsec.jp/psj14/PSJ2014_Sergei-Alex_SCADASL%20-%20root%20via%20sms%20last.pdf

[12] Fixing the cell network flaw that lets hackers drain bank accounts, Lily Hay Newman, https://www.wired.com/2017/05/fix-ss7-two-factor-authentication-bank-accounts/

[13] SQL Injection in Solar-Log WEB, https://vulners.com/ptsecurity/PT-2015-01

[14] Sergey Gordeychik, Aleksandr Timorin: SCADA StrangeLove: Too Smart Grid in da Cloud http://scadastrangelove.blogspot.com/2014/12/31c3-too-smart-grid-in-da-cloud.html

[15] Could hackers turn the lights out? Mark Ward, http://www.bbc.com/news/technology-35204921

[16] Analysis of the Cyber Attack on the Ukrainian Power Grid, http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[17] CYBER-PHYSICAL ATTACKS ON CRITICAL INFRASTRUCTURE
Sergey Gordeychik, Alexander Timorin
http://www.securitytube.net/video/16617

[18] Hopeless Relay Protection for Substation Automation
Kirill Nesterov, Alexander Tlyapov
https://recon.cx/2017/brussels/talks/hopeless_relay_protection.html