PA018 – ADVANCED TOPICS IN IT SECURITY

CRITICAL INFRASTRUCTURES

Daniel Tovarňák, Tomáš Pitner, Bacem Mbarek

Fall 2021

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY

MOTIVATION

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY

lasaris

Motivation/1

- Recent Reuters article (Oct 10, 2016): **IAEA chief: Nuclear power plant was disrupted by cyber attack**
- "**This is not an imaginary risk**," Amano told Reuters and a German newspaper during a visit to Germany that included a meeting with Foreign Minister Frank-Walter Steinmeier.
- "This issue of **cyber attacks on nuclear-related facilities or activities should be taken very seriously**. We never know if we know everything or if it's the tip of the iceberg."

Motivation/2

- Korea Hydro & Nuclear Power Co Ltd, which operates 23 nuclear reactors in South Korea, said in **2014 it was beefing up cyber security after non-critical data was stolen from its computer systems**, although reactor operations were not at risk.
- In April, German utility RWE increased its security after its Gundremmingen **nuclear power plant was found to be infected with computer viruses**. The company said they did not appear to have posed a threat to operations.
- Security experts say blowing up a nuclear reactor is beyond the skills of militant groups, but the **nuclear industry has some vulnerabilities** that could be exploited.

Motivation/3

- **Healthcare sector** – during the Covid-19 outbreak, the number of cyberattacks (DDoS, ransomware) against healthcare service providers, namely large hospitals, grew significantly – Brno Faculty Hospital (March 2020), Regional Hospital in Benešov (earlier)
- ENISA identifies healthcare as the most traditional critical sector affected by growing cybercrime danger:
- *"Connected medical devices transform the way the healthcare industry works, both within hospitals and between different actors of the healthcare industry."*

Important Note on 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

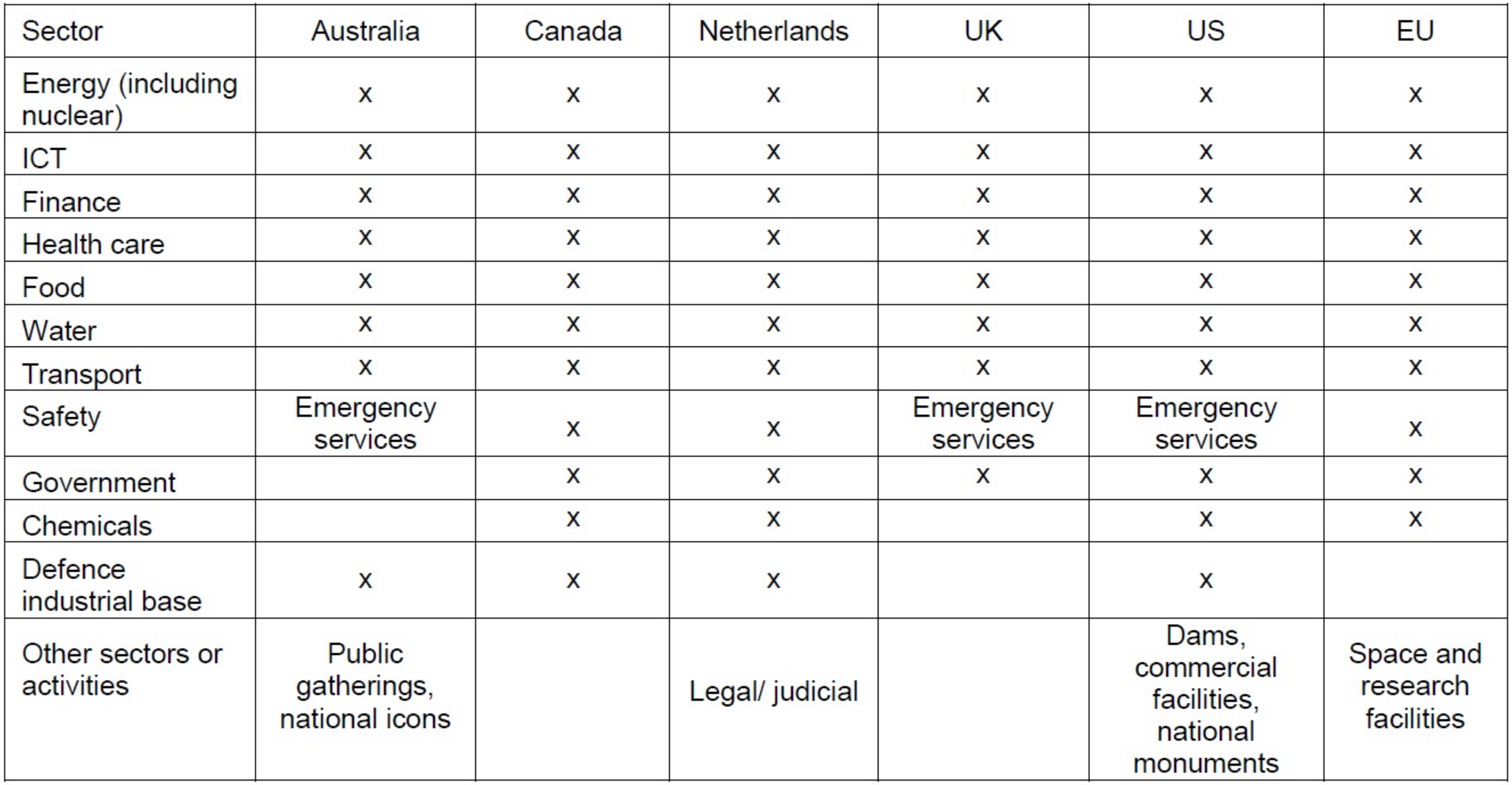
CRITICAL INFRASTRUCTURE

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY

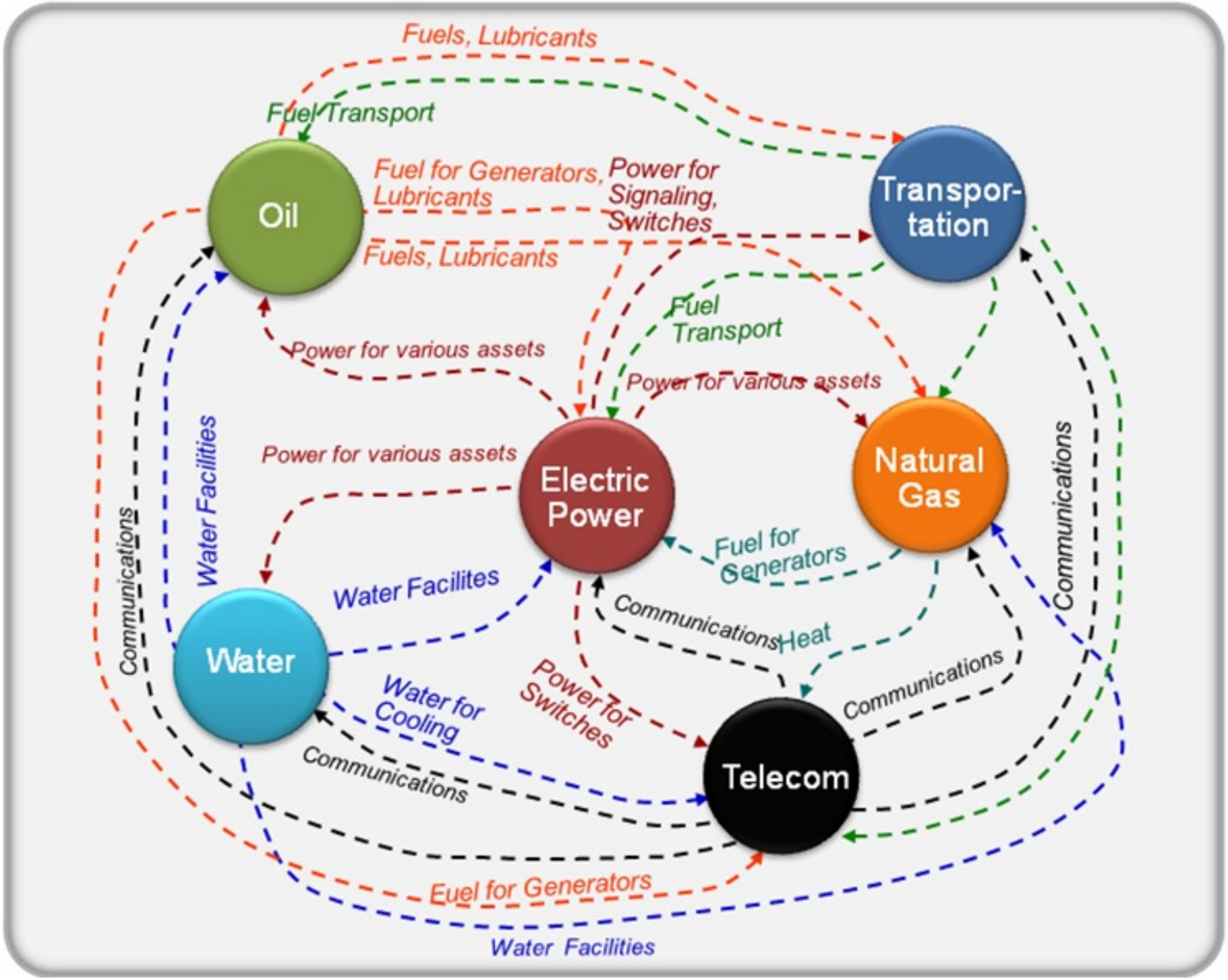
lasaris

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

Important Note on Terminology cont'd.

- As a consequence the terminology in the domain of Critical (Information) Infrastructures is fragmented
- It is almost impossible to find the *best* definition of a particular term
- For **illustration purposes**, we will provide definitions used by Czech legislation, e.g. *Cyber Security Act*. (BLUE text)

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

PROTECTION OF CYBERSPACE

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY

Cyberspace

- The current challenge of CII protection is **mainly** the protection of its Cyberspace
  - (i.e. apart from protecting CII physically)

- It is commonly said that the Cyberspace has no boundaries, but:
  - „...securing U.S. Cyberspace."
  - „...confidentiality of the Czech Republic's cyberspace..."
  - „...European cyberspace..."

- CII induces the Cyberspace at question

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].

Cyber…

- **Information Security** – the protection of information and inf. systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide *{confidentiality, integrity, availability, …}*+.
- **Cybersecurity** – infosec of the Cyberspace
- **Cyber attack** – malicious activity (w.r.t. infosec), where the Cyberspace is the target or source of such activity
- **Cyber crime** – criminal activity (w.r.t. infosec and law), where the Cyberspace is the target or source of such activity

The (Czech) Act on Cybersecurity

- Strangely enough, the Act does not define the notion of Cybersecurity
- We interpret it in a way, that the Act itself is considered by the policy makers to be a general means for achieving Cybersecurity
- It roughly follows the path of Cyberspace – Information Security – Cybersecurity

Cyber Attack

- Targets
  - Public sector
  - Private sector
  - Individuals and households
- Outcomes
  - Consequences in Cyberspace
  - Consequences in Physical World
  - Cyber-Assisted Attack
    - Physical Attack combined with Cyber Attack

MAJOR CYBERATTACKS AGAINST CII

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY

lasaris

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)

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

- Local (Initial) Self-replication
  - Removable Media
- Network Propagation
  - MS Windows Shared Folders
  - MS Windows RPC vulnerability
  - MS Windows Print Spooler vulnerability

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

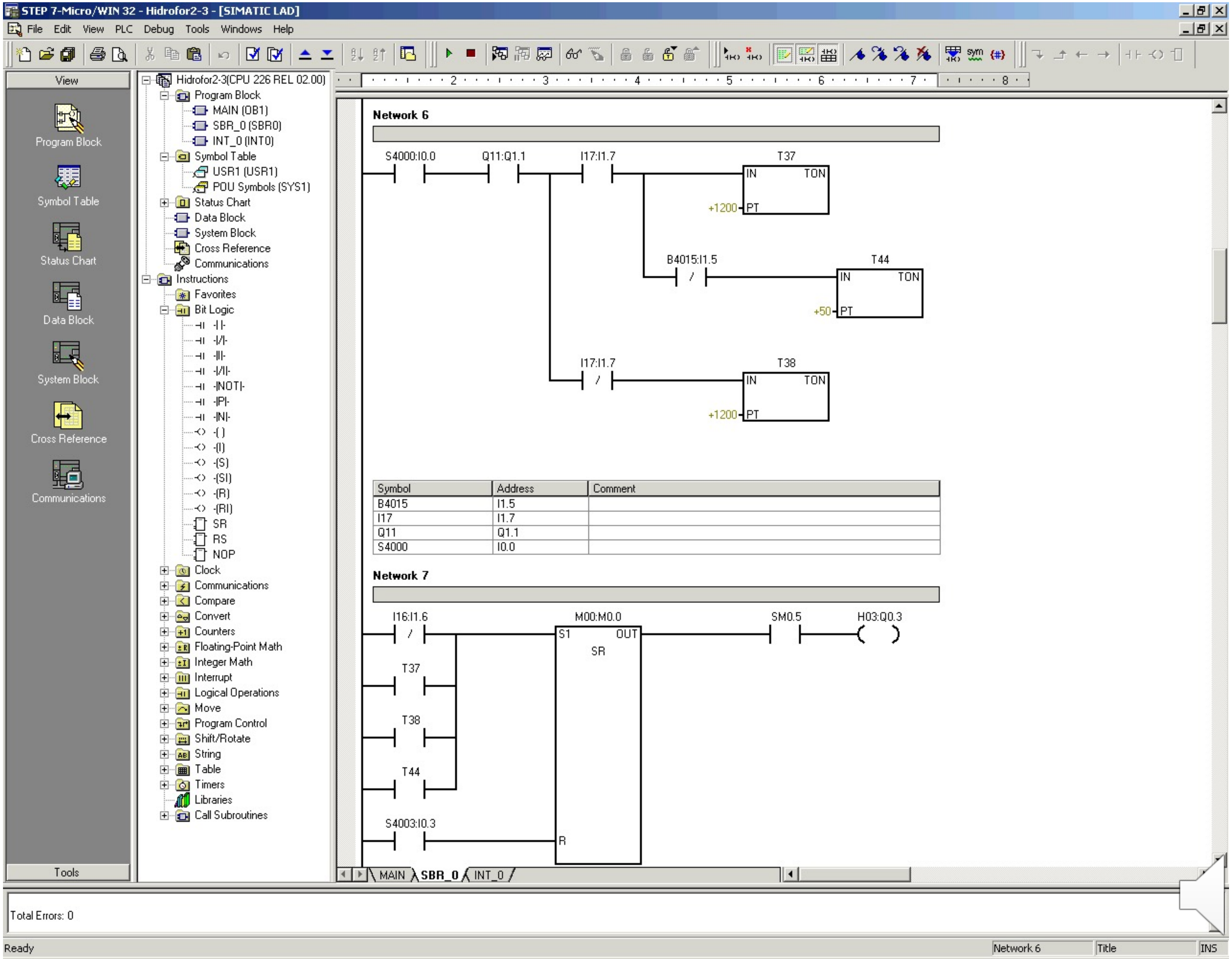
Stuxnet – Note on PLCs

- Industrial computers used for automation
- Set of logical inputs and outputs (logical high and low) connected to a microcomputer
- Based on the programming, the output values change depending on the input values
- Many simpler devices can be connected to PLC, e.g. Switches, Valves, Actuators, Pumps, Fans, etc.

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)



Network 6

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

Network 7

Total Errors: 0

Ready

Stuxnet – Targeting PLCs

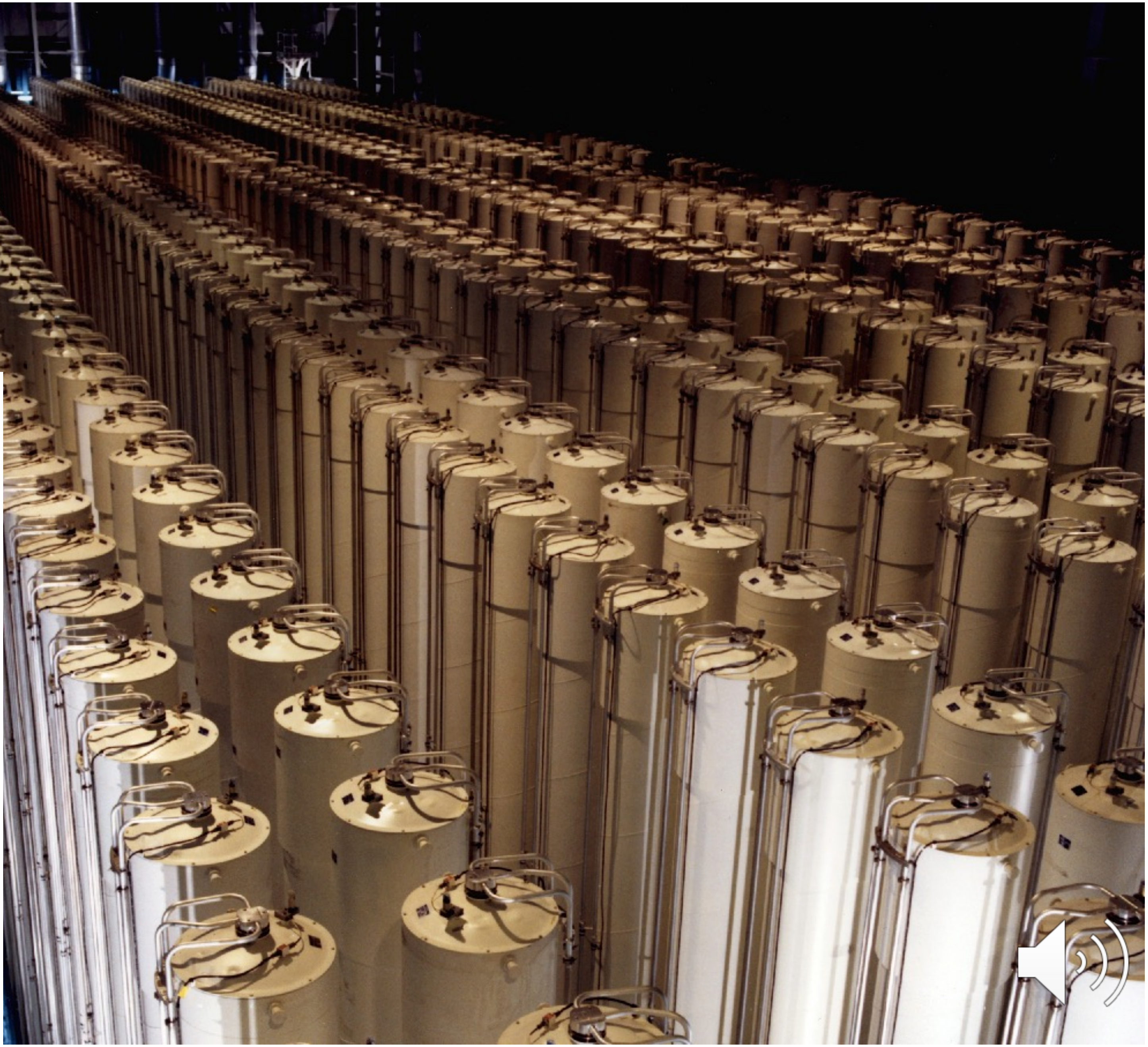
- Requires the PLC to be equipped with particular type/version of CPU and communications module
- Requires **frequency converter drives** from at least one of two specific vendors to be connected
  - FCD is a power supply that can change the frequency of the output, which controls the speed of a motor
- After the infection the malicious PLC code determines if the frequency drives are running between 807 Hz and 1210 Hz

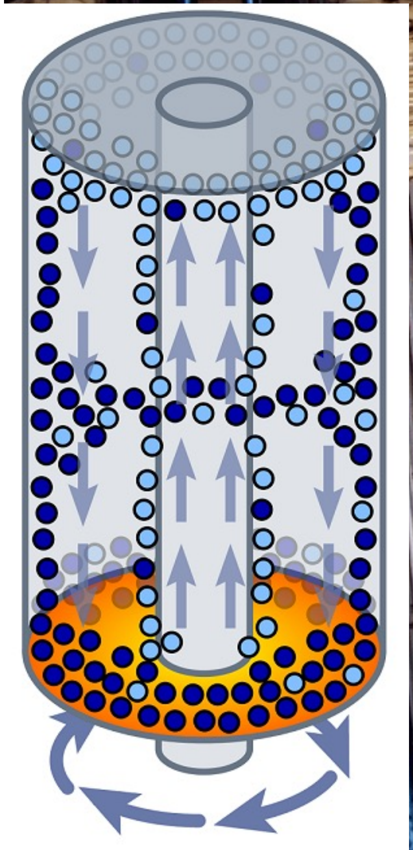
Stuxnet – Malicious Activity on the PLC

- After some time (days) the core malicious activity is executed
- The frequency of the drives are periodically changed to 1410Hz, 2Hz, and 1064Hz over the course of several months
- The PLC code records the previous operating frequencies and play them back to avoid detection

Stuxnet – Speculated Target

- The frequencies are considered to be quite high and limit the potential speculated targets in industry
- It is a typical operating frequency of gas centrifuges which are used for **uranium enrichment**
- The targeting requirements (versions of PLCs, frequency drives and their frequencies) and other facts hint at **Natanz nuclear facilities, Iran**





Stuxnet – Natanz nuclear facilities

- As of Sep. 2010 approximately 60% of infected hosts were in Iran
- In 2009 “serious nuclear accident” occurred in Natanz plant (WikiLeaks)
- In six-month period (2009/2010) more than 10 percent of the Natanz plant's 9,000 centrifuges were dismantled (according to UN video-footage)

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.

PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

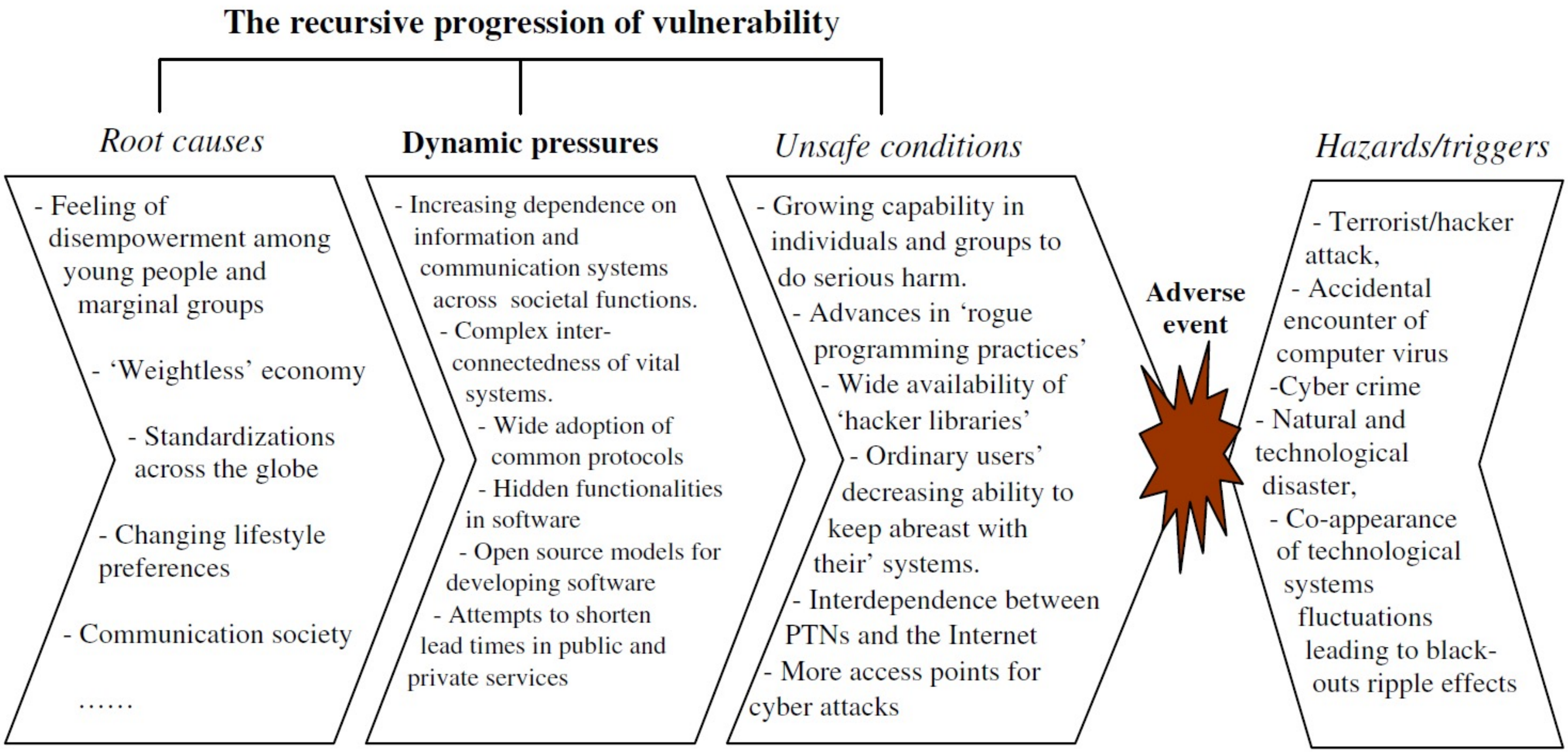
FACULTY OF INFORMATICS
MASARYK UNIVERSITY

C(I)I Protection not an easy task

- We have not discussed many aspects that render the C(I)I protection to be a very interesting problem

- **Vulnerability**
- C(I)Is are **unbounded and networked**
- **Human factor**
- **Private vs. Public**
- **Complexity**

Challenge: CII Vulnerability



The recursive progression of vulnerability

Root causes

- Feeling of disempowerment among young people and marginal groups
- ‘Weightless’ economy
- Standardizations across the globe
- Changing lifestyle preferences
- Communication society

……

Dynamic pressures

- Increasing dependence on information and communication systems across societal functions.
- Complex inter-connectedness of vital systems.
- Wide adoption of common protocols
- Hidden functionalities in software
- Open source models for developing software
- Attempts to shorten lead times in public and private services

Unsafe conditions

- Growing capability in individuals and groups to do serious harm.
- Advances in ‘rogue programming practices’
- Wide availability of ‘hacker libraries’
- Ordinary users’ decreasing ability to keep abreast with their’ systems.
- Interdependence between PTNs and the Internet
- More access points for cyber attacks

Adverse event

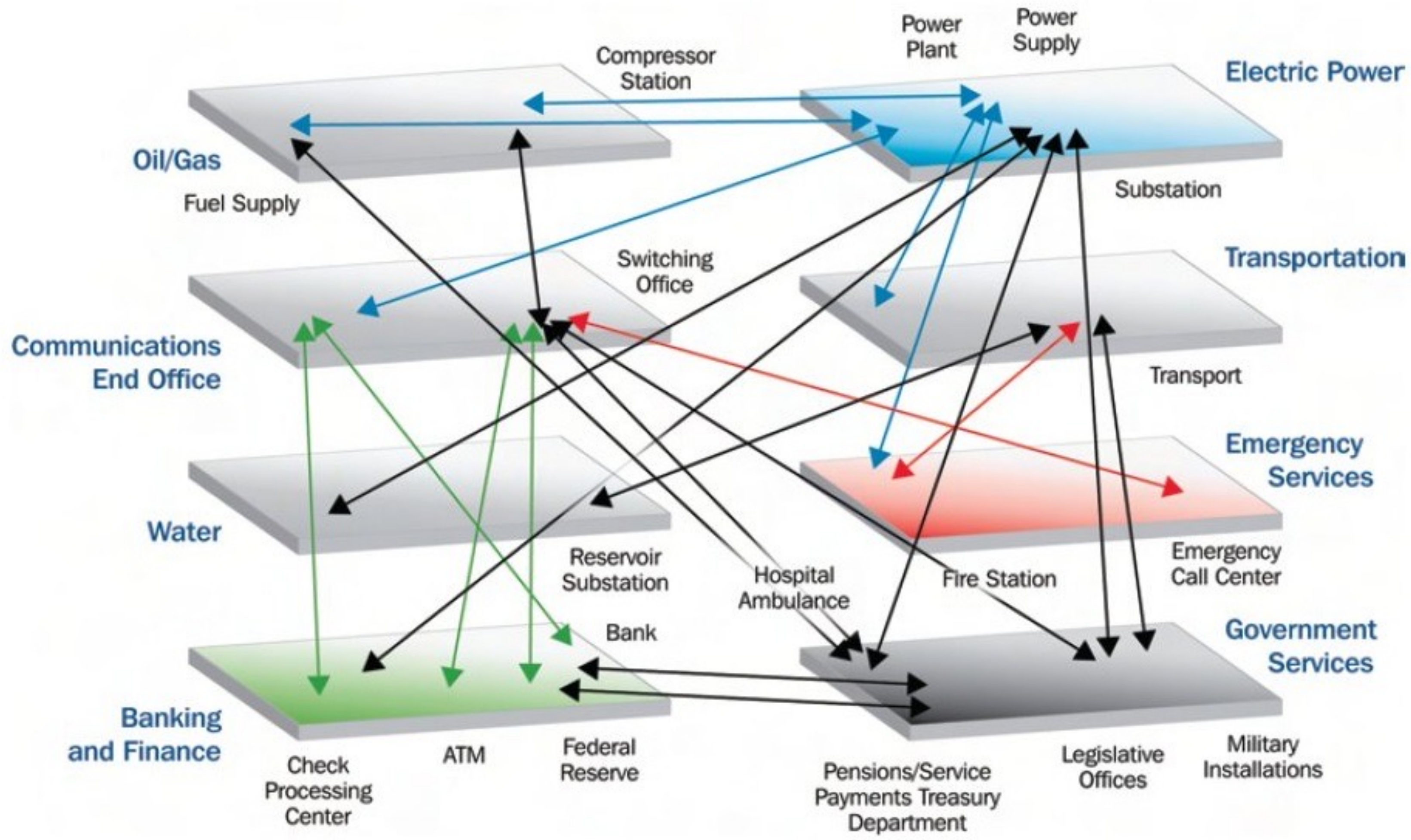
Hazards/triggers

- Terrorist/hacker attack,
- Accidental encounter of computer virus
- Cyber crime
- Natural and technological disaster,
- Co-appearance of technological systems fluctuations leading to black-outs ripple effects

Hellström T., 2007. Critical infrastructure and systemic vulnerability: Towards a planning framework

Challenge: C(I)Is are unbounded and networked

- Both in real-world and Cyberspace
- Especially in the case of CII there are **no physical barriers** nor **political boundaries**
- Identifying **responsibilities** in terms of security policies is not easy (regulatory compliance, malicious activity tracking)
- CIs are an **increasingly large-scale**, **interconnected** open network, and **dynamically** evolving environment



Dept. of Homeland Security (US), **National Infrastructure Protection Plan**
www.dhs.gov/files/programs/editorial_0827.shtm

Challenge: Human factor

- Critical infrastructures depend on human decisions
- As the complexity grows the human actors’ expertise and knowledge must also be able to do so
- Knowledge of ordinary tasks may become inadequate to face emergencies
- Insider threat is enormous as well as human error

Challenge: Public vs. Private sector

- There are many actors even in single C(I)I
- Many (if not most) infrastructures are private, yet the state has the responsibility and must rely on information sharing
- Public-private partnership/platform is needed

Challenge: Complexity

- Large networks are **inherently unstable**
- No (ICT) system can be considered **ultimately secure**
- Local disruptions may have an **impact on many countries**
- **Global legal frameworks** and **institutions** are lacking
- Global players face huge administrative burden when responding to **fragmented national** C(I)IP policies

CYBERSECURITY IN EU

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY

lasaris

The Key Bodies in EU (w.r.t. Cybersec)

- **Legislation**
  - European Commission
- **Policy/Guidelines**
  - ENISA: European Network and Information Security Agency
- **Law Enforcement**
  - Europol
- **Defense and Response**
  - TF-CSIRT: Collaboration of Security Incident Response Teams
  - National CERTs

Example: ENISA Guidebook – PLAN/DO

- Set the **vision, scope, objectives** and priorities
- Follow a **national risk assessment** approach
- Take stock of existing policies, regulations and capabilities
- Develop a **clear governance** structure
- Identify and **engage stakeholders**
- Establish **trusted information-sharing** mechanisms
- Develop national **cyber contingency** plans
- Organize **cyber security exercises**
- Establish **baseline security requirements**

Example: ENISA Guidebook – PLAN/DO

- Establish **incident reporting** mechanisms
- User **awareness**
- Foster **R&D**
- Strengthen **training and educational** programmes
- Establish an **incident response** capability
- Address **cyber crime**
- Engage in **international cooperation**
- Establish a **public–private partnership**
- Balance **security with privacy**

Cybersecurity on National Level

- **Governmental** level
  - e.g. establishment of coherent actions on Cybersecurity within the government (departments, ministries)
- **National** level
  - e.g. establishment of public-private collaboration platform
- **International** level
  - e.g. collaboration with international partners
  - e.g. non-governmental agreements between technical certification bodies

CYBERSECURITY IN CZECH REPUBLIC

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY

lasaris

Cybersecurity in Czech Republic

- Czech Republic, The Act no. 181/2014 Coll. on the Cyber Security
- (updated: 104/2017 Sb., 183/2017 Sb., 205/2017 Sb., 35/2018 Sb., 12/2020 Sb., 111/2019 Sb., 12/2020 Sb., 261/2021 Sb.)
- Masaryk University was part of the legislation process
  - Also Czech CyberCrime Centre of Excellence (C4E) Project
- Follows general **information security approach** (risk-based, ISO27k-like)

The Act on the Cyber Security

- Defines **liable persons** in the context of national Cybersecurity
  - **NÚKIB** (National Cybersecurity Agency – in Brno) as the head
- Establishes the notion of **National-CERT**
- Establishes the notion of **Government-CERT**
- **Liable persons** defined in the Act must implement and execute security controls to ensure information security in cyberspace.

CYBERATTACKS IN CZECH REPUBLIC

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

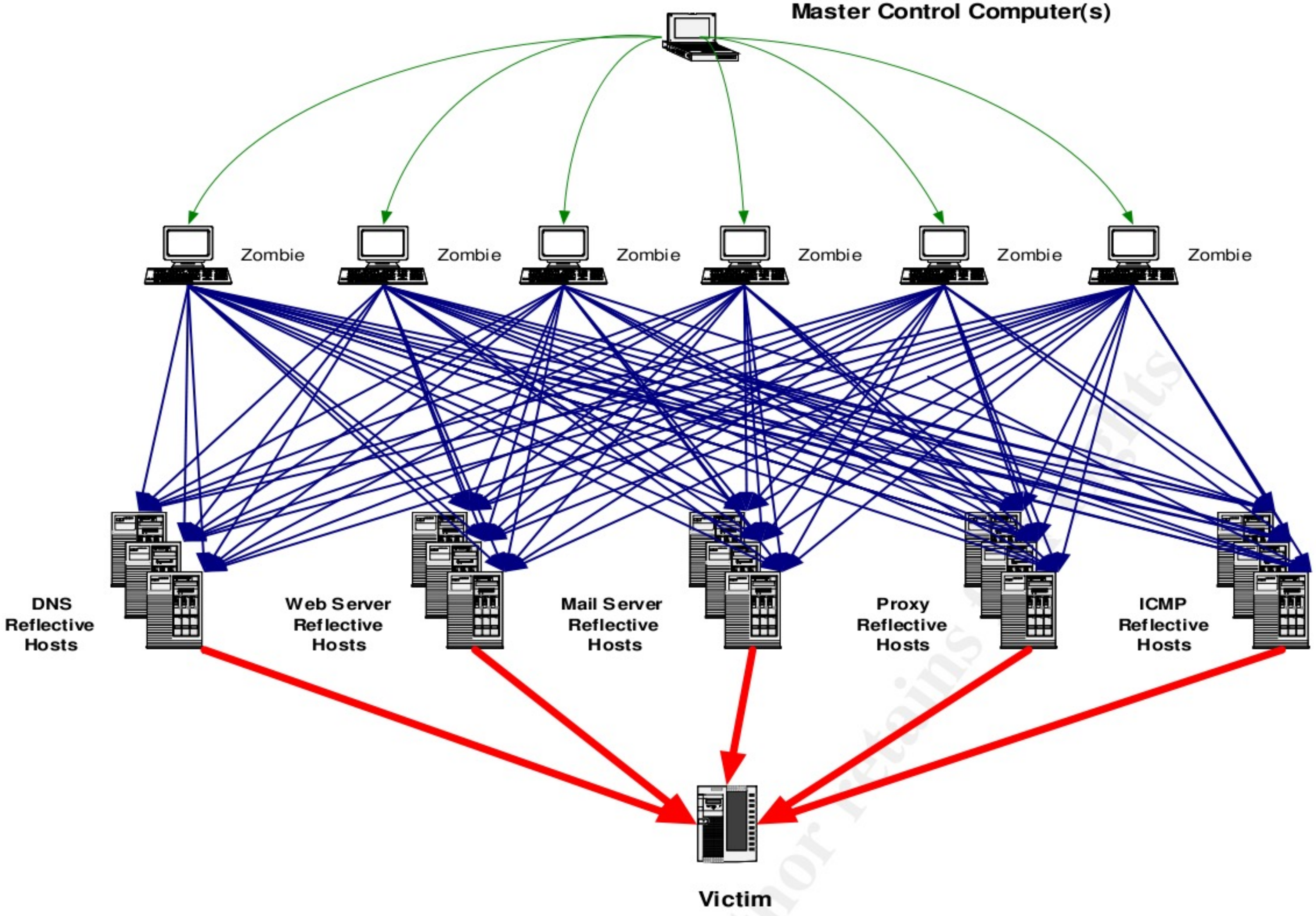
FACULTY OF INFORMATICS
MASARYK UNIVERSITY

lasaris

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

DRDoS


Master Control Computer(s)
Zombie
Zombie
Zombie
Zombie
Zombie
Zombie
DNS Reflective Hosts
Web Server Reflective Hosts
Mail Server Reflective Hosts
Proxy Reflective Hosts
ICMP Reflective Hosts
Victim

Czech Republic Attacks (2013) – Targets

- **Monday**: *Major news web-servers (idnes.cz, ihned.cz, novinky.cz, e15.cz)*
- **Tuesday**: *Largest web-search engine (seznam.cz)*
- **Wednesday**: *Web-servers of several banks. E-commerce and payment gateways outage reported.*
- **Thursday**: *Mobile network operators*

- Reports of dpp.cz outage, Car registry outage
- DPP SMS Tickets gateway outage

Czech Republic Attacks (2013)

- In many cases the malicious traffic did not reach the targeted servers – it overloaded the systems along the route (firewalls, load balancers).

- The traffic on CESNET border links **peaked at ~300k flows/s**
  - Can be considered relatively weak

- Rather well prepared attacks with **obvious knowledge** of Czech internet

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)

CII IN POWER SECTOR

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

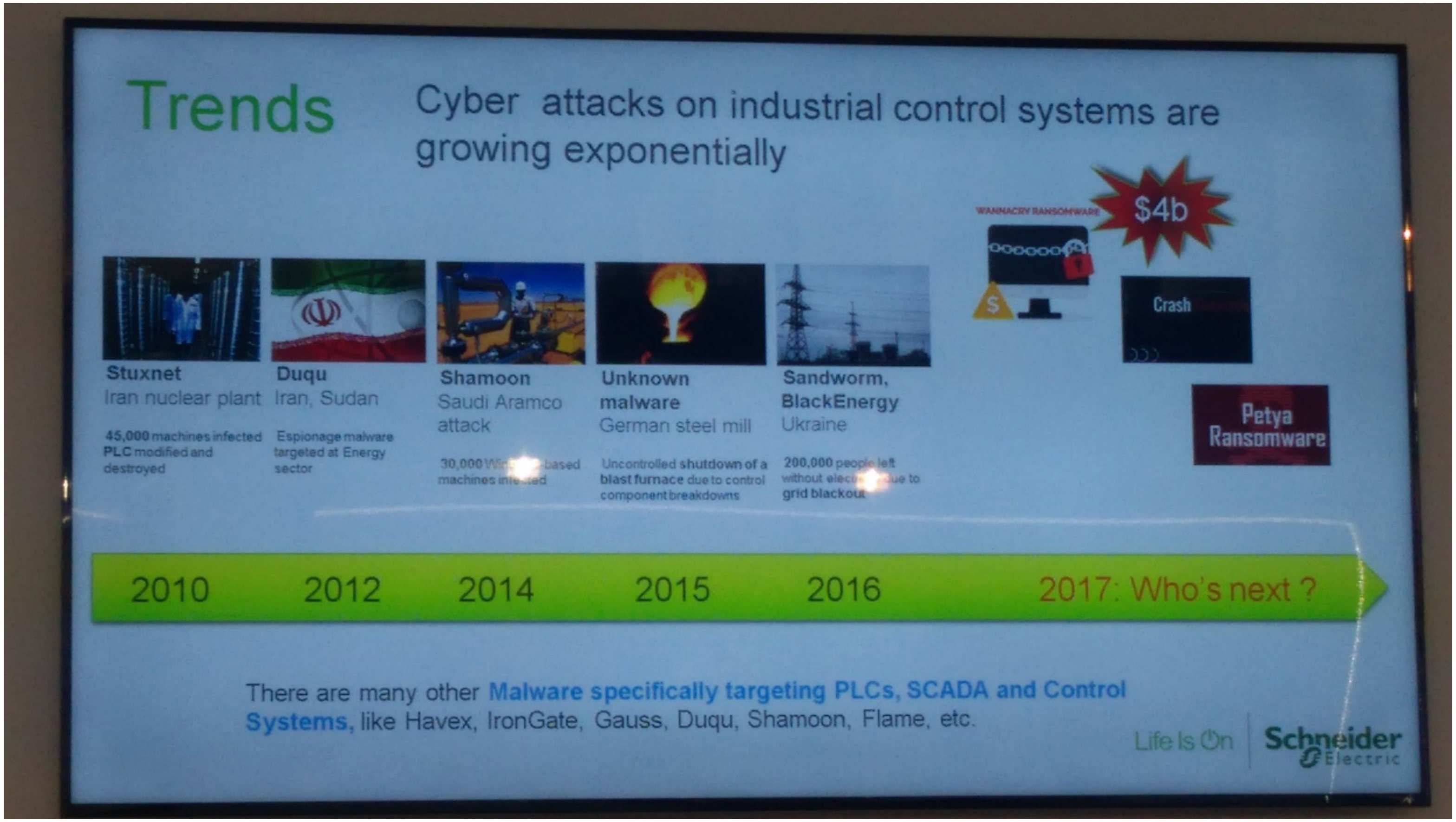
FACULTY OF INFORMATICS
MASARYK UNIVERSITY

lasaris

Motivation

- **Industroyer – A cyberweapon can disrupt power grids** (Washington Post, June 12, 2017)
- **Trump signs cybersecurity order** (CNBC, May 11, 2017)
- **Ukraines Power Outage Was a Cyberattack** (Reuters, Jan 18, 2017)
- **US Finds Proof: Cyberattack on Ukraine Power Grids** (CNN, Feb 3, 2016)
- **A Worm in the Centrifuge** (Economist, Sep 10, 2010)
- *… More to come?*

Motivation – trends



Trends

Cyber attacks on industrial control systems are growing exponentially

Stuxnet
Iran nuclear plant
45,000 machines infected
PLC modified and destroyed

Duqu
Iran, Sudan
Espionage malware targeted at Energy sector

Shamoon
Saudi Aramco attack
30,000 Windows-based machines infected

Unknown malware
German steel mill
Uncontrolled **shutdown of a blast furnace** due to control component breakdowns

Sandworm, BlackEnergy
Ukraine
200,000 people left without electricity due to **grid blackout**

2010 2012 2014 2015 2016 2017: Who's next ?

There are many other **Malware specifically targeting PLCs, SCADA and Control Systems,** like Havex, IronGate, Gauss, Duqu, Shamoon, Flame, etc.

Life Is On | Schneider Electric

Source: Schneider Electric, Hub Session on Grid Intelligence, EUW 2017

Critical Inf. Infrastructure in Energy sector

- For PA108 aimed at electricity. Electricity lifecycle:
  - **Production** – power stations (EHV, HV levels), distributed (renewable) resources (MV, LV levels)
  - **Transmission** – EHV, HV levels; long distance or transboundary
  - **Distribution** grid – HV, MV, LV levels
  - **Consumption** – MV or LV levels; combined with production (=*prosumers*)

What are Smart Grids

- **Smart** and **Grids**
- Enhanced (electricity, or gas/water/heating/cooling) power grids
- Intelligent **measurements, protection, control**
- **Cybersecurity** is a must (by design)

Purpose of Smart Grids

- Smart Grids should help to ensure
  - Secure reliable **transmission** and **distribution** of electricity
  - Integration of **renewables**
  - Changes in **consumption** patterns
  - **Decoupling**
  - **Globalization** ("regionalization"), international market and cooperation

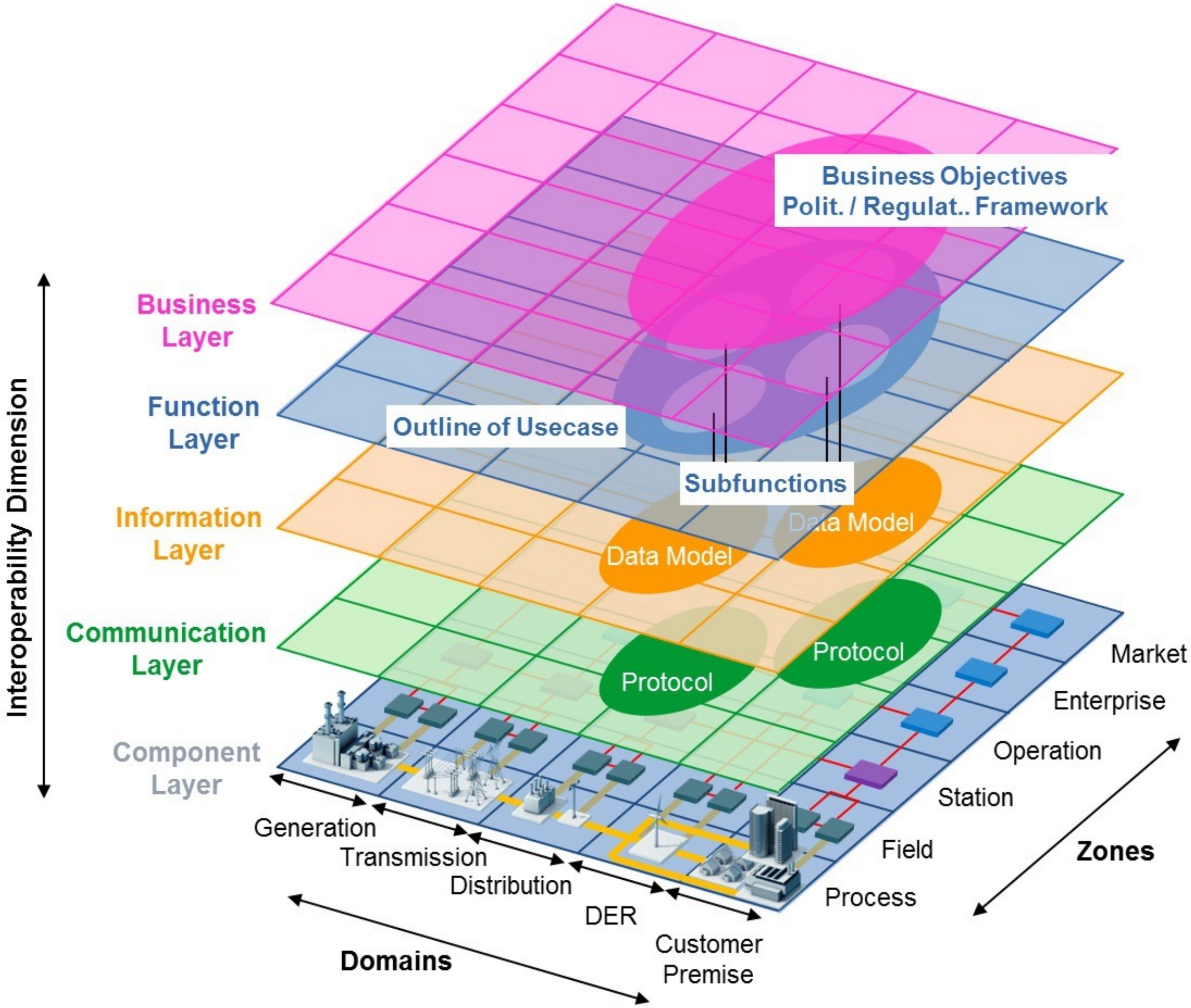
Electricity grid size

- **Centralized production** spots – large power stations
- **Transmission** EHV, HV grid – hundreds or thousands km lines
- **Distribution** HV, MV grid – tens or hundreds km lines
- **Low voltage** MV or LV grid – km or tens of km lines

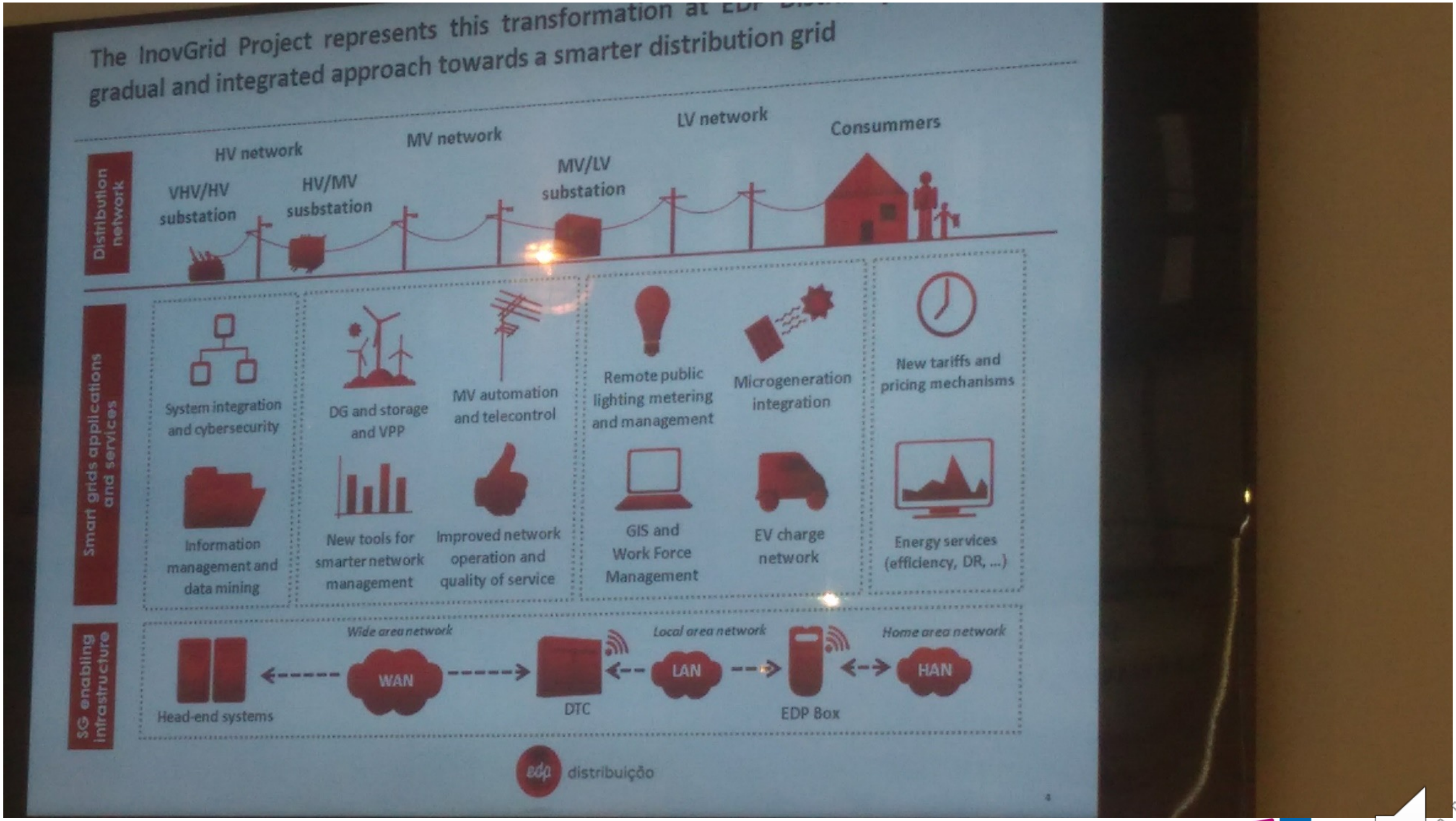
Future electricity grid – Smart Grid

- Why we need the electricity grid to be smart?
- Electricity production of now and future:
- **Sustainable production** – renewables (wind, solar, bio)
- **Resilient grid** – reliable, secure, self-healing, island operation
- **Efficient consumption** – efficiency at smart homes
- **Intelligent monitoring and control** – quality and reliability of service, shorter outages, fast and cost-efective response
- **Distributed production** – small and spread

Smart Grid Architecture Model (EU)



Smart grid architecture

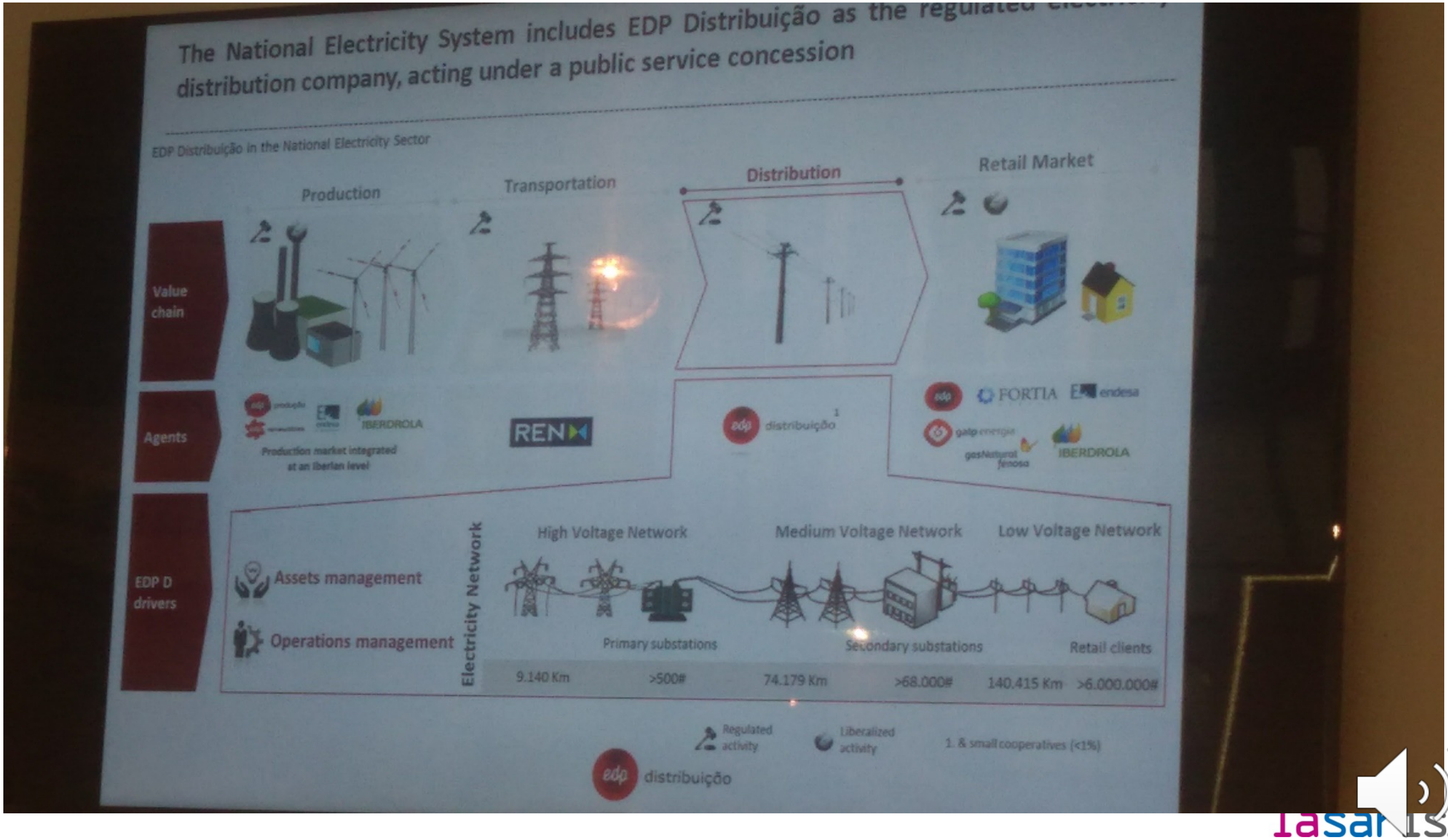


The InovGrid Project represents this transformation at EDP
gradual and integrated approach towards a smarter distribution grid

Distribution network
HV network
MV network
LV network
Consummers
VHV/HV substation
HV/MV susbstation
MV/LV substation
Smart grids applications and services
System integration and cybersecurity
DG and storage and VPP
MV automation and telecontrol
Remote public lighting metering and management
Microgeneration integration
New tariffs and pricing mechanisms
Information management and data mining
New tools for smarter network management
Improved network operation and quality of service
GIS and Work Force Management
EV charge network
Energy services (efficiency, DR, ...)
SG enabling infrastructure
Wide area network
Local area network
Home area network
Head-end systems
WAN
DTC
LAN
EDP Box
HAN
edp distribuição

Source: Energias de Portugal, Hub Session on Grid Intelligence, EUW 2017

Smart grid architecture



The National Electricity System includes EDP Distribuição as the regulated electricity distribution company, acting under a public service concession

EDP Distribuição in the National Electricity Sector

1. & small cooperatives (<1%)

edp distribuição

Smart grids functions

- Levels of view:
  - **Business**
  - **Technical**

  - **Grid operation control**
  - **Monitoring**
  - **Measurements** (billing, QoS, regulatory indicators)

Smart grids architectures

- Comumunication technology entities
  - **Head-end-system** (HES)
  - **Remote Terminal Units** (RTU), **Data Concentrators** (DCU)/**Gateways** (GW)
  - **Smart meters**, remote-controlled **switchgears**, **disconnectors**, various **sensors** and **probes**
  - IT and OT network active elements: **switches, modems, repeaters**
  - Physical **comumunication lines**
  - **Wireless** connections, **external** infrastructure

Risks in smart grids

- Risk conditions that may lead to **malfunctioning** and/or **damage**
- **Operational risks** – operational parameters out of defined normal limits (overvoltage, undervoltage, overcurrent, frequency fluctuations, high reactive power, higher harmonic frequencies…) caused by external factors – consumers, producers, natural conditions
- **Physical risks** – risks related to physical world
  - Physical intrusion and/or damage
- **Cyber risks** – risks related to operation of the „smart" part – IT and OT

SCADA

Supervisory Control And Data Acquisition

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

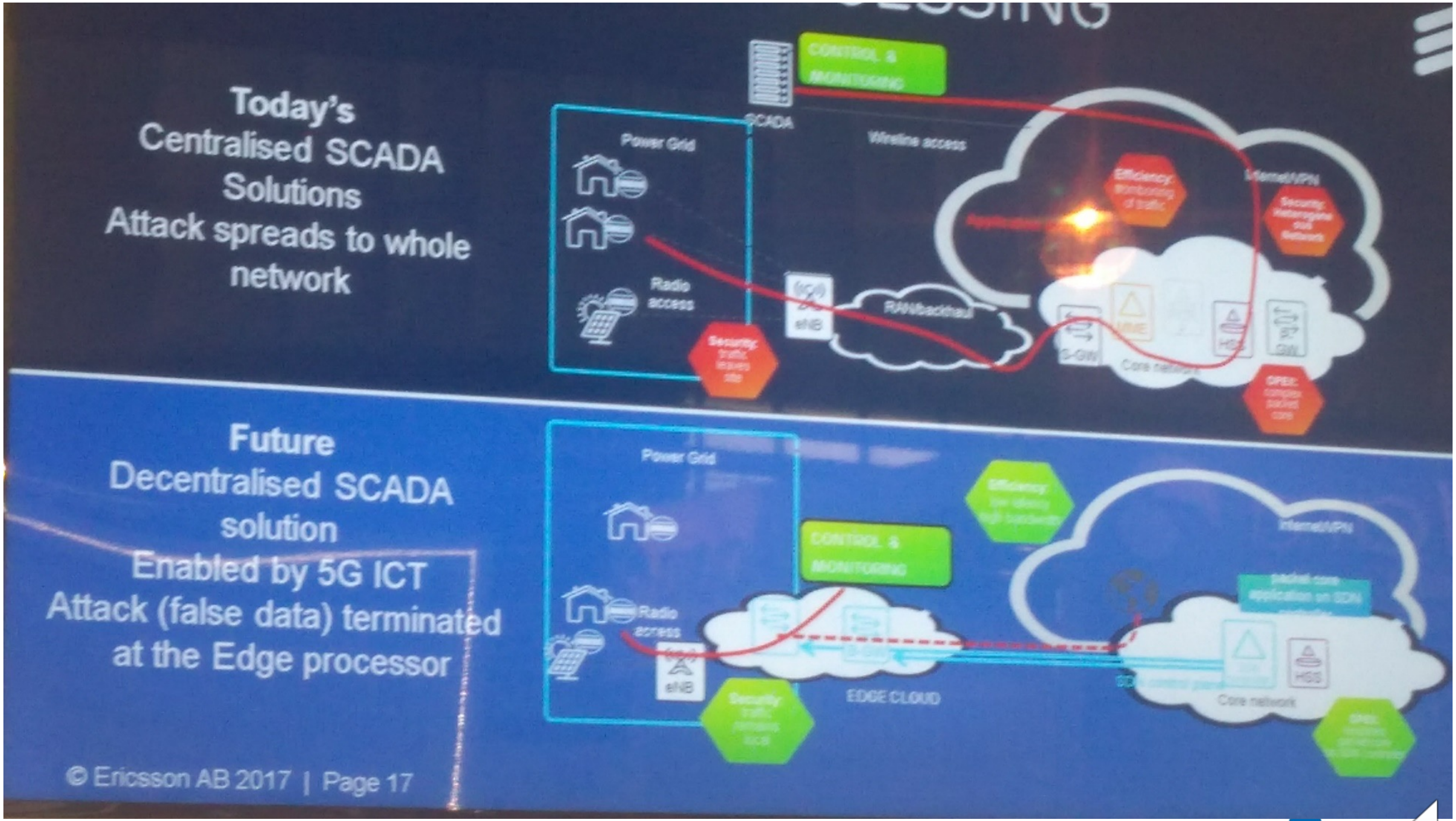
FACULTY OF INFORMATICS
MASARYK UNIVERSITY

lasaris

SCADA security

- What is **SCADA**
- Role in **Smart grids**
- **Operational technology** security vs **Information technology** security

SCADA



Today's
Centralised SCADA
Solutions
Attack spreads to whole
network

Future
Decentralised SCADA
solution
Enabled by 5G ICT
Attack (false data) terminated
at the Edge processor

© Ericsson AB 2017 | Page 17

Source: Ericsson AB, Hub Session on Grid Intelligence, EUW 2017

Industrial Control Systems / SCADA are vulnerable

ICS in the past

- **Isolated** from IT
- **Proprietary** protocols
- **Special** hardware
- **Proprietary** embedded OS
- **Physical** wiring

ICS now

- **Bridged** to IT
- **Internet** protocols
- **General** purpose HW
- **Mainstream** OS
- + fiber and wireless

SCADA is vulnerable

- PLCs, RTUs are low-performance computers controlling physical components, e.g. **valves, pumps, motors**
- Though the use of proprietary protocols, attacks can be used:
  - Lack of **authentication**
  - No **encryption**
  - **Backdoors**
  - **Buffer** overflow
  - … Tailored attacks

OT or IT?

- Trend: Operational and Information Technology are merging
- Traditionally *Operational Technology*:
  - **Functionality** has priority
  - **Proprietary** protocols, interfaces
  - **Not connected** to outside internet
  - **Availability** is most important
  - Few data, **confidentiality no issue**

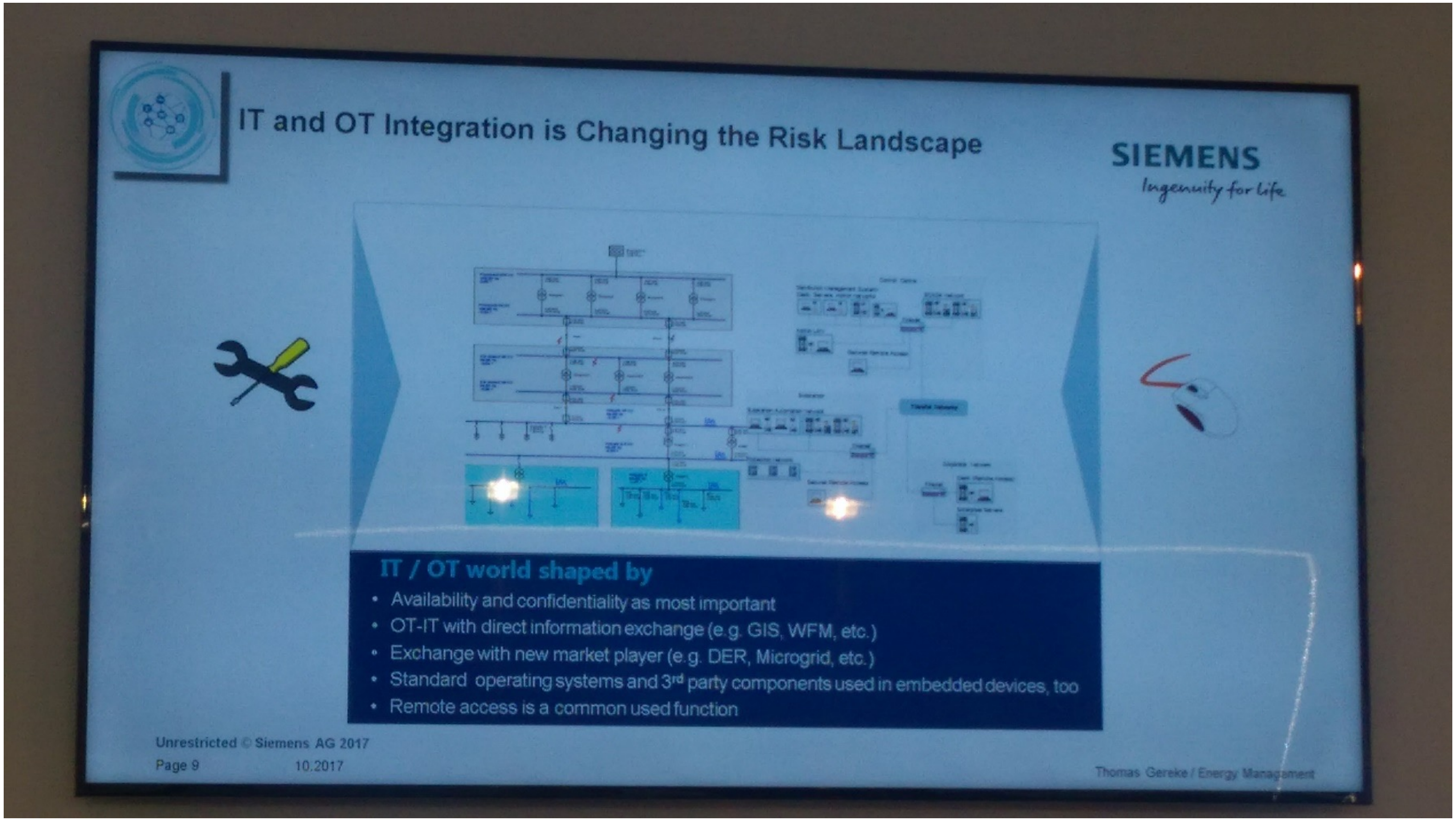
Source: Siemens AG, Hub Session on Grid Intelligence, EUW 2017

OT or IT?

- Now more *Information Technology*:
  - **Standard OSs**, interfaces
  - **Communicating with/via internet**
  - Most **data confidential**
  - **Availability** not so relevant

Source: Siemens AG, Hub Session on Grid Intelligence, EUW 2017

OT vs IT security



IT and OT Integration is Changing the Risk Landscape

SIEMENS
Ingenuity for life

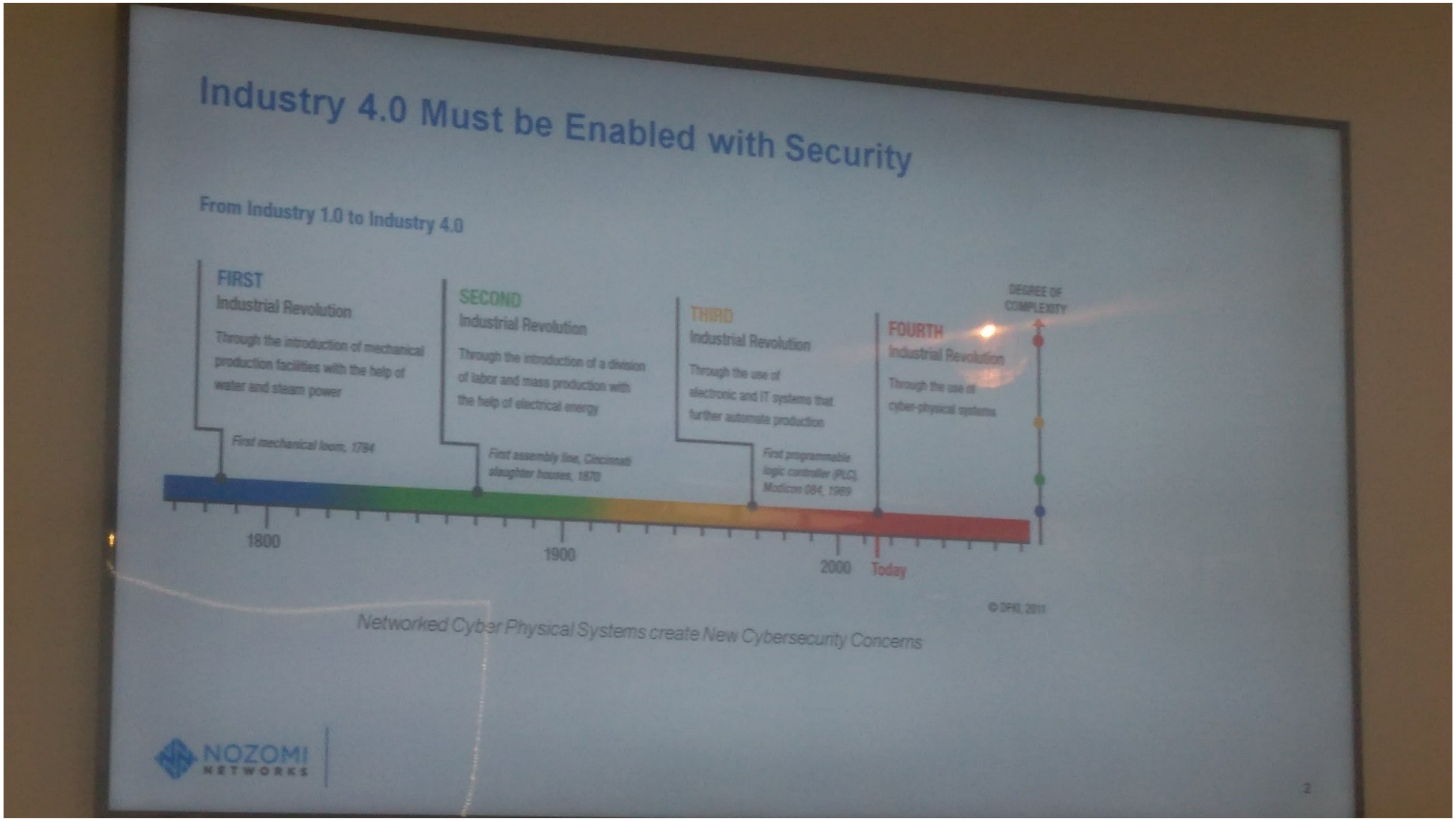
IT / OT world shaped by

- Availability and confidentiality as most important
- OT-IT with direct information exchange (e.g. GIS, WFM, etc.)
- Exchange with new market player (e.g. DER, Microgrid, etc.)
- Standard operating systems and 3rd party components used in embedded devices, too
- Remote access is a common used function

Unrestricted © Siemens AG 2017
Page 9 10.2017

Thomas Gereke / Energy Management

Industry 4.0 security



Industry 4.0 Must be Enabled with Security

From Industry 1.0 to Industry 4.0

FIRST
Industrial Revolution
Through the introduction of mechanical production facilities with the help of water and steam power

First mechanical loom, 1784

SECOND
Industrial Revolution
Through the introduction of a division of labor and mass production with the help of electrical energy

First assembly line, Cincinnati slaughter houses, 1870

THIRD
Industrial Revolution
Through the use of electronic and IT systems that further automate production

First programmable logic controller (PLC), Modicon 084, 1969

FOURTH
Industrial Revolution
Through the use of cyber-physical systems

Networked Cyber Physical Systems create New Cybersecurity Concerns

Source: Nozomi Networks, Hub Session on Grid Intelligence, EUW 2017

Business point of view

- Also non-technical factors/conditions
- **Business continuity**
- Customer p.o.v., **privacy, reputation**

Master Business Continuity

- Define Master Business Continuity early
- Depends on:
  - How **large** is the infrastructure?
  - How to determine **critical incidents** => emergency?
  - Is **manual grid** operation realistic? How long/extend?
  - Do we **depend on SCADA**?

Data protection pro- or contra- consumer?

- User (consumer) has **no detailed info**
- Has very general or non-applicable info from media
- Must be reassured:
  - **Secure** (private) data transmission
  - **Certified** independently
  - Respect for **regulation**
- Not complicated
  - No details needed, **No access restrictions**

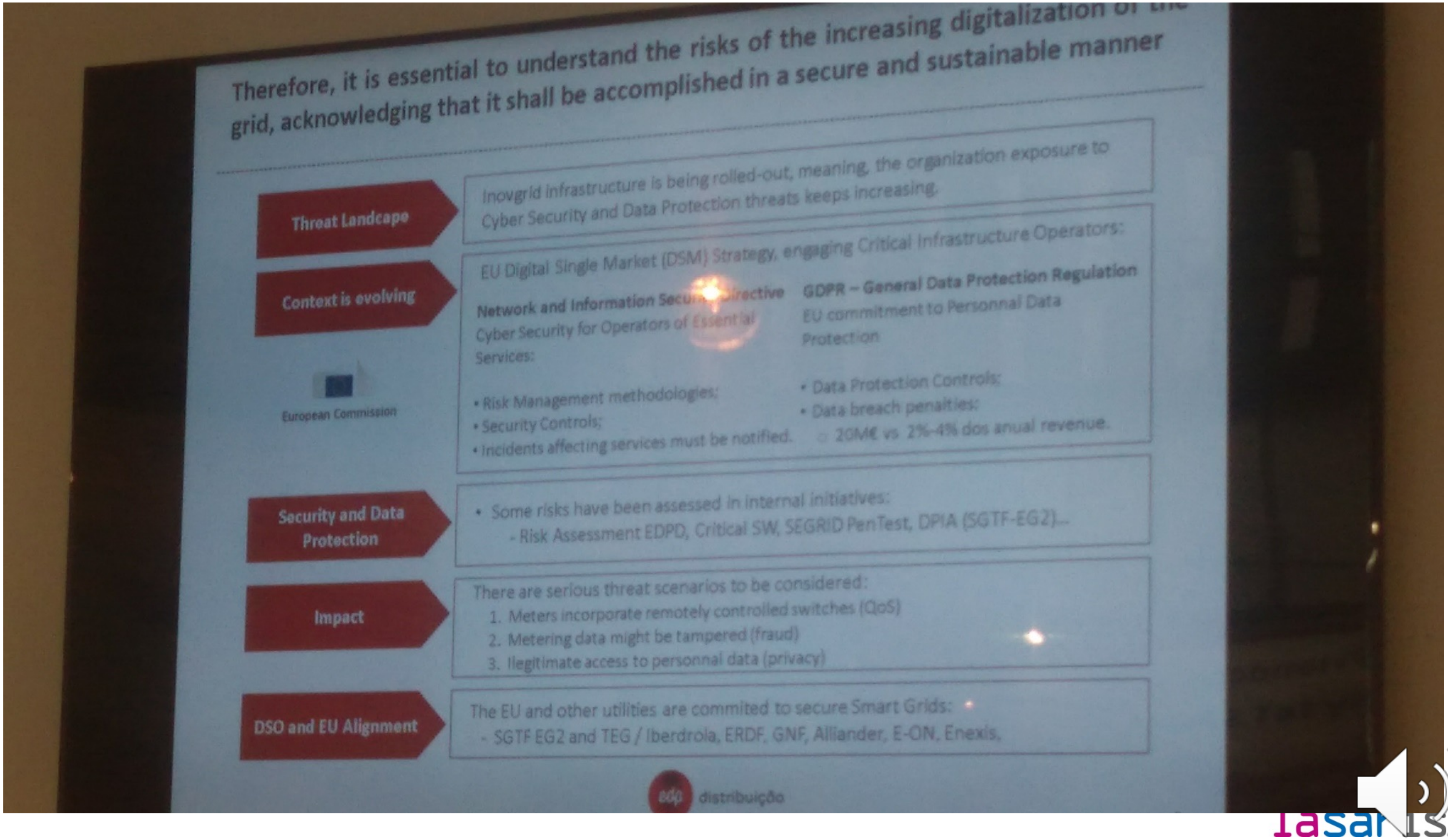
Security and Privacy

- Strict legal and business conditions for both
- May or may not be in contradiction
- Integrated approach needed
- Now with GDPR in mind
- **General Data Protection Regulation** (GDPR) (Regulation (EU) 2016/679)

Need for advanced ISMS

- **Information Security Management System**
- Integrated security, privacy
- No isolated solutions
- Connected responsibility
- Data protection is legal requirement - **GDPR**
- **ISO/IEC AWI 27552** extension to ISO 27001
  - ensure good governance around data protection and that it gets anchored at board level
  - changes reflect the need to align with ISO standard + existing standard with the GDPR

Context, GDPR, Security



Therefore, it is essential to understand the risks of the increasing digitalization of the grid, acknowledging that it shall be accomplished in a secure and sustainable manner

Threat Landcape

Inovgrid infrastructure is being rolled-out, meaning, the organization exposure to Cyber Security and Data Protection threats keeps increasing.

Context is evolving

EU Digital Single Market (DSM) Strategy, engaging Critical Infrastructure Operators:

Network and Information Security Directive
Cyber Security for Operators of Essential Services:

- Risk Management methodologies;
- Security Controls;
- Incidents affecting services must be notified.

GDPR – General Data Protection Regulation
EU commitment to Personnal Data Protection

- Data Protection Controls;
- Data breach penalties:
  - 20M€ vs 2%-4% dos anual revenue.

European Commission

Security and Data Protection

- Some risks have been assessed in internal initiatives:
  - Risk Assessment EDPD, Critical SW, SEGRID PenTest, DPIA (SGTF-EG2)...

Impact

There are serious threat scenarios to be considered:

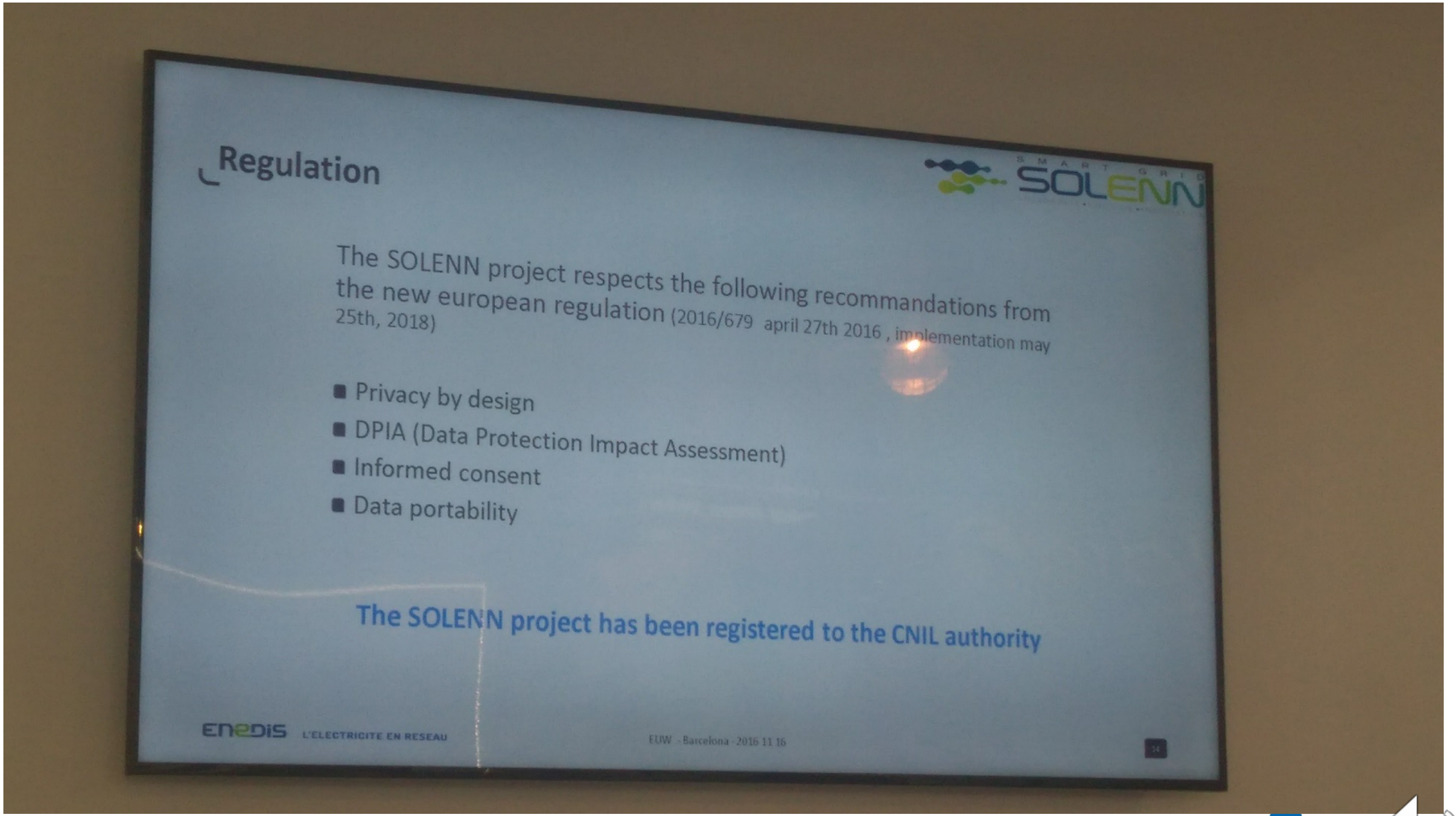
1. Meters incorporate remotely controlled switches (QoS)
2. Metering data might be tampered (fraud)
3. Ilegitimate access to personnal data (privacy)

DSO and EU Alignment

The EU and other utilities are commited to secure Smart Grids:
- SGTF EG2 and TEG / Iberdrola, ERDF, GNF, Alliander, E-ON, Enexis,

edp distribuição

GDPR



Regulation

SMART GRID SOLENN

The SOLENN project respects the following recommandations from the new european regulation (2016/679 april 27th 2016 , implementation may 25th, 2018)

- Privacy by design
- DPIA (Data Protection Impact Assessment)
- Informed consent
- Data portability

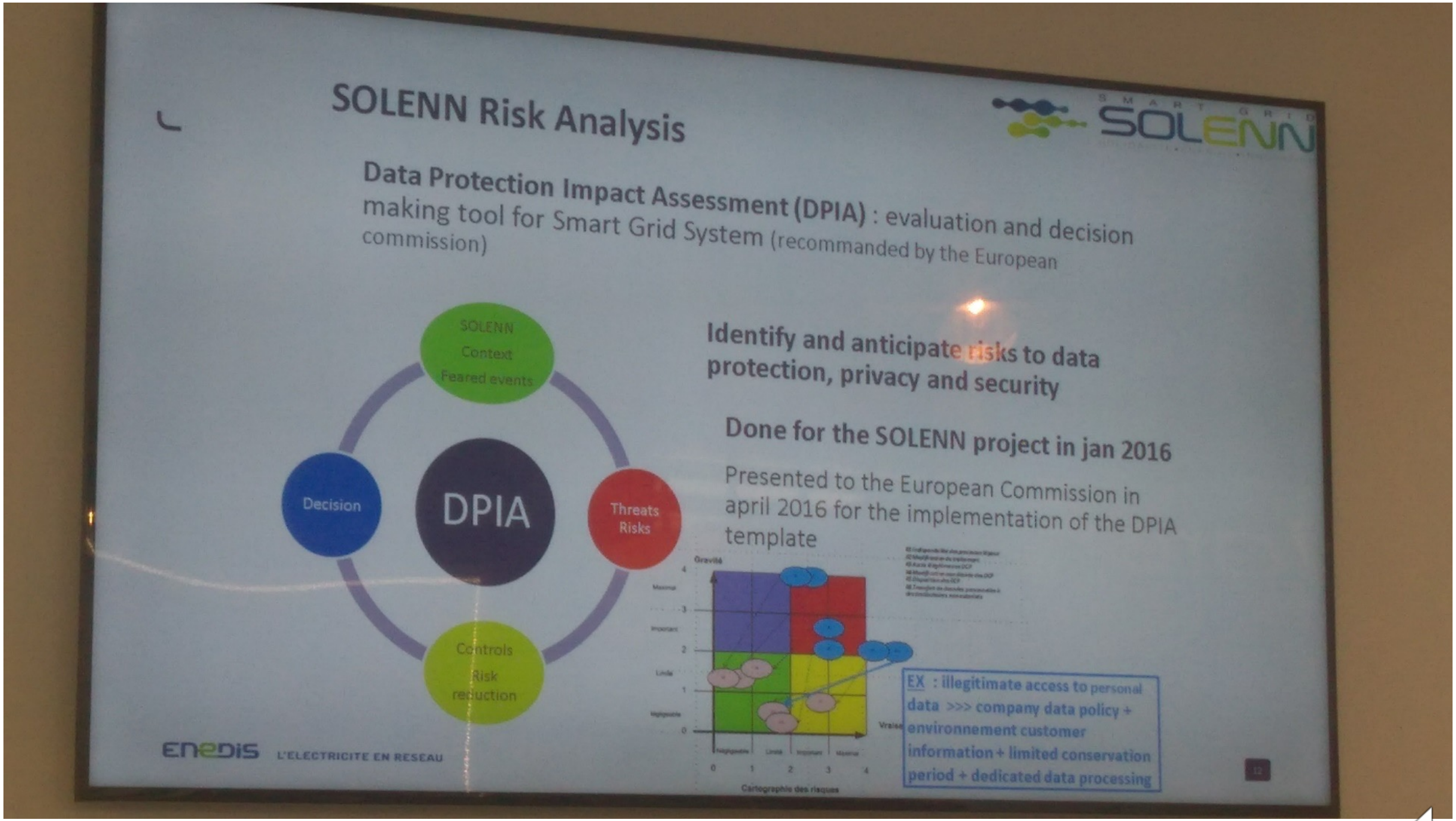
The SOLENN project has been registered to the CNIL authority

ENEDIS L'ELECTRICITE EN RESEAU

EUW - Barcelona - 2016 11 16

14

DPIA



SOLENN Risk Analysis

SMART GRID SOLENN

Data Protection Impact Assessment (DPIA) : evaluation and decision making tool for Smart Grid System (recommanded by the European commission)

Identify and anticipate risks to data protection, privacy and security

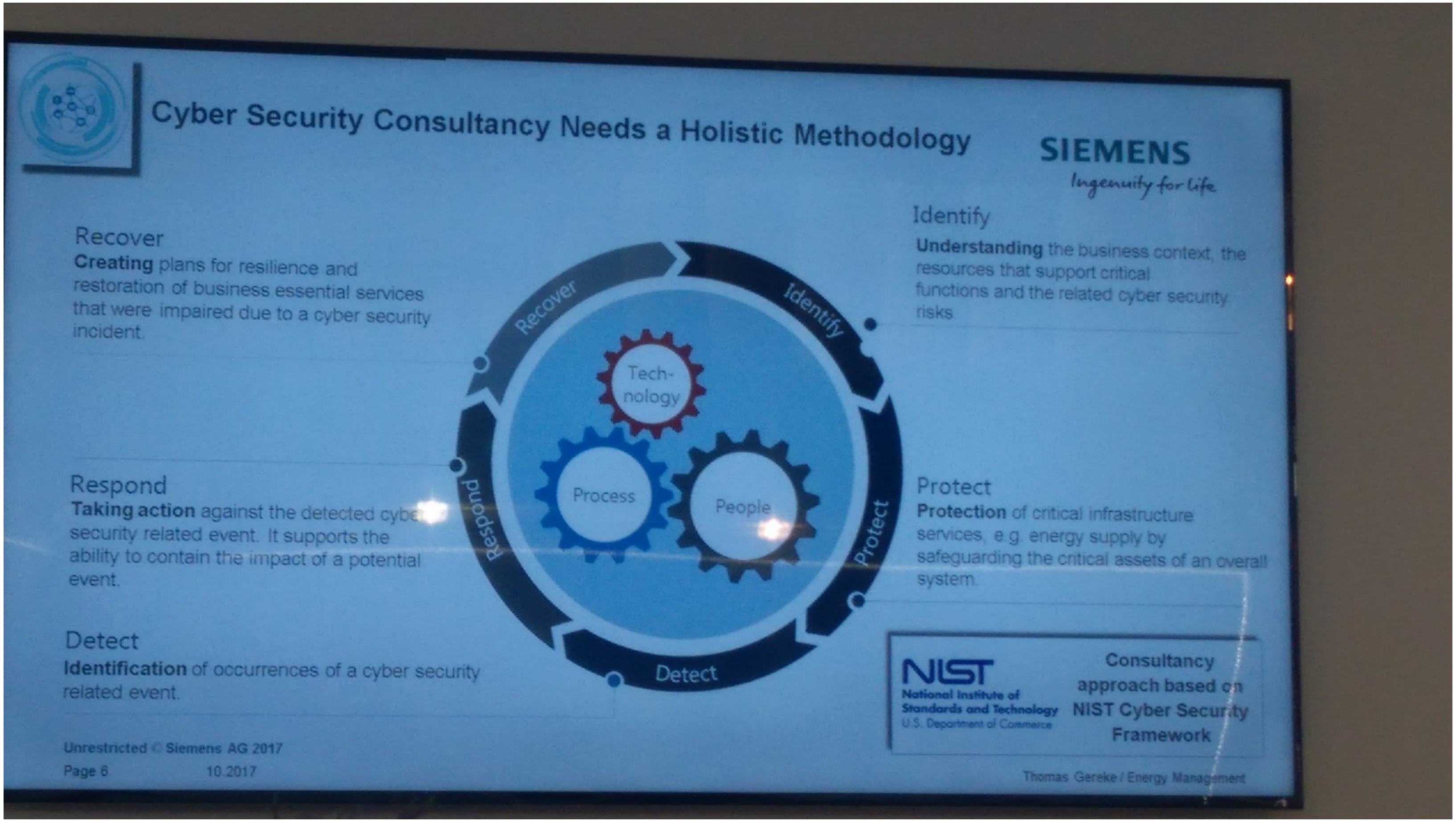
Done for the SOLENN project in jan 2016

Presented to the European Commission in april 2016 for the implementation of the DPIA template

EX : illegitimate access to personal data >>> company data policy + environnement customer information + limited conservation period + dedicated data processing

ENEDIS L'ELECTRICITE EN RESEAU

Holistic approach



Cyber Security Consultancy Needs a Holistic Methodology

SIEMENS
Ingenuity for life

Recover
Creating plans for resilience and restoration of business essential services that were impaired due to a cyber security incident.

Respond
Taking action against the detected cyber security related event. It supports the ability to contain the impact of a potential event.

Detect
Identification of occurrences of a cyber security related event.

Identify
Understanding the business context, the resources that support critical functions and the related cyber security risks.

Protect
Protection of critical infrastructure services, e.g. energy supply by safeguarding the critical assets of an overall system.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Consultancy approach based on NIST Cyber Security Framework

Unrestricted © Siemens AG 2017
Page 6 10.2017

Thomas Gereke / Energy Management

SUMMARY

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY

lasaris

Summary

- We have discussed the notion of Critical Infrastructure and its 21st century extension – Critical Information Infrastructure

- Apart from protecting the CII physically, the protection of its Cyberspace is the main focus

- Cybersecurity can be seen as an extension of infosec
  - The peculiarities of Cyberspace must be considered

Course Reading – Week 3

- Julia E. Sullivan, Dmitriy Kamensky: **How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid, The Electricity Journal**, Volume 30, Issue 3, 2017, Pages 30-35, ISSN 1040-6190, (http://www.sciencedirect.com/science/article/pii/S1040619017300507)

- **TeleBots are back: Supply-chain attacks against Ukraine**, available from https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/
- **KillDisk now targeting Linux: Demands $250K ransom, but can't decrypt,** available from https://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/

Literature

- UK NCSC: *New Cyber Attack categorisation system to improve UK response to incidents* (2018)
- Ottis, Rain. *Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective.* Proceedings of the 7th European Conference on Information Warfare. (2008).
- Bronk, Chris and Tikk-Ringas, Eneken, *Hack or Attack? Shamoon and the Evolution of Cyber Conflict* (2013). Available at SSRN: http://ssrn.com/abstract=2270860
- CZ.NIC a CSIRT.CZ, *Rekapitulace (D)DOS útoků ze dnů 4. 3. – 7. 3.* (2013). Available at: https://www.csirt.cz/files/csirt/Rekapitulace-utoky-20120311.pdf