Your trusted security partner

www.safetech.ro

safetech
Your trusted security partner

SAFETECH OVERVIEW

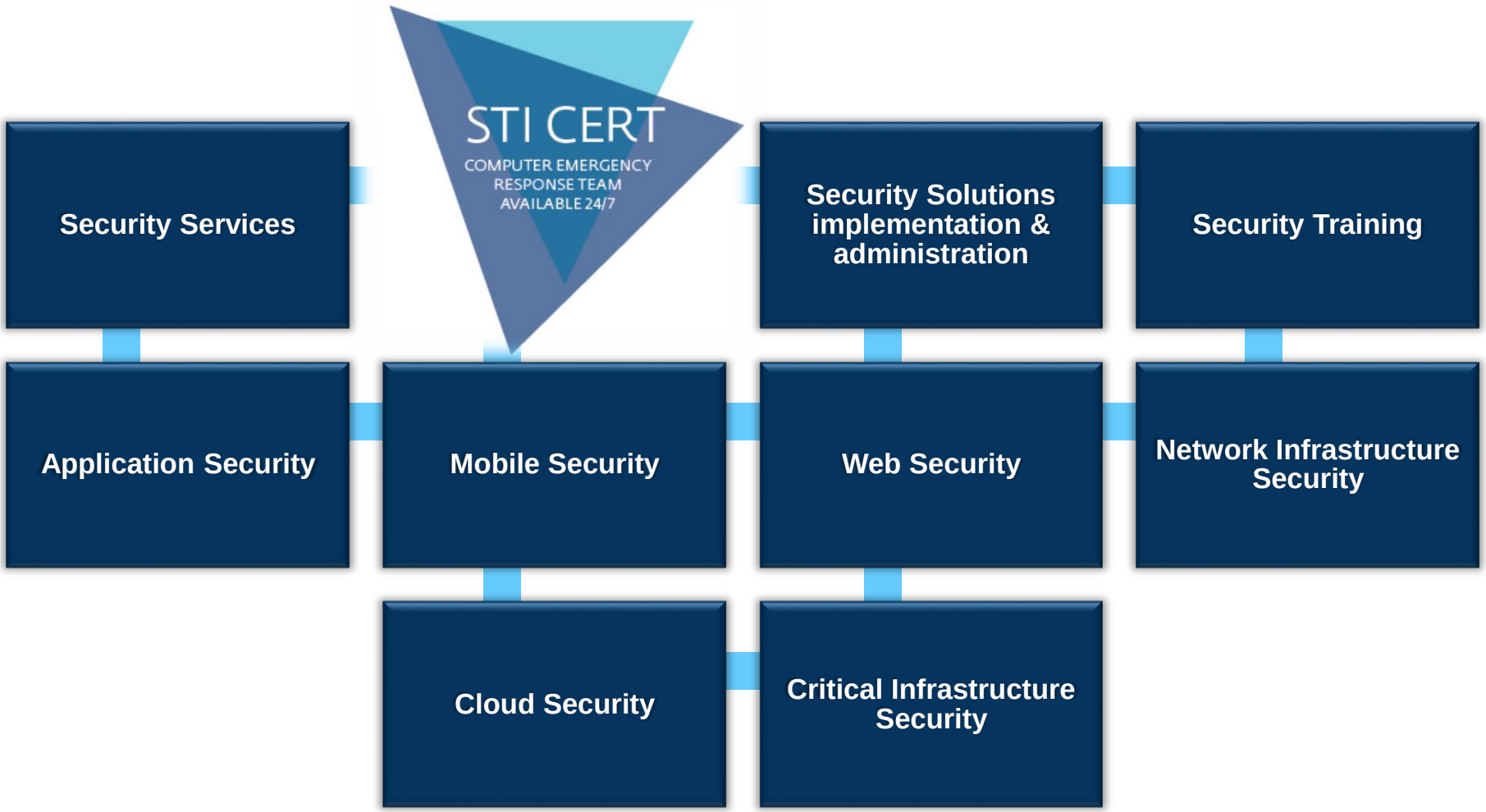
- Founded in 2011 by a team of information security experts;
- The market leader in Romania;
- Headquarters in Bucharest;
- 25 employees (only full-time employees);
- + 100 customers
- + 200 security projects managed
- + 20 partners (top security solutions providers)
- Operating the sole private incident response center operational in Romania

  - Markets: Romania, USA, Luxembourg, Netherlands, Moldova, Albania.
  - Business verticals: Government, Regional and Local Administration, Energy, Defense, Banking & Insurance, Health & Medical.

safetech
Your trusted security partner

SAFETECH

CORE COMPETENCIES



safetech
Your trusted security partner

A TEAM OF TOP SECURITY EXPERTS

To maintain our partnership solid, we continuously invest in improving the quality of our staff, looking for the most innovative security solutions and short intervention time. Our technical engineers holds certification as:

- **LPT** — Licensed Penetration Tester (EC — COUNCIL)
- **OSCP** — Offensive Security Certified Professional (Offensive Security)
- **CSSLP** — Certified Secure Software Lifecycle Professional (ISC2)
- **CEH** — Certified Ethical Hacker (EC — COUNCIL)
- **CRISC** — Certified in Risk and Information Systems Control
- **ECSA** — EC Council Certified Security Analyst
- **CISA** — Certified Information Systems Auditor (ISACA)
- **CISSP** — Certified Information Systems Security Professional (ISC2)
- **CISM** — Certified Information Security Manager
- **HID** — HID Certified Professional
- **CIPP / IT** — Certified Information Privacy Professional / Information Technology
- **CPSSE** — Certified Professional for Secure Software Engineering
- **CCSA** — CheckPoint Certified Security Administrator
- **CCSE** — CheckPoint Certified Security Expert
- **CCSI** — CheckPoint Certified Security Instructor
- **CPSC** — CheckPoint Partner Sales Certification
- **CCSP** - CheckPoint Certified Collaborative Support Provider

safetech
Your trusted security partner

EXPERIENCE IN COMPLEX SECURITY PROJECTS

Our experience comes from important and relevant projects closed across last three years in Government – Public Sector, which represent our company core business, Banking & Insurance, Energy and Public Utilities

Public Administration	Enterprise companies	Enterprise companies	Financial Sector	IT Integrators	IT companies
MINISTERUL EDUCAȚIEI CERCETĂRII TINERETULUI ȘI SPORTULUI	ROMTELECOM	electrica S.A.	Raiffeisen BANK	TEAMNET	BIT software
INSTITUTUL NATIONAL DE CERCETARE - DEZVOLTARE ÎN INFORMATICĂ	Frontal COMMUNICATION	IRCAT	ING BANK	SIVECO ROMANIA SA	OMNILOGIC
ANAF	bwin	Kandia Dulce	VOLKSBANK ROMÂNIA	UTI GROUP	METOPIA
CNADNR	ArcelorMittal	ANCOM	Credit EuropeBank	kapsch	INTRASOFT INTERNATIONAL
		emon	otpbank	novensys	iSDC
		TAROM	Cetelem	S&T Consulting. Integration. Outsourcing.	Security Innovation THE APPLICATION SECURITY COMPANY
					YMENS

safetech
Your trusted security partner

OUR PARTNERS

ACTIVIDENTITY part of HID Global
Bitdefender
BalaBit IT Security
Check Point SOFTWARE TECHNOLOGIES LTD.
CyberX Securing the Industrial Internet
cisco
CHECKMARX Application Security Made Easy
DARKTRACE
HID
illusive
IMPERVA
InfoBay A Secure Path to Share Your Data
JUNIPER NETWORKS
mailarchiva
McAfee
MobileIron
paloalto NETWORKS
proofpoint
SECURITY INNOVATION
SpectorSoft Authorised Partner
TREND MICRO
ZABBIX

OUR CLIENTS ADDRESS TODAY'S CHALLENGES WITH TOMORROW'S SOLUTIONS PROVIDED BY OUR PARTNERS, WHO ENJOY WIDE INTERNATIONAL EXPERTS RECOGNITION.

Cyber Security and SCADA Systems

Mihai RAUTA

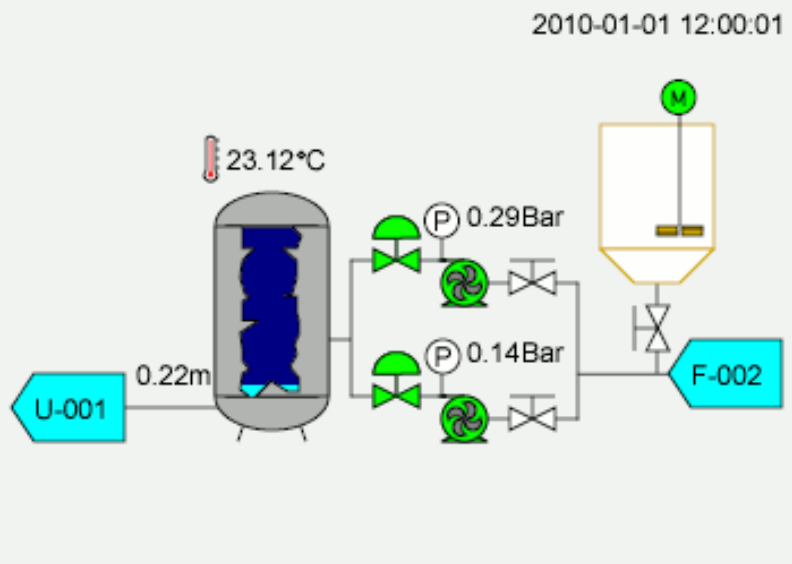
Senior Information Security Consultant

Critical Infrastructure …

Supervisory Control and Data Acquisition system (SCADA) is an automation control system designed to gather data in real time from remote locations in order to control equipment and conditions

SCADA has two elements:

- The process, system and machinery you want to control and monitor
- A network of intelligent interconnected devices that interface with the first system through sensors and control outputs



safetech
Your trusted security partner

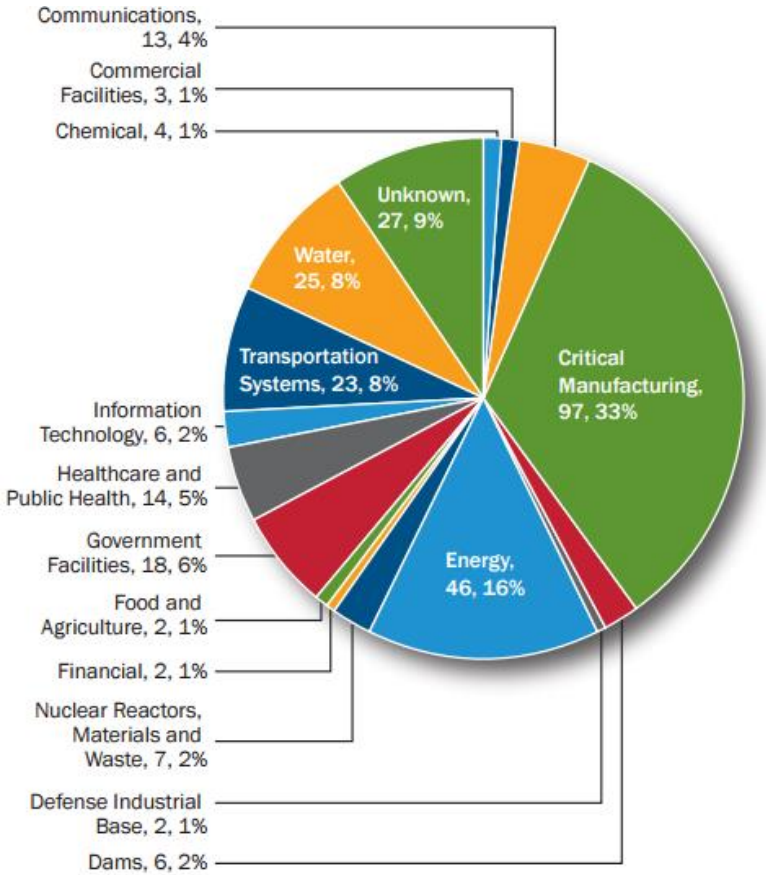
… at Risks

Like other IT systems, SCADA systems are prone to attacks, but the consequences are much greater:

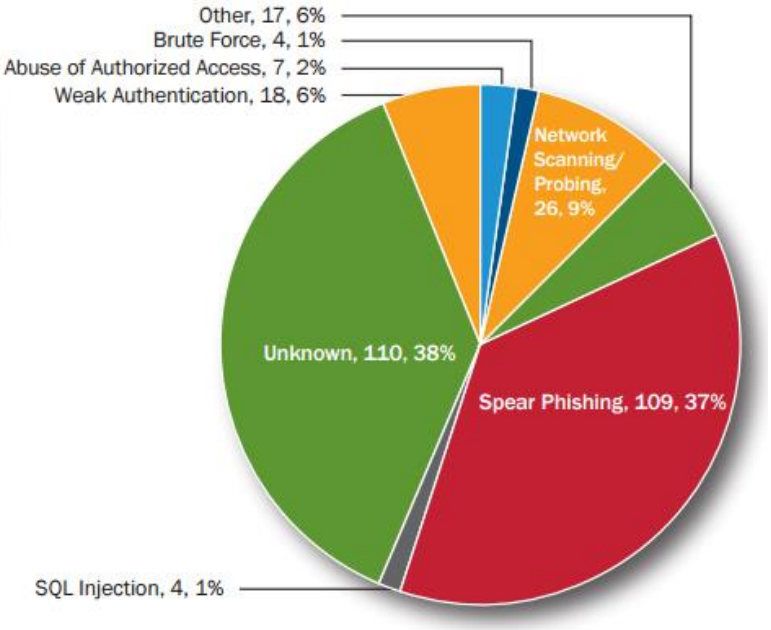
- Power failures
- Water pollution and floods
- Disruption of transportation systems
- Catastrophic disasters of Production Lines

safetech
Your trusted security partner

ICS-CERT Reported Targeted Attacks



FY 2015 Incidents by Sector, 295 total.



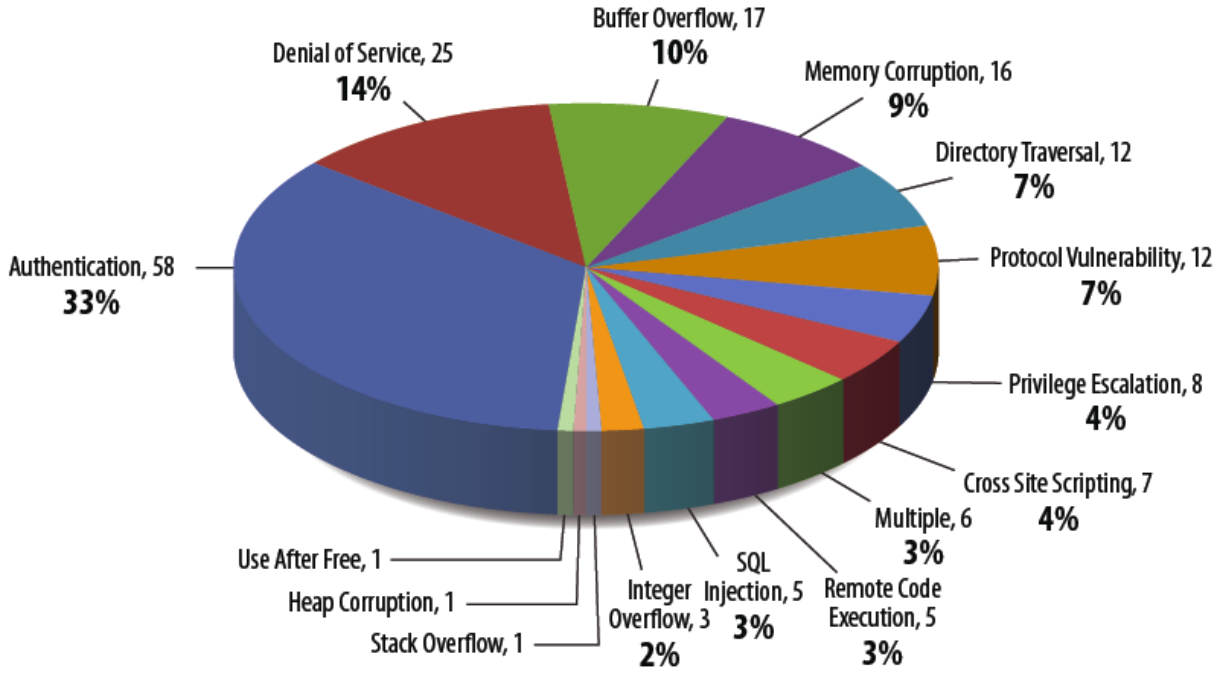
FY 2015 Incidents by Attempted Infection Vector, 295 total.

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

safetech
Your trusted security partner



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.

Key SCADA attack methods

safetech
Your trusted security partner

- **Distributed denial of service (DDoS)** may remotely shut down the power at key sites, interrupting secured physical communication links by signal jamming surveillance cameras or even flight-control signals

- **Buffer overflows** which occurs when a program or process tries to store more data in temporary storage than it can hold, is widely used attack method

- **SQL injection** remains one of the most potent attack vectors across multiple applications because there are so many entry points

- **Spear phishing,** an attacker simply does his social media homework on an system administrator of a large industrial company and baits the person to open an attachment, for example by sending an tempting email

Latest spear phishing campaigns are based on using recurrent neural networks (machine learning) that learn from social networks postings about targeted person

Important Attacks

safetech
Your trusted security partner

- 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

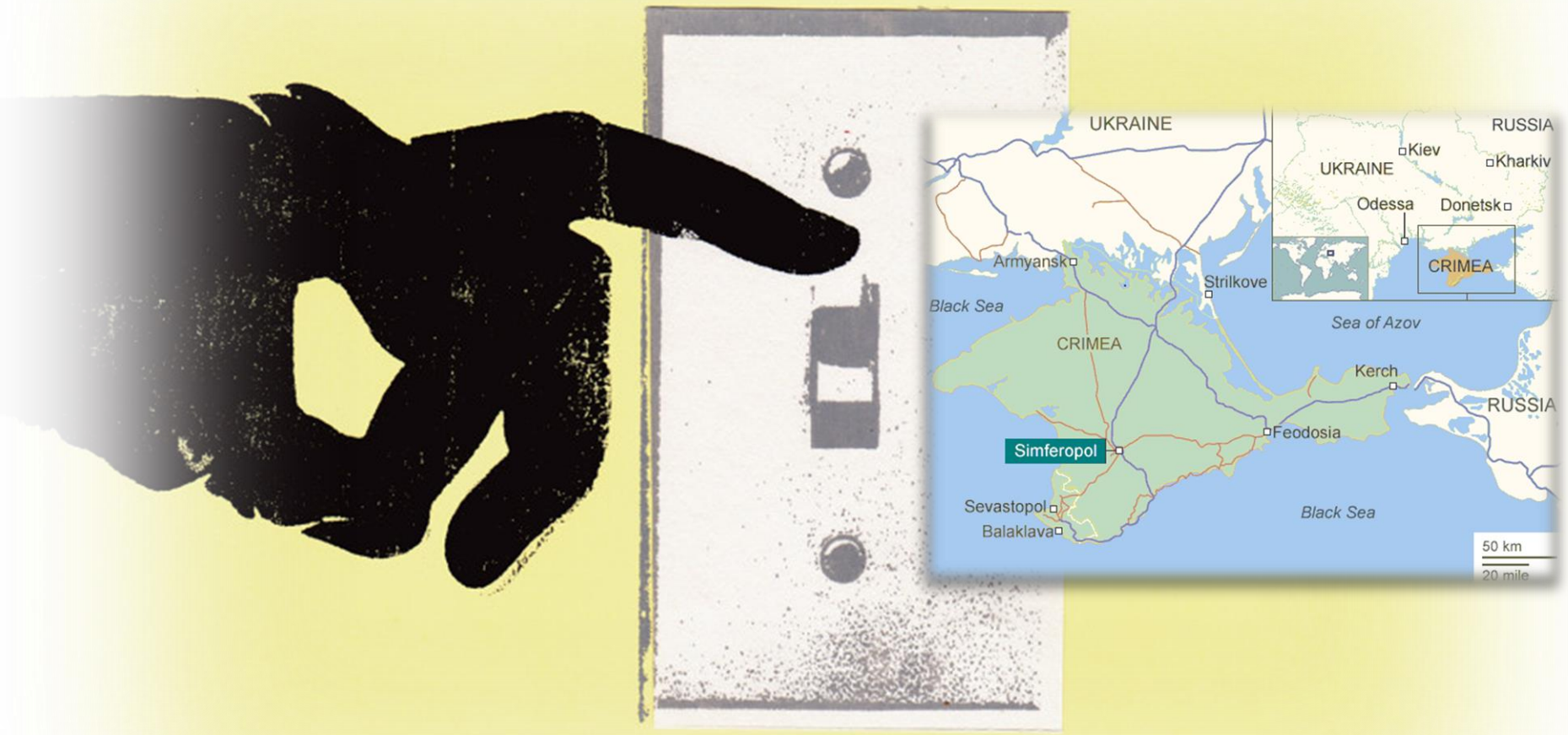
The first confirmed hack to take down a power grid

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

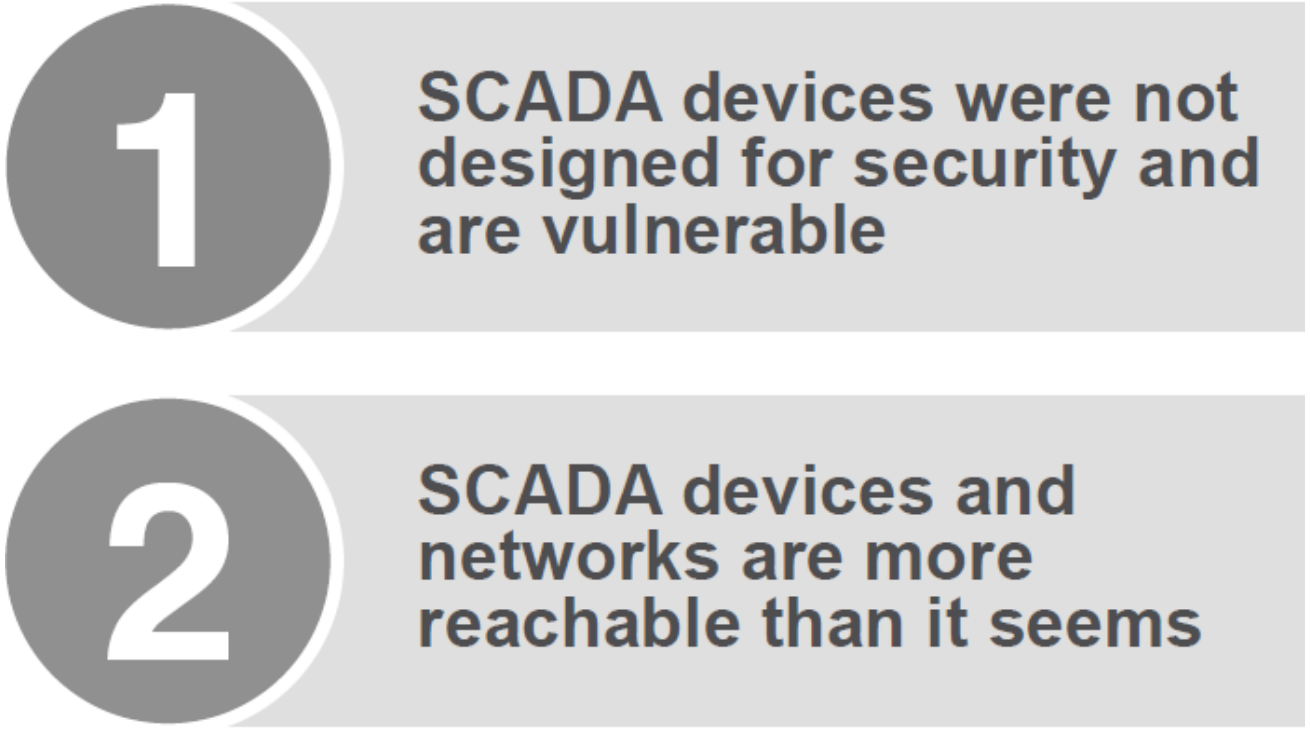
Since mid-2015, the BlackEnergy APT group has been actively using spear-phishing emails carrying malicious Excel or Word documents with macros to infect computers in a targeted network.



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.

Why attacks can happen ?

safetech
Your trusted security partner



The ERIPP and SHODAN search engines can be leveraged to search for Internet-facing ICS devices and have made it easier than ever for attackers to identify potential targets. ICS-CERT has issued an advisory warning the ICS community of these tools.

Controllers are vulnerable

safetech
Your trusted security partner

- Programmable Logic Controllers (PLC) are purpose-built computers used for automation of electromechanical processes such as control of pumps, valves, pistons, motors, etc.

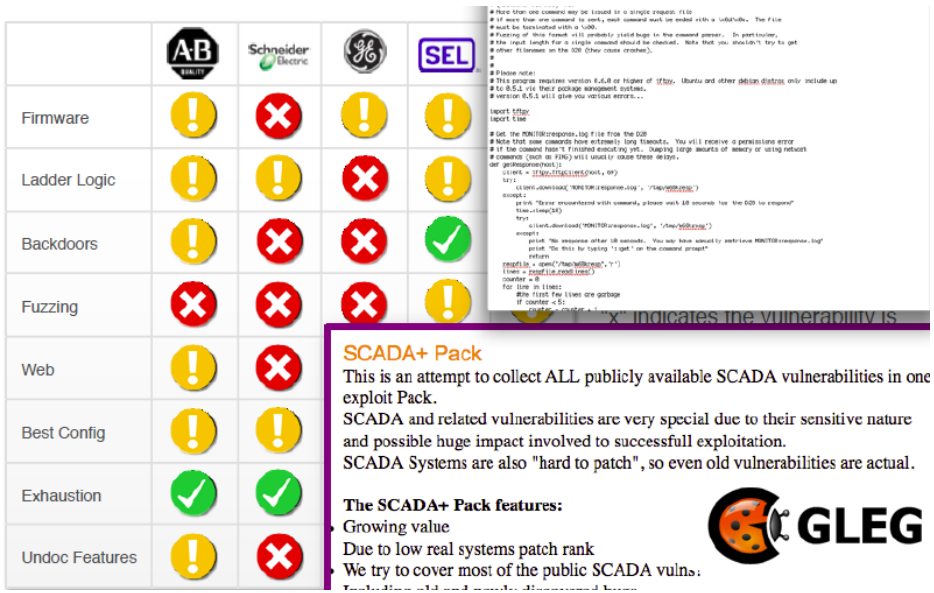
- PLCs are small computers. They have software applications, accounts and logins, communication protocols, etc.

- Analysis of PLCs from leading vendors shows variety of vulnerabilities:
  - Backdoors
  - Lack of authentication and encryption
  - Weak password storage
  - Bugs leading to buffer overruns

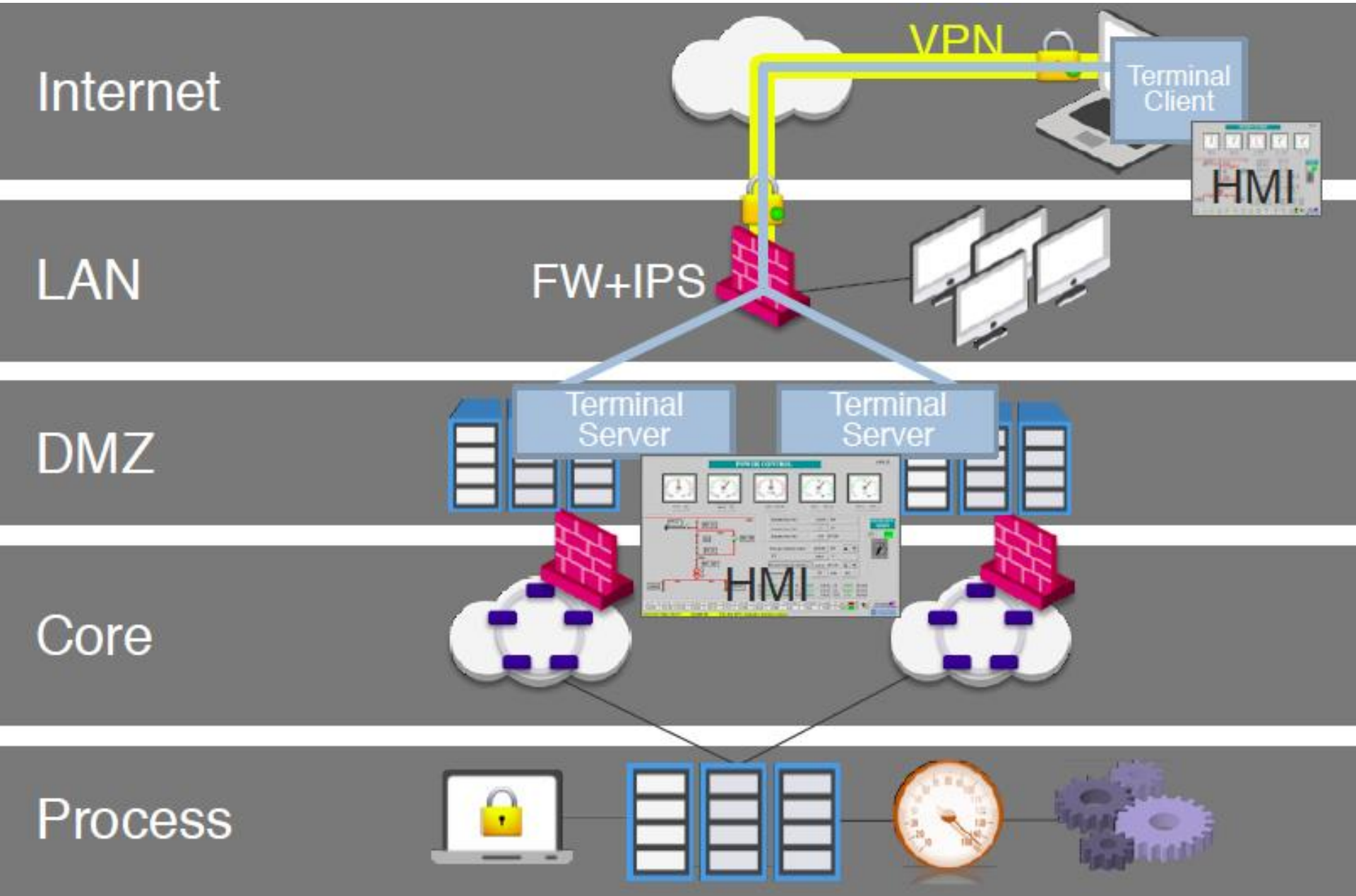
PLCs are Insecure By Design

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.

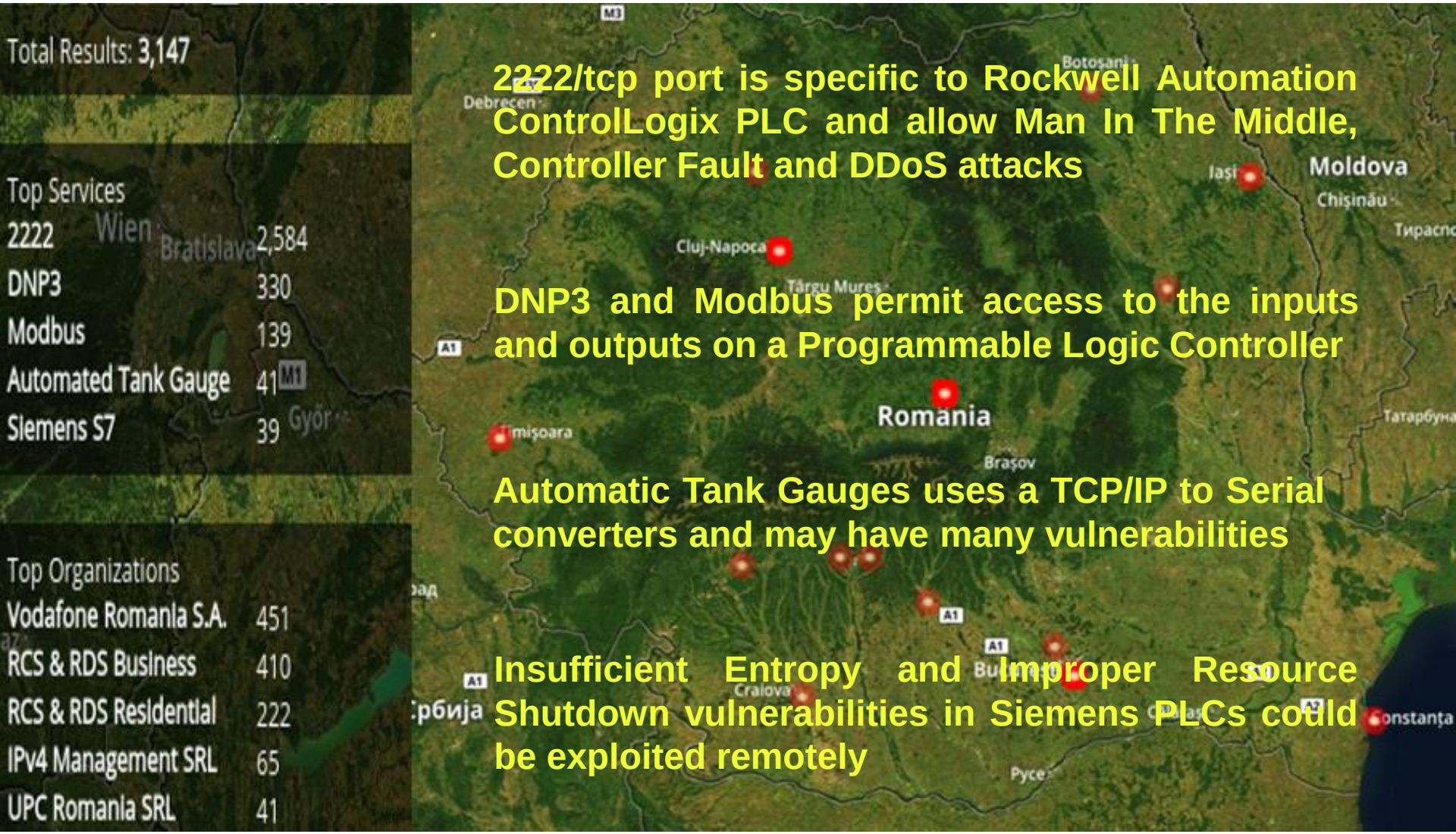
The SCADA and ICS are insecure by design and in most cases don't require an exploit to affect the process in disastrous ways.



IT and SCADA networks are interconnected



ROMANIA – SCADA Devices Connected to Internet*



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

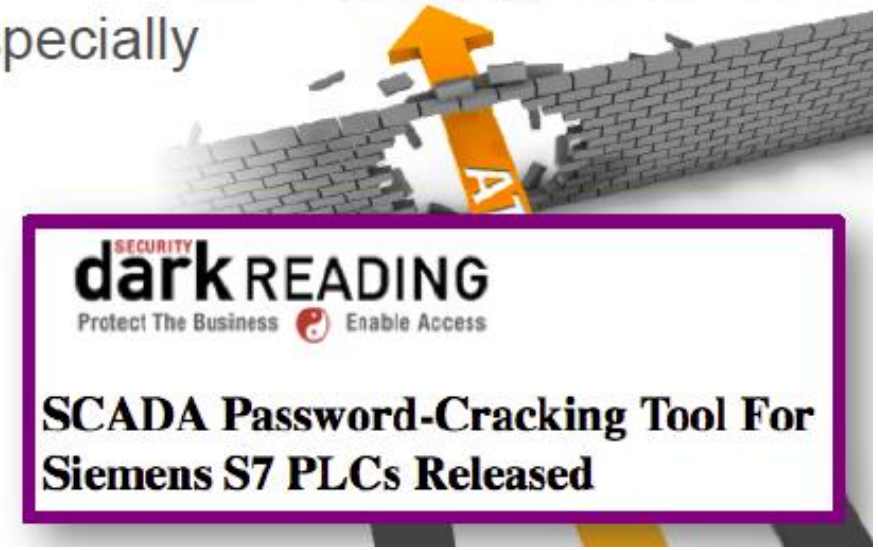
Automatic Tank Gauges uses a TCP/IP to Serial converters and may have many vulnerabilities

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

Attack, How-To?

safetech
Your trusted security partner

- **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



Protect, How-To?

1. Defense in Depth for LAN and DMZ Networks

2. Specialization Required for Core and Process Networks

Defense in depth for DNZ and LAN networks

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

Finding the Needle in a Haystack

Machine learning cyber security solutions for detecting “pattern of life” and deviations from normality

Specialization for Core and Process Networks with Xsense from CyberX

safetech
Your trusted security partner

- 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

Safetech approach for SCADA security

safetech
Your trusted security partner

Independently Log ALL SCADA activity

Define Baseline
(Allowed / Not Allowed / Suspicious)

Identify Deviations

Alert / Prevent

safetech

Your trusted security partner

www.safetech.ro

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