SECURITY OF CRITICAL INFRASTRUCTURES

Tomáš Pitner

IT pro praxi 2022

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

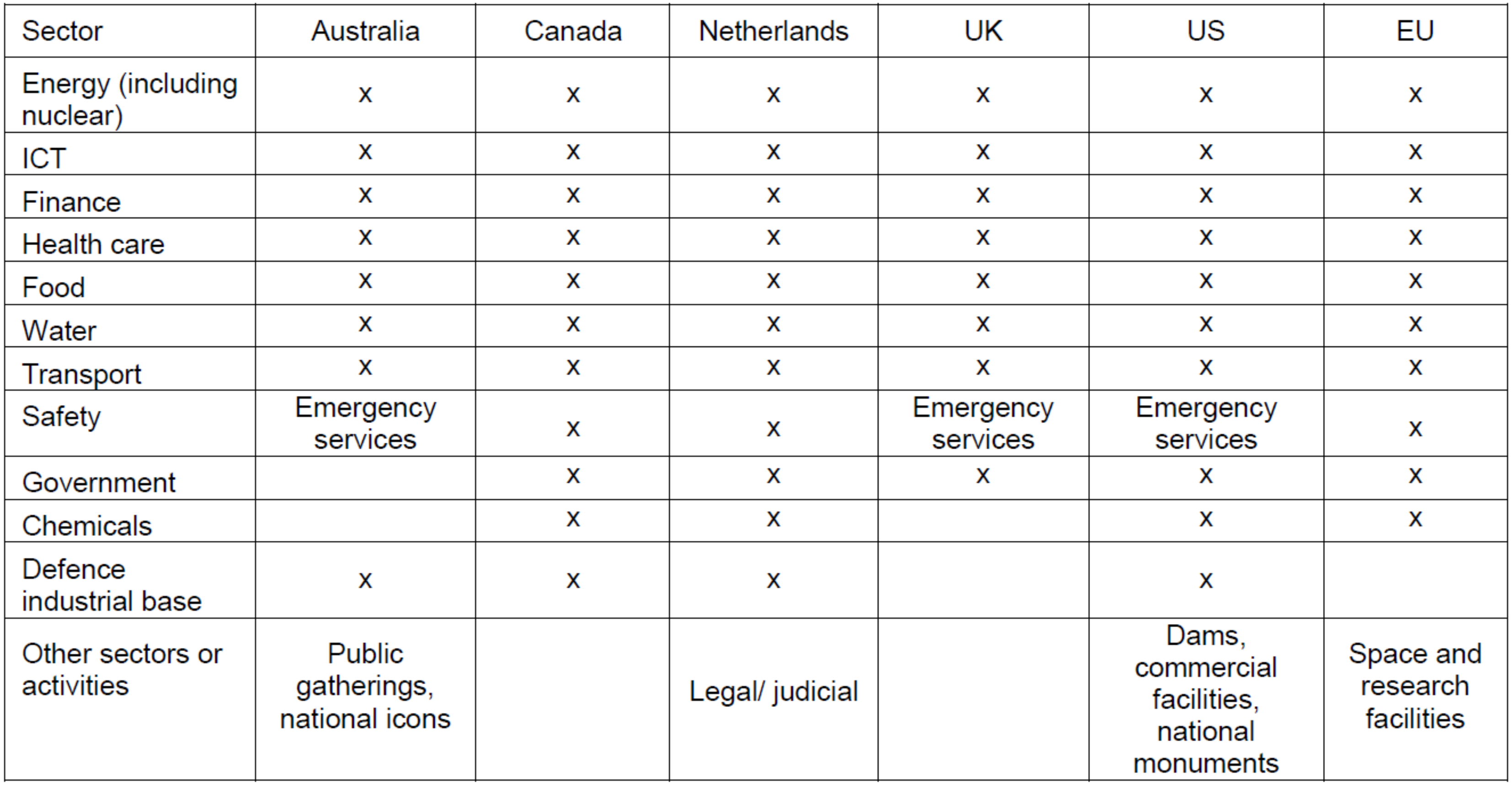
FACULTY OF INFORMATICS
MASARYK UNIVERSITY

Terminology

- The domain of Critical (Information) Infrastructures is rather complex

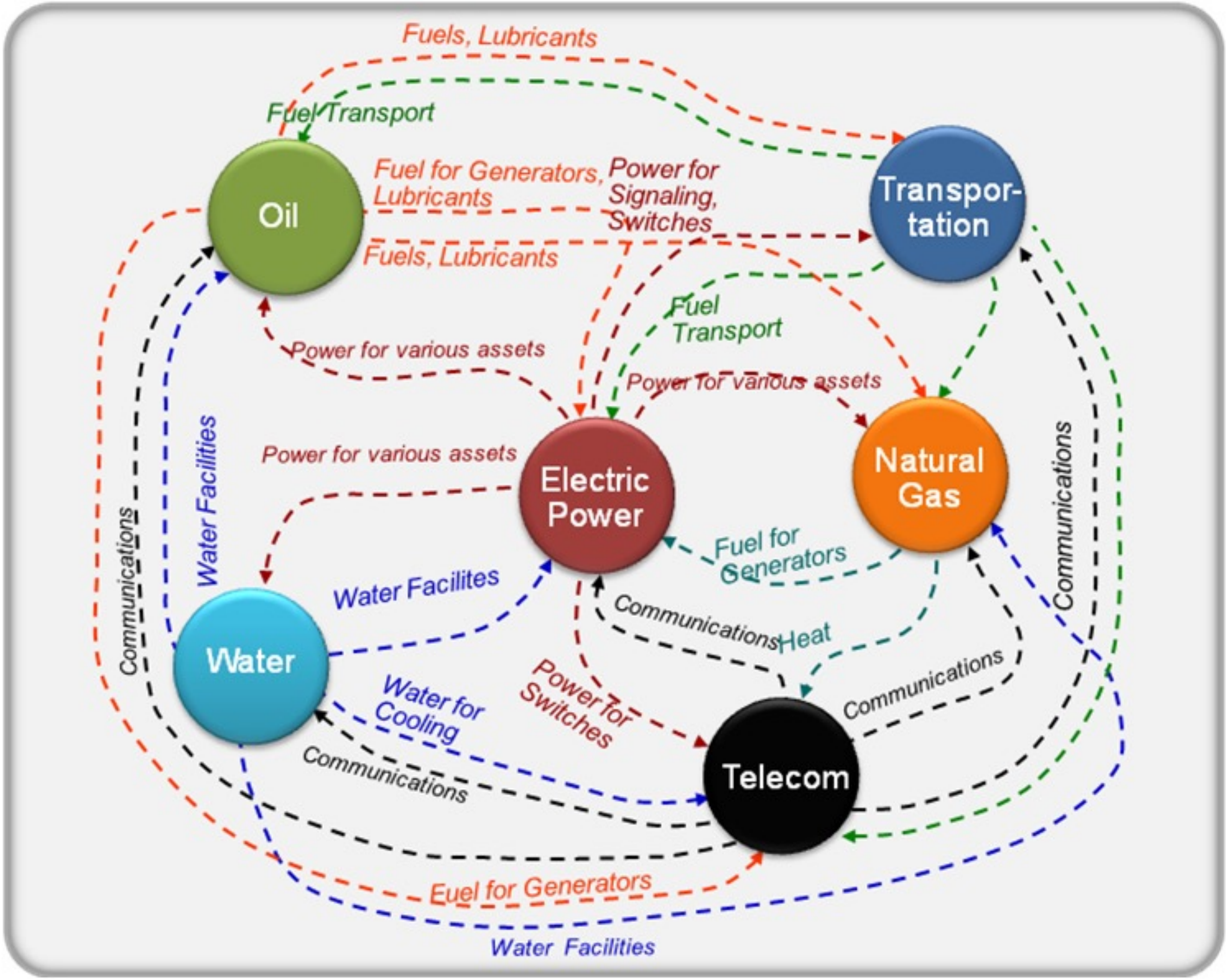
- There are many entities and organizations concerned with this domain
  - **Countries**
  - Unions/Federations
  - **Standards** organization
  - **Private** organizations

What is Critical Infrastructure?



Sector	Australia	Canada	Netherlands	UK	US	EU
Energy (including nuclear)	x	x	x	x	x	x
ICT	x	x	x	x	x	x
Finance	x	x	x	x	x	x
Health care	x	x	x	x	x	x
Food	x	x	x	x	x	x
Water	x	x	x	x	x	x
Transport	x	x	x	x	x	x
Safety	Emergency services	x	x	Emergency services	Emergency services	x
Government		x	x	x	x	x
Chemicals		x	x		x	x
Defence industrial base	x	x	x		x	
Other sectors or activities	Public gatherings, national icons		Legal/ judicial		Dams, commercial facilities, national monuments	Space and research facilities

OECD (2008) , Protection of critical infrastructure and the role of investment policies relating to national security



Rinaldi, S. et al. 2001. Identifying, understanding and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine

Critical Infrastructure

- ***Element of Critical Infrastructure*** *– element such as building, device, resource, and public infrastructure defined by law (decided by so-called cross-cutting and sectoral criteria).*
- ***Critical Infrastructure*** *– element, or system of elements of Critical Infrastructure whose disruption of functionality would result in a* ***serious impact on state security, basic living needs of citizens, public health and well-being, and state economy****.*

Czech Republic, The Act no. 240/2000 Coll. on Crisis Management

Critical Information Infrastructure

- The penetration and interoperability of ICT is ever-growing
- ICT is nowadays a part of many CIs
- The protection of CI means also protection of its ICT
- The **information infrastructure** is becoming CI itself

Critical Information Infrastructure

- ***Critical Information Infrastructure*** *– element, or system of elements of Critical Infrastructure in the sector of communication and information systems.*

  Czech Republic, The Act no. 181/2014 Coll. on the Cyber Security

- The law defines several categories of **technological elements** for the sector of communication and information systems

Sector of communication and IS

- Technological elements of:
  - wired communication networks
  - cellular communication networks
  - radio and TV broadcasting networks
  - satellite communication
  - mail services
  - information systems

Czech Republic, Act No. 432/2010 Coll. Criteria for determining the elements of critical infrastructure

The Act on Cyber Security

- *Cyberspace – digital environment that enables creation, processing and exchange of information originated in information systems, services and electronic communication networks.*

- *Information security – ensuring confidentiality, integrity and availability of information.*

Czech Republic, The Act no. 181/2014 Coll. on the Cyber Security

Cyberspace (union of existing definitions)

- *Interconnected virtual environment consisting of:*
  - Information (in any form)
  - Communications
  - Social and Human interactions
  - Application and Services
  - Internet and Networks
  - *Hardware* (in the terms of information it holds)*

- More on this topic
  - Rajnovic D., Cyberspace – What is it?, 2012. [Online]. Available: http://blogs.cisco.com/security/cyberspace-what-is-it/ [Accessed: 2014-Sep-29].

MAJOR CYBERATTACKS AGAINST CII

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY

Evil Corp, we have delivered on our promise as expected. The people of the world who have been enslaved by you have been freed. Your financial data has been destroyed. Any attempts to salvage it will be utterly futile. Face it: you have been owned.

– MR ROBOT

2007 Estonia Cyber-attacks

- Part of a wider political conflict between Estonia and Russia over the relocation of a Soviet-era monument in Tallinn

- Mainly Distributed Denial of Service attacks (**22 days**)
  - public and government web servers
  - e-mail servers, **DNS servers and routers**

- Majority of malicious traffic originated outside of Estonia

2007 Estonia Cyber-attacks

- Targets
  - government, president, parliament, police, banks
  - Internet service providers (ISPs), online media

- Very sophisticated and large attack at the time
  - pings, botnets, router vulnerabilities

- Responsibility?
  - False flag operation to frame Russia
  - Grass root level response
  - Russian information operation against Estonia

2007 Estonia Cyber-attacks

- Instructions disseminated in many Russian language forums and websites

- Due to the nature of Internet, it is hard to collect evidence (and equally hard to submit it)
  - Traffic can be routed through another country
  - Missing/immature legal grounds

- Russian state attorney refused to cooperate in order to track down its residents
  - Only one person convicted – acting from within Estonia

2012 Saudi Aramco Cyber-attack

- Saudi Arabia’s national oil and gas firm
  - Holds 10% of global oil supply with sales over $200B p.a.
  - Est. 33k soldiers and 5k guards are protecting its facilities
  - The level of ICT security is subject of discussion

- Politically motivated cyber crime (Hacktivism)

- Reportedly **30,000** infected machines (75%)
  - Potential data loss
  - Operational costs
  - Service disruption (1-2 weeks)

lasaris

2012 Saudi Aramco Cyber-attack

- Use of *Shamoon* virus (W32.Disttrack)
  - Self-replicating MS Windows-based worm
  - Hardcoded day of attack – 15th August 2012 08:08 UTC
  - Corrupts files on hard-drive of the infected machine

- Three main components
  - *Dropper*: main component that drops other modules and is the first to infect the system
  - *Reporter*: module that reports infection information back to the attacker
  - *Wiper*: module that contains destructive functionality

2012 Saudi Aramco Cyber-attack

- Introducing Shamoon probably required physical access to computer in the Aramco's network
- Infected machine served as a proxy for C&C server and spread the infection to the rest of the network
  - Pseudo-random propagation via Remote Task Scheduler
- Reportedly, drilling and production data were lost
- In addition, the machines were rendered virtually unusable due to MBR corruption

Consequences of CA in Physical World

- Let us assume that some Cyber-physical system is part of the given Cyberspace
- The Cybersecurity (infosec of Cyberspace) is compromised
- Then, Cyber-attack manifests itself in the physical world
- Example: Traffic lights connected to traffic control

Stuxnet

- Semi-targeted computer worm (discov. June 2010)
  - Promiscuous, yet narrowly targeted
- Targets
  - Supervisory Control And Data Acquisition (SCADA) systems
  - Programmable Logic Controllers (PLCs)
- Used several zero-day vulnerabilities
- The provided information is based on available analyses and lab experiments

Stuxnet – Infecting Windows machines

- Performs privilege escalation (user SYSTEM)
- Installs kernel-mode drivers to hide files and inject code
    - The drivers were digitally signed using two stolen certificates (JMicron and Realtek)
- The ability to communicate with command-and-control servers and other worm instances

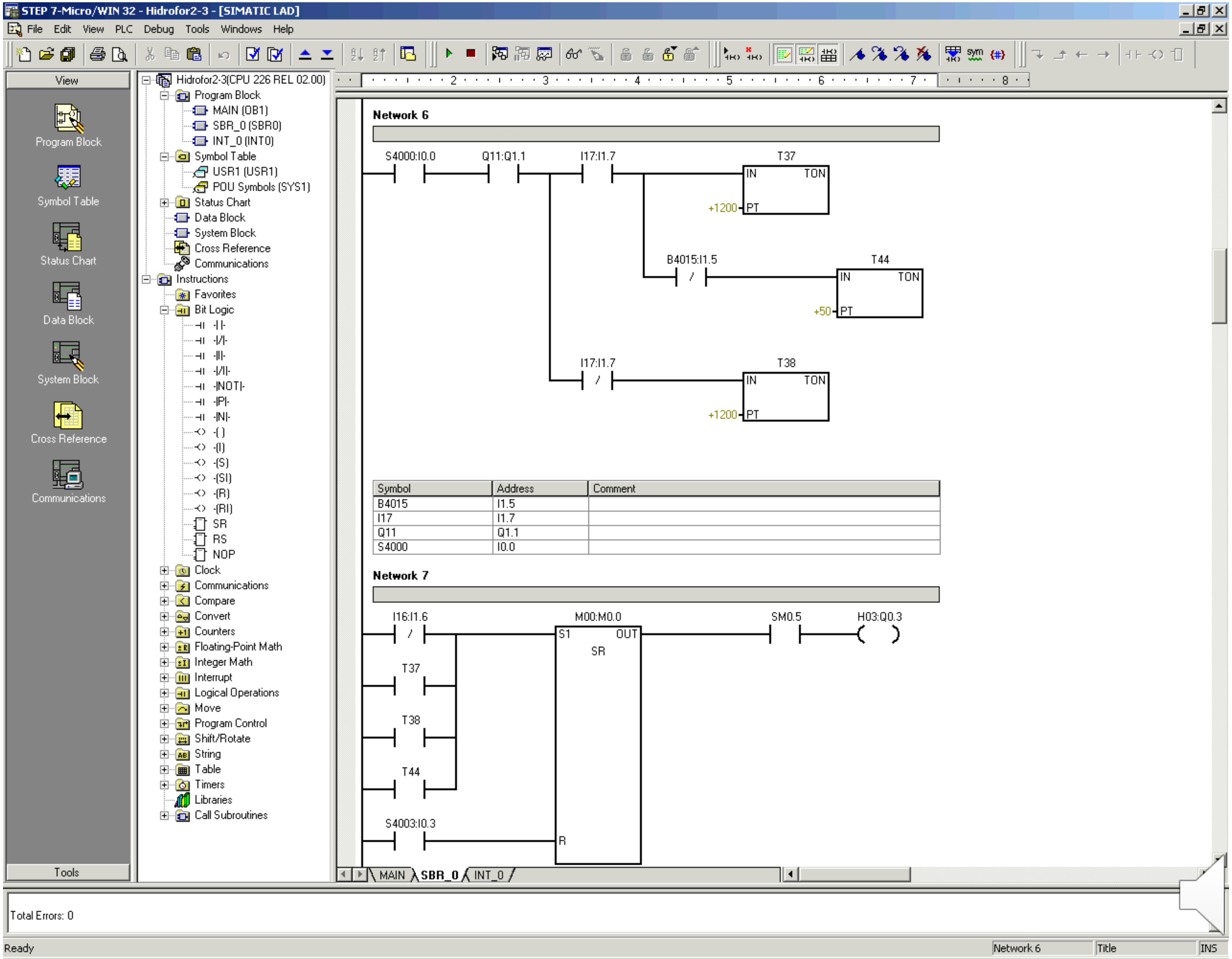
CPU314C-2 DP
SIEMENS
1A1-A102
SF
BF
DC5V
FRCE
RUN
STOP
PUSH
MRES
1A1-A104
1A1-A105
1A1-A106
1A1-A107
A102/X1
A102/X2
-A104
-A105
-A106
-A107
60.0
POWER
FUNC.
RUN
STOP/RESET
WARNING

Stuxnet – Targeting PLCs

- Searches for Siemens SIMATIC WinCC or STEP 7 SCADA software on the Windows machines, it is **inert otherwise.**

- Machines with the software are used to program, debug, and configure connected PLCs (via data-cable)

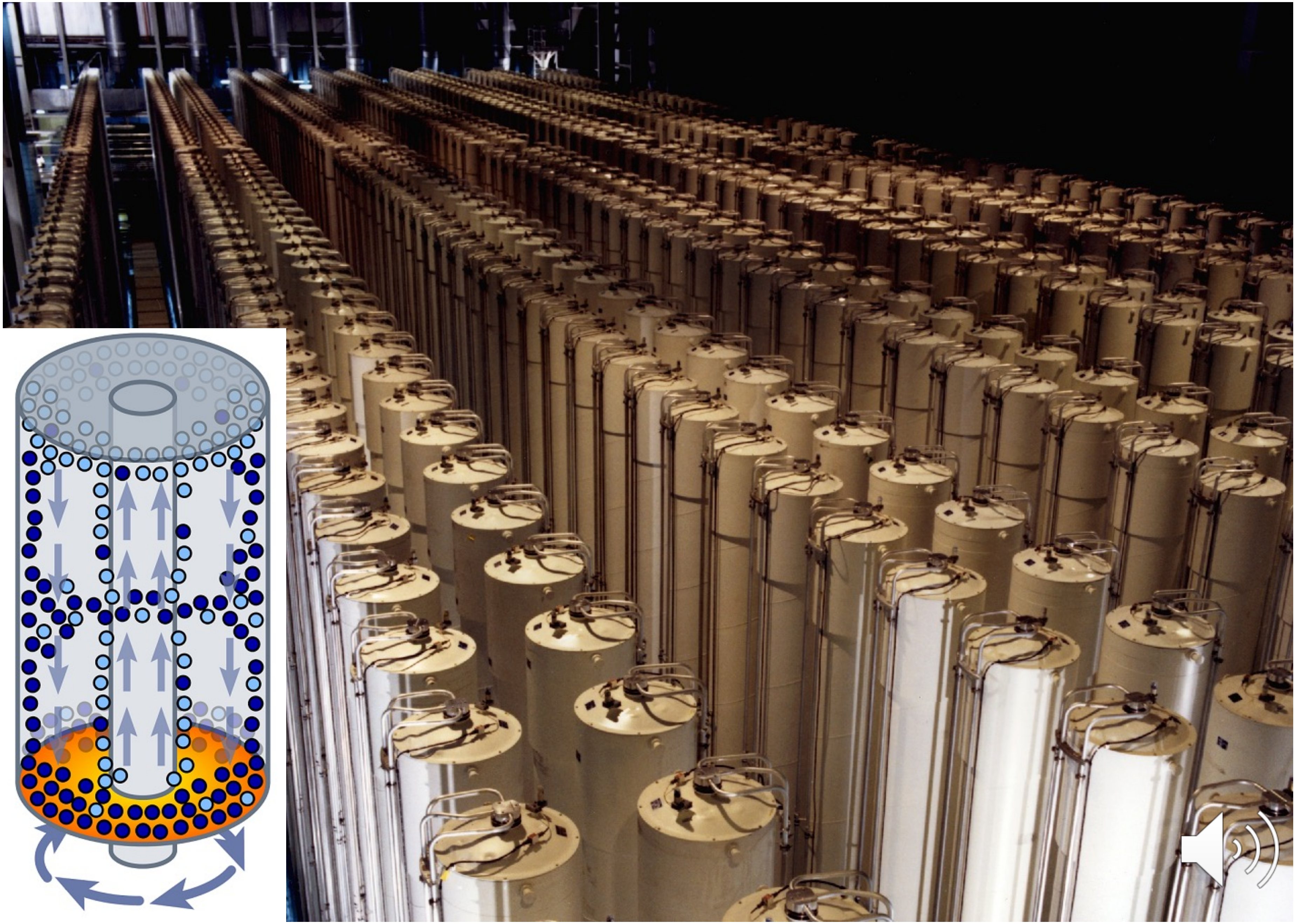
- It infects the programming software (the project files) in order to propagate malicious PLC code into the PLC (only if certain conditions are met)



Symbol	Address	Comment
B4015	I1.5	
I17	I1.7	
Q11	Q1.1	
S4000	I0.0	

Total Errors: 0

Ready



Ukraine Power Grid Under Attack in 2015

- „Attack successful compromised information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to the end consumers.“
- **30 substations switched off**
- **230,000 people without electricity** for 1 to 6 hours

- Wikipedia

Ukraine Power Grid Under Attack in 2015

- Compromise of corporate networks using **spear-phishing** emails with BlackEnergy malware;
- **seizing SCADA under control**
- remotely **switching substations off**;
- **disabling/destroying IT infrastructure** components (uninterruptible power supplies, modems, RTUs, commutators);
- **destruction of files** stored on servers and workstations with the KillDisk malware;
- **denial-of-service attack** on call-center to deny consumers up-to-date information on the blackout.

Ukraine a year after… (2016)

- **Industroyer**[1] (a.k.a. **Crashoverride**) is a malware framework considered to have been used in the cyberattack on Ukraine's power grid on December 17, 2016.
- The attack cut **a fifth of Kiev**, the capital, off power for **one hour** and is considered to have been a large-scale test.

The cause: *Industroyer*

- Discovered by Slovak internet security company ESET
- Architecture of the threat:
- **Main** backdoor is used to control all other components:
  - connects to its remote Command & Control servers
  - to receive commands from the attackers
- **Additional backdoor** as alternative persistence mechanism
  - regain access to a targeted network in case the main backdoor is detected and/or disabled.

The cause: *Industroyer*

- **A launcher component** is a separate executable
  - launching the payload components and the data wiper component.
  - contains a specific activation time and date
- **Four payload components** target particular industrial communication protocols specified in the following standards:
  - IEC 60870-5-101, IEC 60870-5-104, IEC 61850, and OLE for Process Control Data Access
  - include mapping the network
  - issuing commands to the specific industrial control devices.
- **A data wiper component** is designed to erase system-crucial Registry keys and overwrite files to make the system unbootable and recovery from the attack harder.

Czech Republic Attacks (2013)

- Series of (Distributed) Denial of Service attacks on public web servers
- Two waves of attacks each day (9am-11am, 2pm-4pm)
- SYN Flood attack with spoofed IP addresses
  - Bounce traffic, Reflection attack
- Most of the traffic originated in RETN network
  - International back-bone fiber-optic network
  - Did not respond to calls for help

Czech Republic Attacks (2020)

- Targeted at hospitals – large (Brno, Olomouc) and small (Benešov)
- Synchronized(?) with Covid-19 outbreak
- 40 M CZK/day in losses
- Largely due to underestimation
- Low investment in HW, OS, but mainly human resources
- Reactive measures immediately applied
- Coordinated help of Czech NSA (NÚKIB), Gov-CERT, CZ.NIC (CSIRT.CZ)