



Your trusted security partner

www.safetech.ro



CORE COMPETENCIES





Securitatea informatica a infrastructurilor Critice

Background Illustration: A collage featuring solar panels, wind turbines, a data center, and a dam, overlaid with a green digital rain effect and binary code.

SYSTEM FAILURE

Mihai RAUTA

Senior Information Security Consultant

Critical Infrastructure at Risks

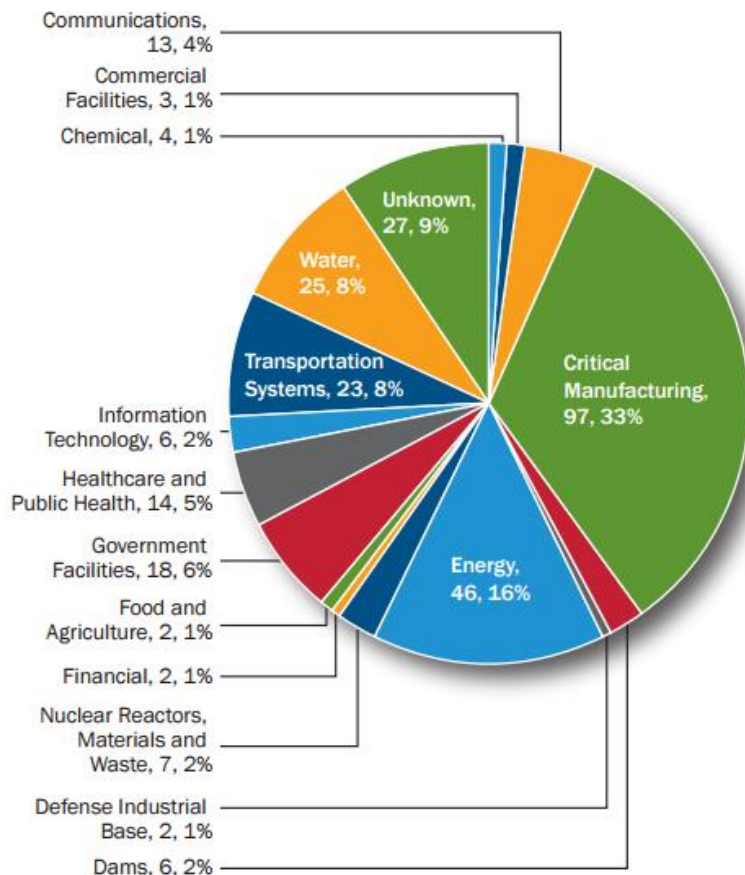
Critical and industrial systems
makes our modern world

Like other IT systems, they
are prone to attacks

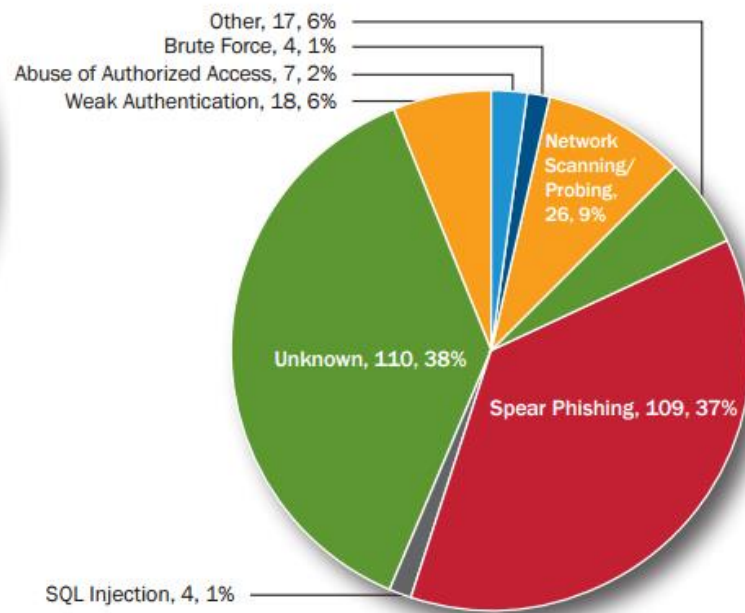
The consequences of such attacks
are much greater:

- **Power failures**
- **Water pollution or floods**
- **Disruption of transportation systems**
- **Malfunction of Production Lines**

ICS-CERT Reported Targeted Attacks in 2015



FY 2015 Incidents by Sector, 295 total.

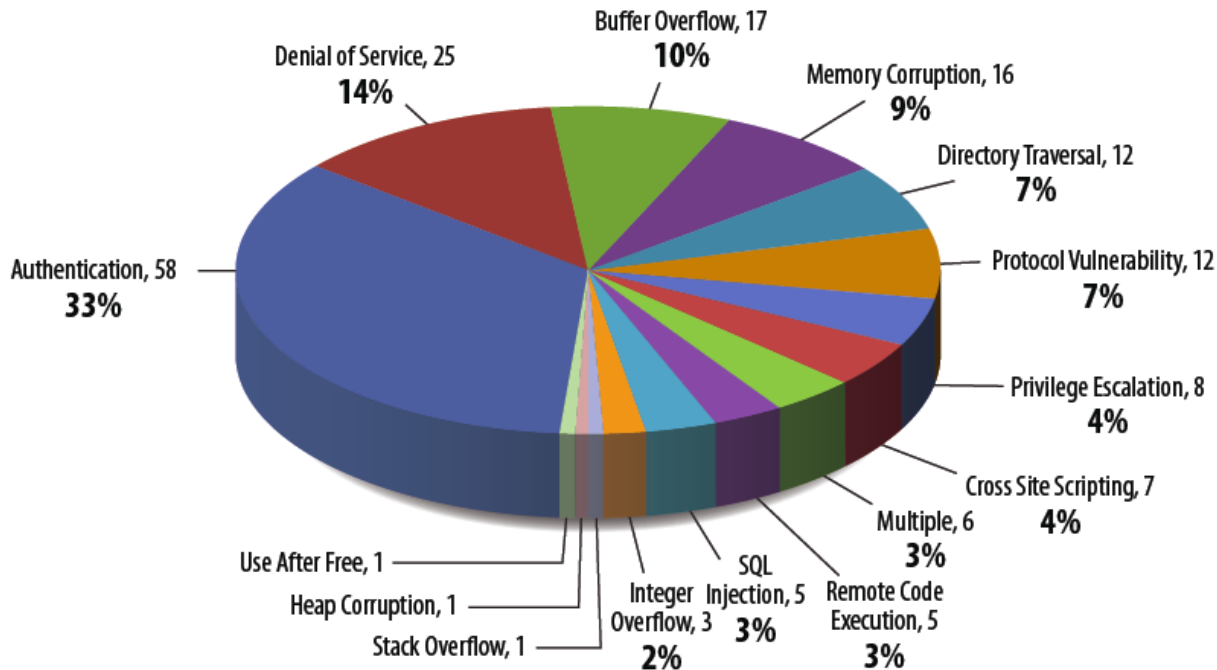


FY 2015 Incidents by Attempted Infection Vector, 295 total.

In 2015, ICS-CERT responded to **295 incidents** reported either directly from asset owners or through other trusted partners.

ICS-CERT assesses that **many incidents are not detected due to a lack of sufficient detection or logging capabilities.**

ICS-CERT Reported Vulnerabilities



Authentication flaws, includes vulnerabilities like **factory hard-coded credentials**, **weak authentication keys**, etc. These tend to be of highest concern because an **attacker with minimal skill level could potentially gain administrator level access** to devices that are accessible remotely over the Internet.

Important Attacks

Stuxnet, Duqu, Flame

Pacific Energy,
Saudi Arabia Aramco

German Power Utility, 50Hertz

Queensland, Harrisburg and Willows
Water System attacks



Computers and manuals sized in Al Qaeda training camps full of SCADA information related to dams and related structures

2015 December 23, Prykarpattya Oblenergo, Ukraine



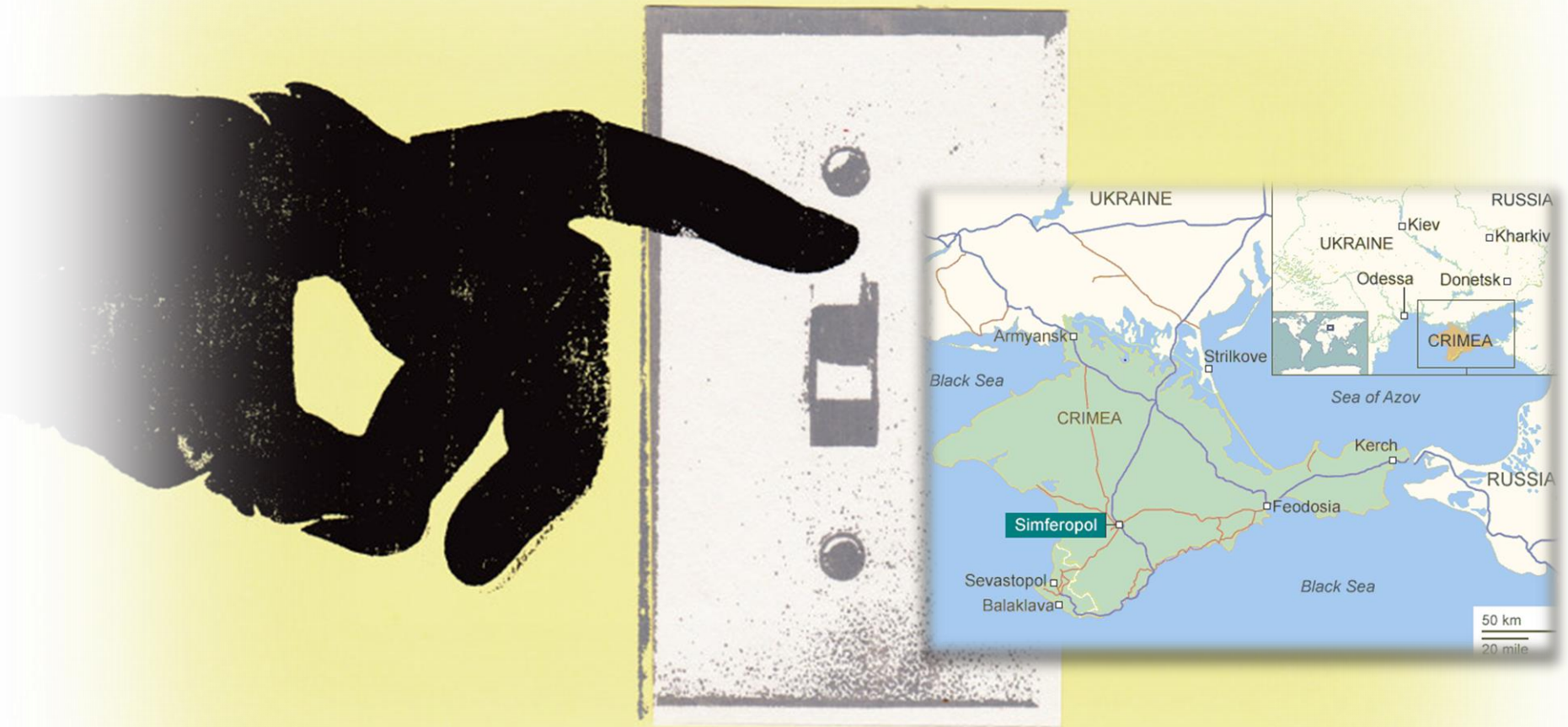
The first confirmed hack to take down a power grid

3 power distribution centers attacked

60 substations, 110kV and 35kV, were taken offline

80,000 customers blackened out for about six hours, more than 230000 people affected

Since mid-2015, the BlackEnergy APT group has been actively using spear-phishing emails carrying malicious Excel or Word documents with macros to infect computers in a targeted network.



The BlackEnergy APT group captured Cyber Security community attention back in 2014 when it began deploying SCADA-related plugins against victims in the ICS and energy sectors around the world. The group is especially active in the following sectors:

- ICS, Energy, government and media in Ukraine
- ICS/SCADA companies worldwide
- Energy companies worldwide

Why attacks can happen ?

1

SCADA devices were not designed for security and are vulnerable

2

SCADA devices and networks are more reachable than it seems

Controllers are vulnerable

- Programmable Logic Controllers (PLC) are purpose-built computers used for automation of electromechanical processes such as control of pumps, valves, pistons, motors, etc.
- PLCs are small computers. They have software applications, accounts and logins, communication protocols, etc.
- Analysis of PLCs from leading vendors shows variety of vulnerabilities:
 - Backdoors
 - Lack of authentication and encryption
 - Weak password storage
 - Bugs leading to buffer overruns



PLCs are Insecure By Design

If you have logical access to a PLC you can Read, Write and otherwise Access the tags/points. Write commands change the process, i.e. open or close valves, raise temperatures, turn things on or off. It is how operators control the process. These are ICS protocols that are insecure by design.

The SCADA and ICS are insecure by design and in most cases don't require an exploit to affect the process in disastrous ways.

	AB	Schneider Electric	GE	SEL
Firmware	!	×	!	!
Ladder Logic	!	!	×	!
Backdoors	!	×	×	✓
Fuzzing	×	×	×	!
Web	!	×		
Best Config	!	!		
Exhaustion	✓	✓		
Undoc Features	!	×		

SCADA+ Pack

This is an attempt to collect ALL publicly available SCADA vulnerabilities in one exploit Pack.

SCADA and related vulnerabilities are very special due to their sensitive nature and possible huge impact involved to successful exploitation.

SCADA Systems are also "hard to patch", so even old vulnerabilities are actual.

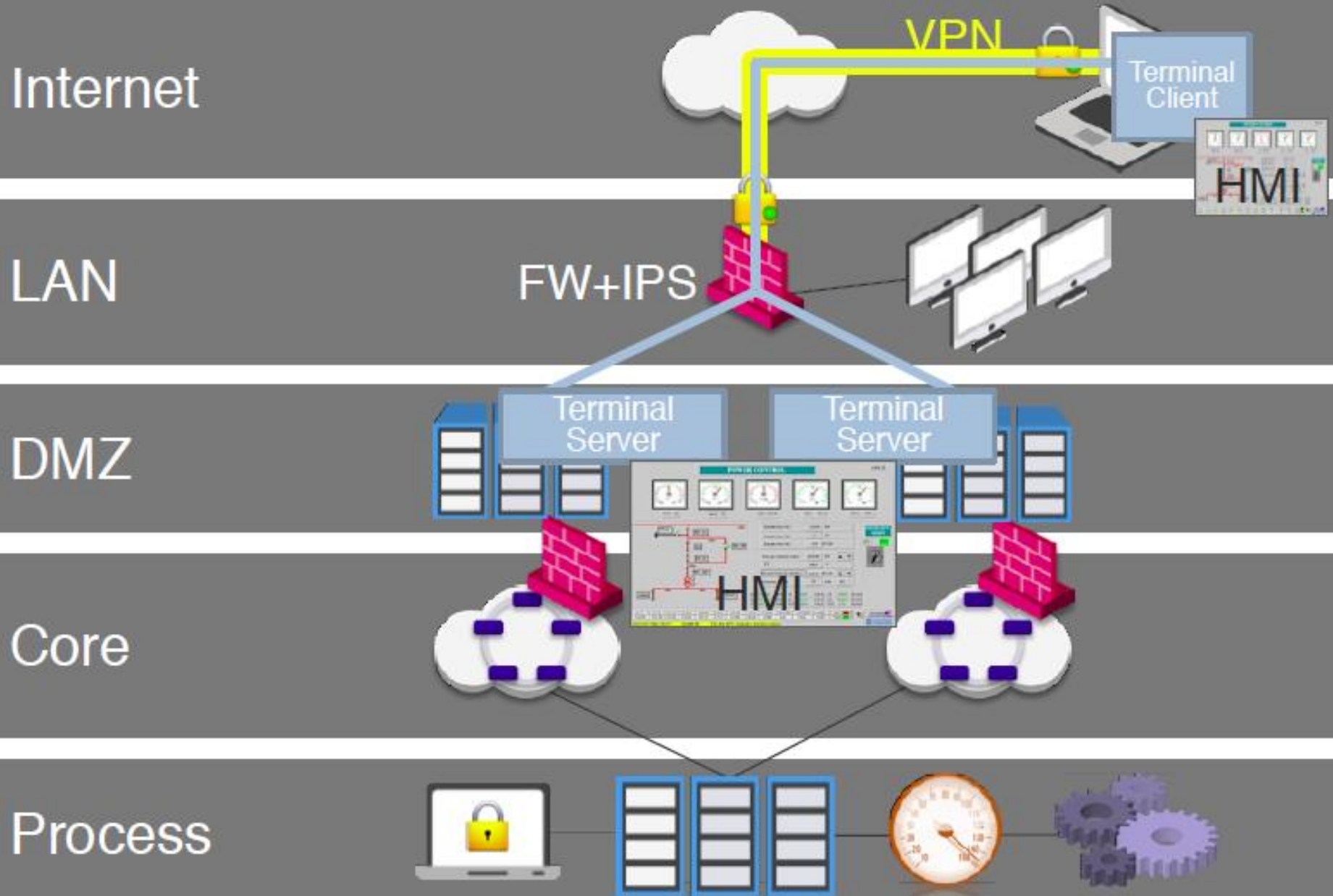
The SCADA+ Pack features:

- Growing value
- Due to low real systems patch rank
- We try to cover most of the public SCADA vulns.

GLEG



IT and SCADA networks are interconnected



ROMANIA – SCADA Devices Connected to Internet*

Total Results: 3,147

Top Services	
2222	2,584
DNP3	330
Modbus	139
Automated Tank Gauge	41
Siemens S7	39

Top Organizations	
Vodafone Romania S.A.	451
RCS & RDS Business	410
RCS & RDS Residential	222
IPv4 Management SRL	65
UPC Romania SRL	41

2222/tcp port is specific to Rockwell Automation ControlLogix PLC and allow Man In The Middle, Controller Fault and DDoS attacks

DNP3 and Modbus permit access to the inputs and outputs on a Programmable Logic Controller

Automatic Tank Gauges uses a TCP/IP to Serial converters and may have many vulnerabilities

Insufficient Entropy and Improper Resource Shutdown vulnerabilities in Siemens PLCs could be exploited remotely

Attack, How-To?

- **Step 1:** get access to the network

- Social Engineering
- Spear phishing
- Drive-by
- USB Keys
- Contractor Laptops
- Maintenance Remote Access Links

- **Step 2:** use a tool-kit or run specially crafted attack

- **Step 3:** alter commands sent to the controllers, or change sensors readings



SECURITY
dark READING
Protect The Business  Enable Access

**SCADA Password-Cracking Tool For
Siemens S7 PLCs Released**

Protect, How-To?

1. Specialization Required for Core and Process Networks

2. Defense in Depth for LAN and DMZ Networks



Safetech approach to protect ICS and SCADA networks

Independently Log ALL SCADA activity

Define Baseline
(Allowed / Not Allowed / Suspicious)

Identify Deviations

Alert / Prevent

Specialization for Core and Process Networks with Xsense from CyberX

- Learns and captures the “DNA signature”(*) of the network
 - No prior knowledge or configuration
- Securing every industrial network within a day
- High detection rates and low false-positive rate
- No risk to on going operations
- Physical appliance/ Virtual machine



Defense in depth for DNZ and LAN networks

- Firewall
- IPS/IDS
- Anti-Bot
- Gateway Anti-Virus
- DLP
- Zero-Day and Sandboxing solution
- SIEM
- Machine learning solutions for detecting pattern of life and deviations from normality



WE ARE COMMITTED TO PROVIDING YOU WITH
THE BEST ANSWER FOR ALL OF YOUR SECURITY NEEDS.

DISCOVER
WHAT WE
CAN DO
FOR YOU

THANK YOU!

mihai.rauta@safetech.ro; www.safetech.ro

