Cybersecurity Institute
Univ. Grenoble Alpes

Cybersecurity of industrial systems. General Introduction and motivation

Stéphane Mocanu,

Laboratoire d'Informatique de Grenoble/INRIA

CTRL-A

stephane.mocanu@inria.fr

LIG

Inria
INVENTEURS DU MONDE NUMÉRIQUE

Industrial Control systems (SCADA)

Cyberphysical Systems

IT

Remote connections

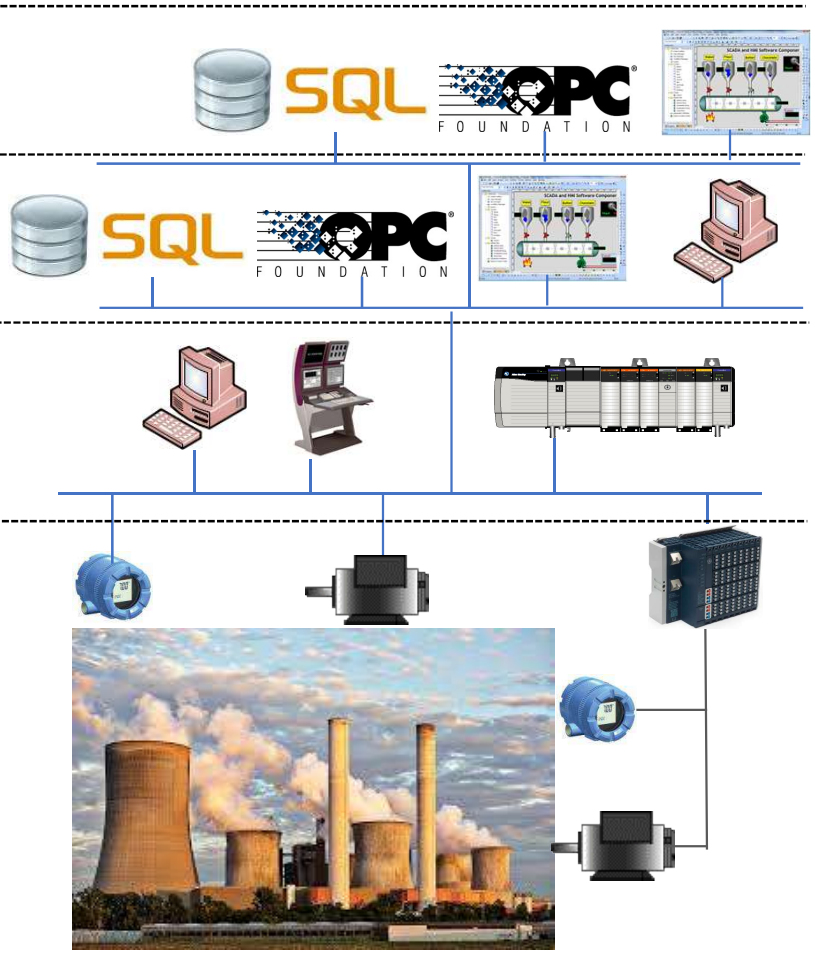
Supervisory and journaling
No real-time

OT
Operational Technology

Controllers
Soft real-time communication

Intelligent sensors and actuators
Hard real time communication

Main asset : the physique plant



SOME DEFINITIONS AND FACTS

- **Cybersecurity triad revisited**
  - **Availability is paramount (keep running under attack)**
  - **Non-repudiation may be crucial (emergency stop)**
  - **Real-time properties are important**
  - **Reaction time to attacks is very short**
- **Attacks targets the physical process**
  - **Stuxnet, BlackEnergy, Industroyer, ….**
- **Behavioral classification**
  - **Event-based : sequential systems (aka Manufacturing) PLC controlled**
    - All manufacturing systems
  - **Time-based : continuous systems (aka Process)**
    - Feedback control based processes
    - Electrical transport and distribution (hybrid)

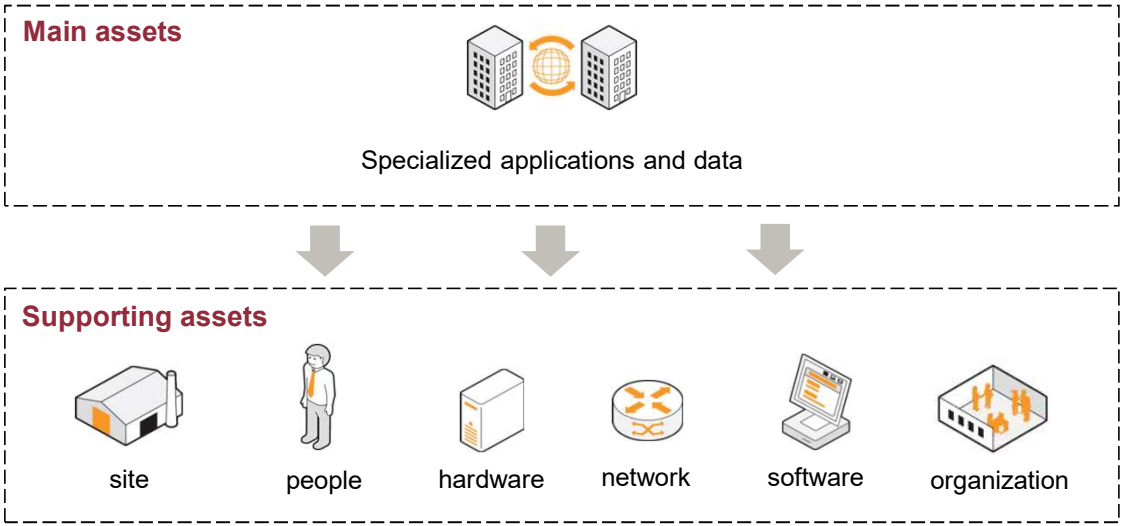
Basic definitions

- **Information System (I.S.)**
  - The set of resources used **to collect, class, stock, manage, disseminate informations** ain a corprate or state organisation
  - Keyword: information, is the main asset for corporations, organizations, public administrations, etc

I.S. is intended to allow and facilitate organisation activity

Basic definitions

- **An organsation I.S. will incluse several sets of assets**



ISO/IEC 27005:2008

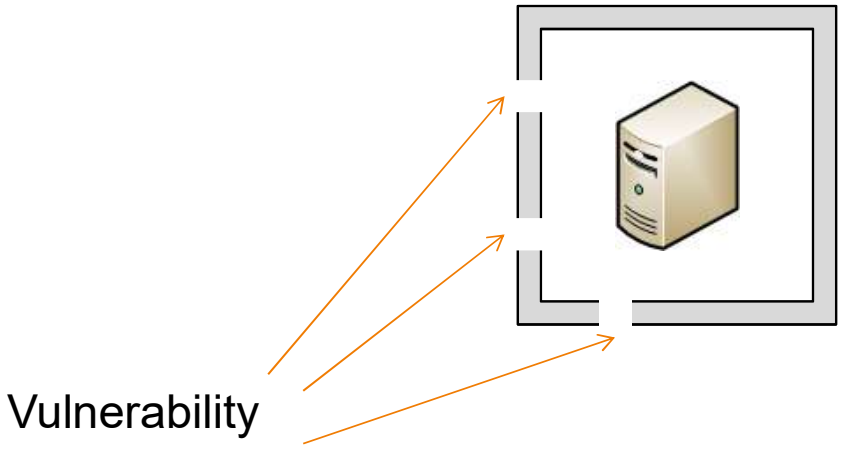
Insuring I.S. security means to insure the security of all these assets

Basic definitions

- **Security aims to reduce information systems risks, in order to limit theirs effects on the organizations activities**
- **Security management is not intended to be obstructionist. On the contrary :**
  - ► Security is intended to provide users the expected quality of service
  - ► Security must guarantee the adequate protection level to the users

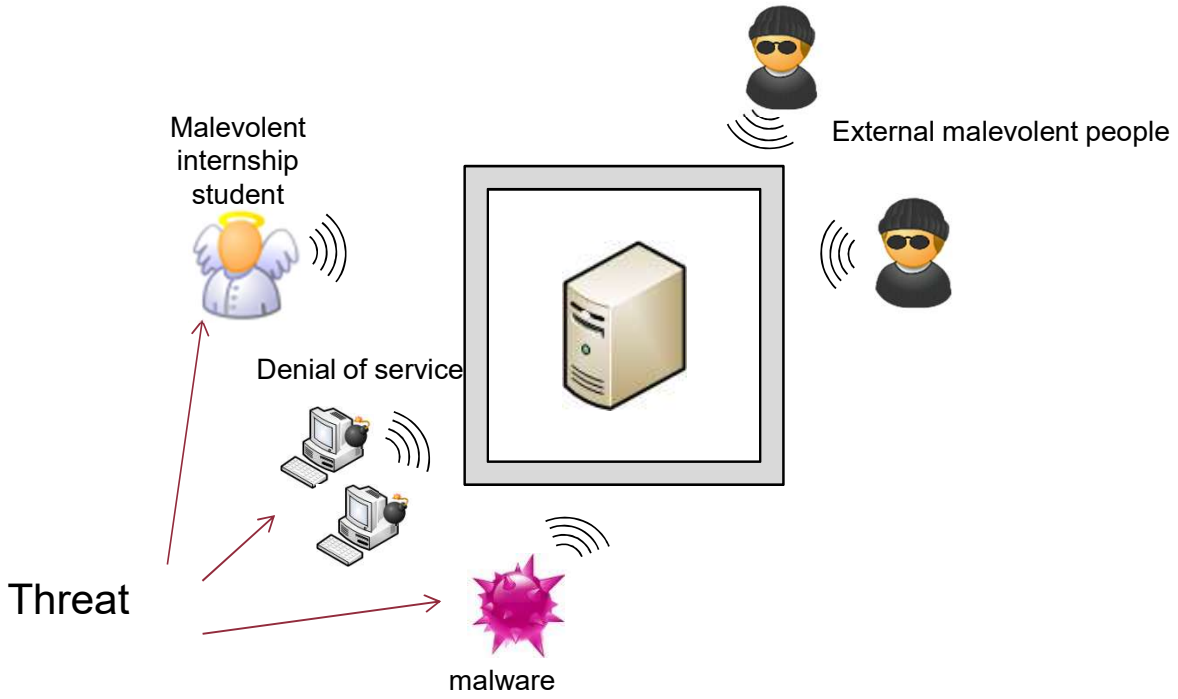
Vulnerability

- **Asset weakness (at design level or manufacturing level, instalation, configuration or use)**



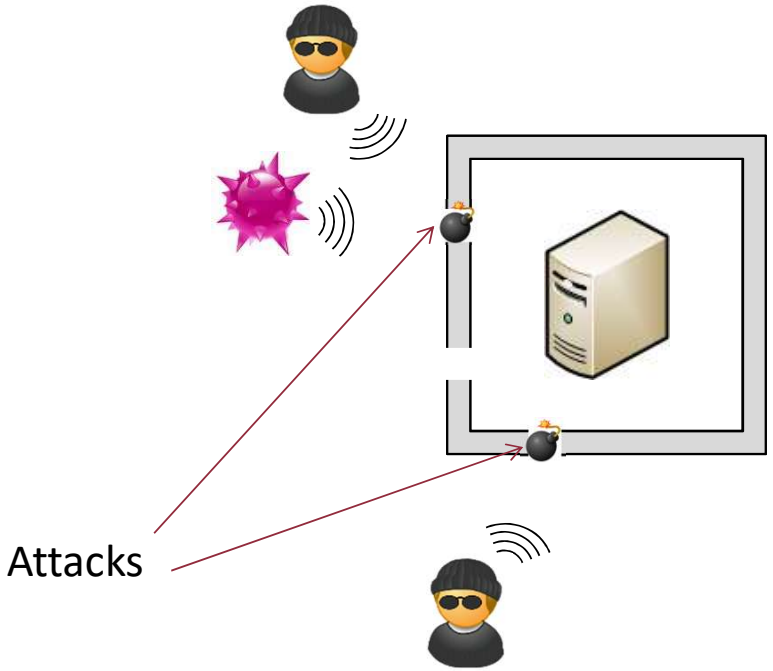
Threat

- A ***possible*** incident source, **that might damage an asset if the threat becomes effective.**



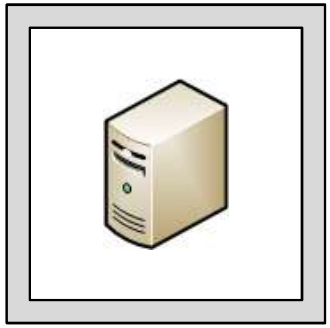
Attack

- **Malicious action intended to violate asset security. An attack is the threat concretization, and needs a vulnerability exploitation.**



Intrusion

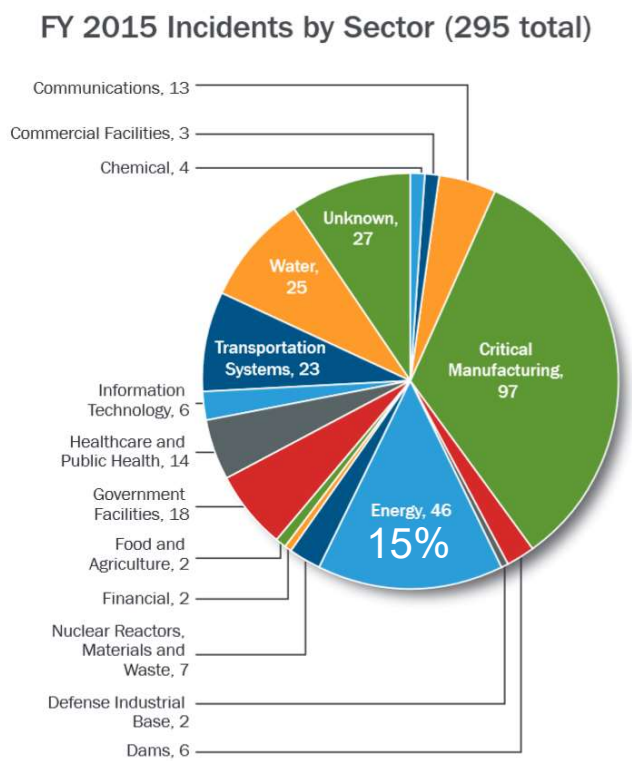
An attack can succeed if and only if there is an explotable vulnerability affecting the asset.

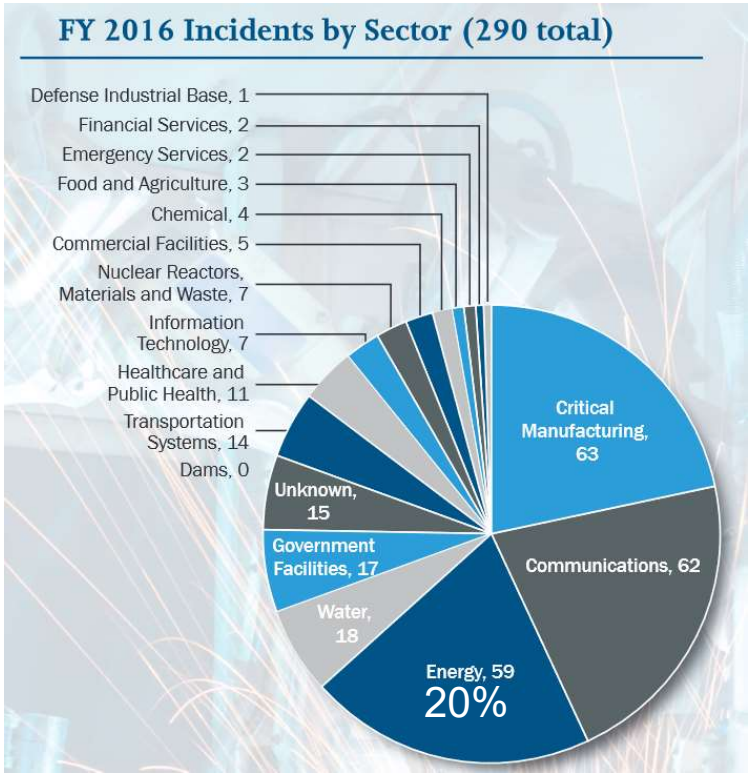


The cybersecurity process aims to ensure that no exploitable vulnerability exists on the asset.

In real life the objective is to control and confine vulnerabilities as the 0 vulnerabilities target is unreachable.

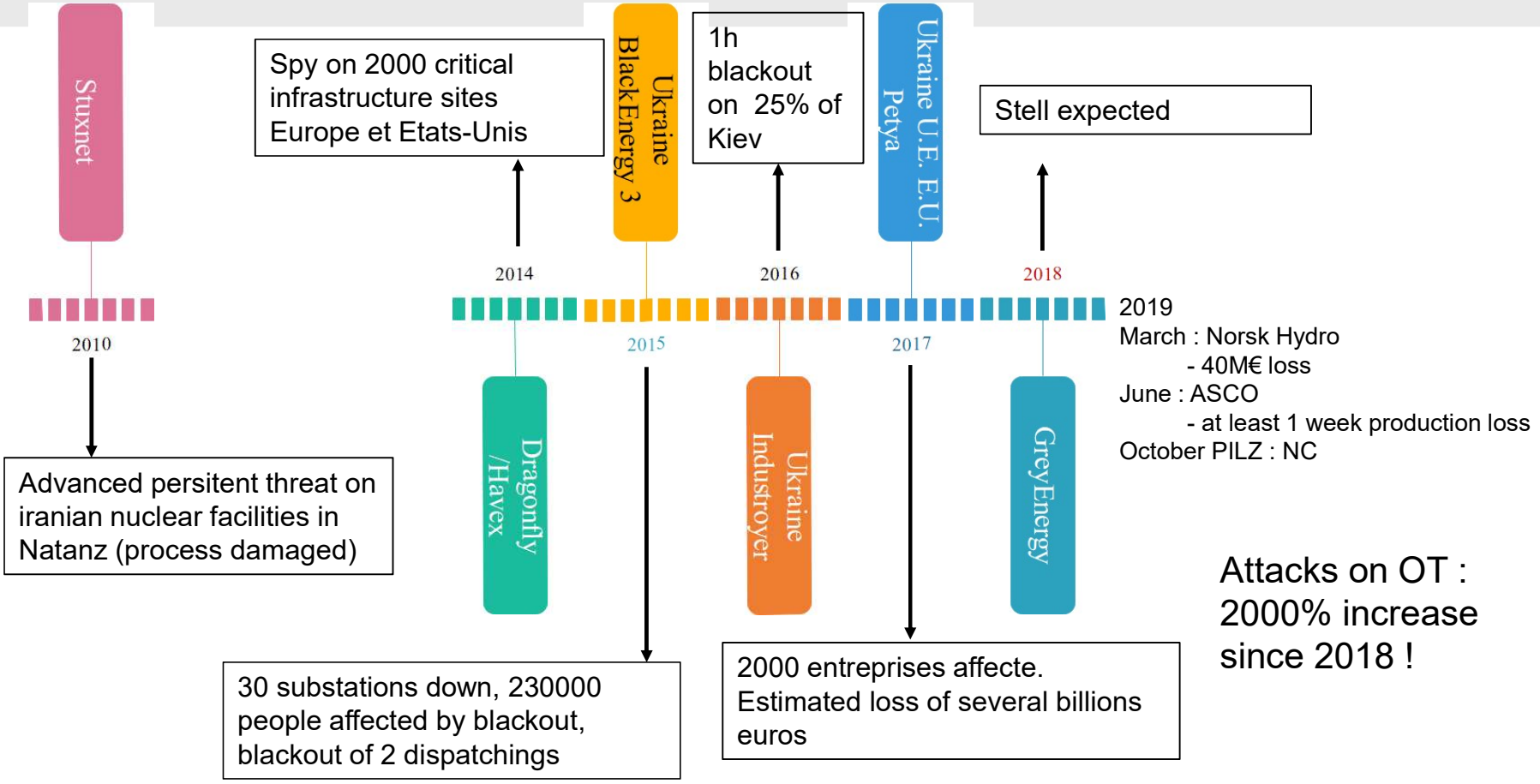
IS ENERGY AT (CYBER)RISK ?





Sources: ICS-CERT https://ics-cert.us-cert.gov/

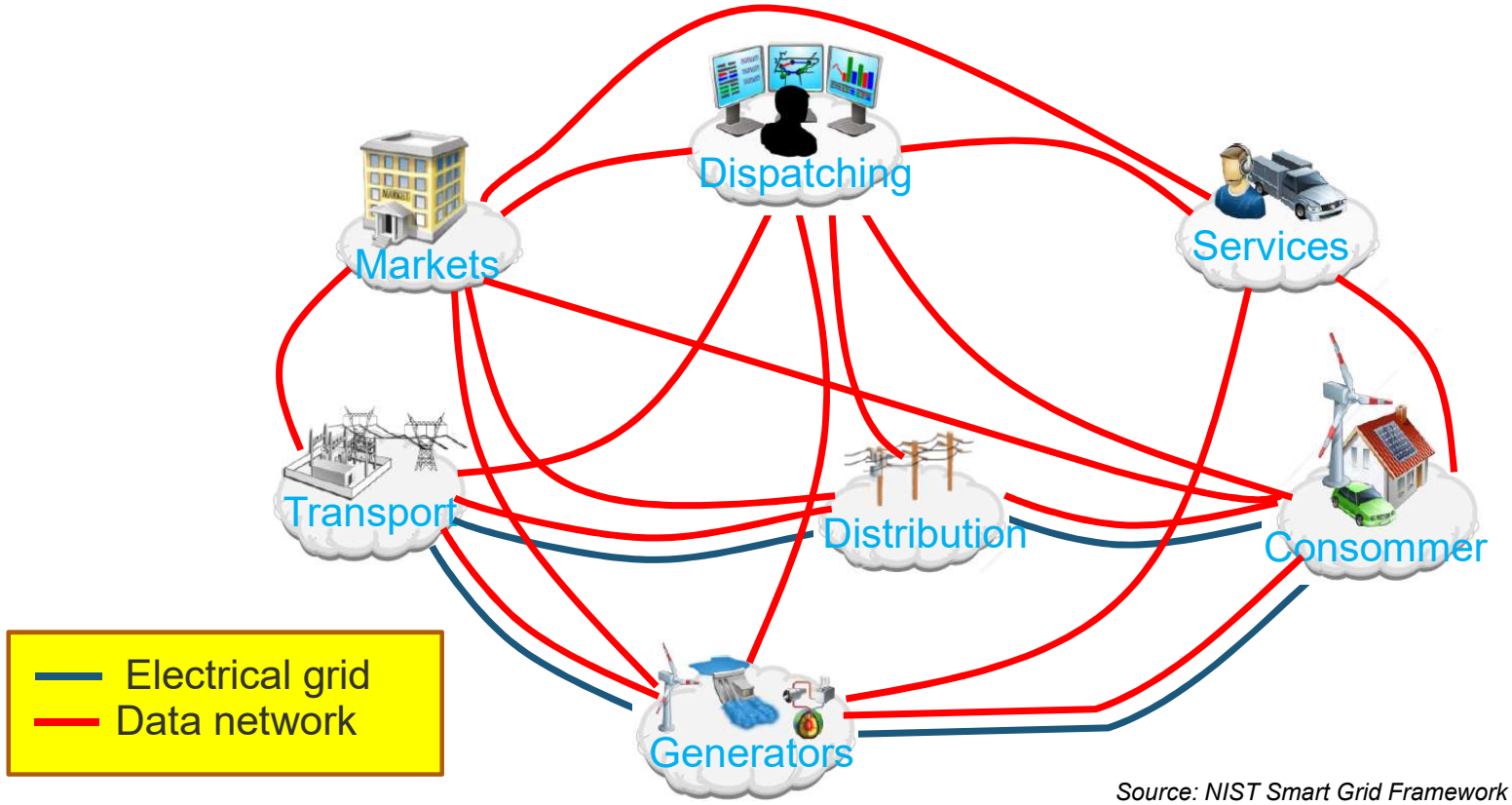
IS IT IMPORTANT ?



Attacks on OT : 2000% increase since 2018 !

WHY IS THE ELECTRICAL GRID EXPOSED

A « dual » networks : electrical and data



Source: NIST Smart Grid Framework 3.0

THREATS 2019

- **Primary attacks (Source BSI-CS005E Top 10 Threats and Countermeasures 2019)**

Top 10 Threats	Trend since 2016
Infiltration of Malware via Removable Media and External Hardware	↗
Malware Infection via Internet and Intranet	↗
Human Error and Sabotage	↑
Compromising of Extranet and Cloud Components	↑
Social Engineering and Phishing	↘
(D)Dos Attacks	↑
Control Components Connected to the Internet	→
Intrusion via Remote Access	→
Technical Malfunctions and Force Majeure	↘
Compromising of Smartphones in the Production Environment	→

- **Secondary attacks**
  - ► **Privilege escalation**
  - ► **Unauthorized access to internal systems**
  - ► **Manipulation of fieldbus communication**
  - ► **Manipulation of network components**

Important remark

Recent mediatic events are Big Game Hunting

- Norsk Hydro
- Southwire
- Altran
- CHU Rouen
- Bouygues Construction

60% RDP attacks

RAAS is today golden mine

Source ANSSI CERTFR-2020-CTI-001

BEYOND RANSOMWARE ATTACKS

- **Process oriented attacks**
  - Malicious controls sent to the process (actuators) using legal frames
  - Injection of false data sensors using legal frames
  - Exploitation of IT/OT and physical process vulnerabilities
- **Leads to**
  - Loss of view
  - Loss of control
  - Physical process damage
- **Proof of concept**
  - "Aurora vulnerability" (thunderbolt-like effect attack) – Idaho National Laboratory
    - Current spikes on the secondary circuit of a generator, faster that the protections relay timing
  - Stuxnet
  - Blackout 2003

U.S. BLACK

NERC
Node Breaker Model Representation

- 200

http://www.creos-net.lu/creos-luxembourg/infra

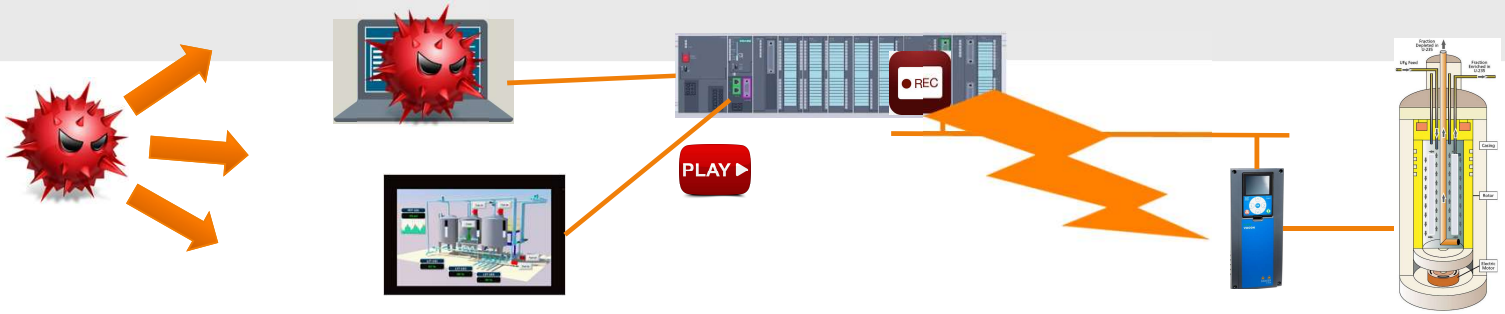
wikipedia

BLACKOUT 2003

- **Starting event : (accidental) false sensor data injection**
- **Exploits cyber et physical system vulnerabilities**
- **Loss of view (false supervisory view)**
- **Loss of control**
- **Physical system damage**
- **Human causalities (collateral)**

- **No protocol syntax or semantics violation**

STUXNET 2010



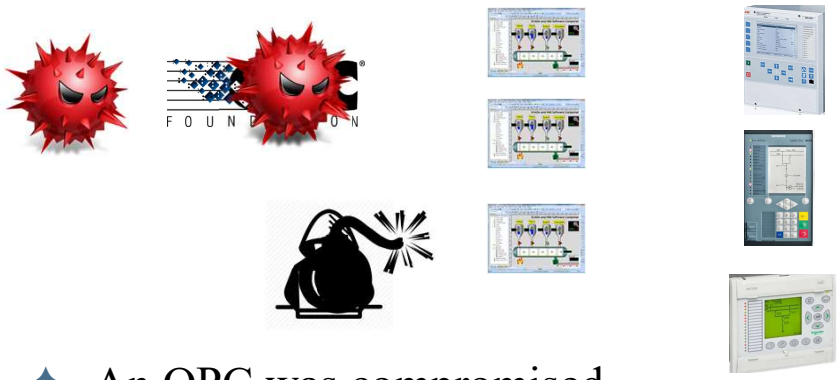
- Search fo Step 7 engineering computers
- Replacement of communication drivers
- Download malicious code to S7-300 PLC
- Search for speed controlers on Profibus
- Recording normal sensor values
- Execution of malicious code and replay the normal behavior to SCADA

STUXNET

- **Deep knowledge of the system (very detailed recognition on site))**
- **No protocol syntax or semantics violation**
- **Loss of view**
- **Loss of control**
- **Physical system damage**

INDUSTROYER/CRASHOVERRIDE

- **Electric grid**
  - **Known protection and automation functions**
  - **State and load distribution unknown**



- An OPC was compromised
- System cartography
- Backdoors open on HMIs
- Remote actions
- Malicious controls sent to protection relays

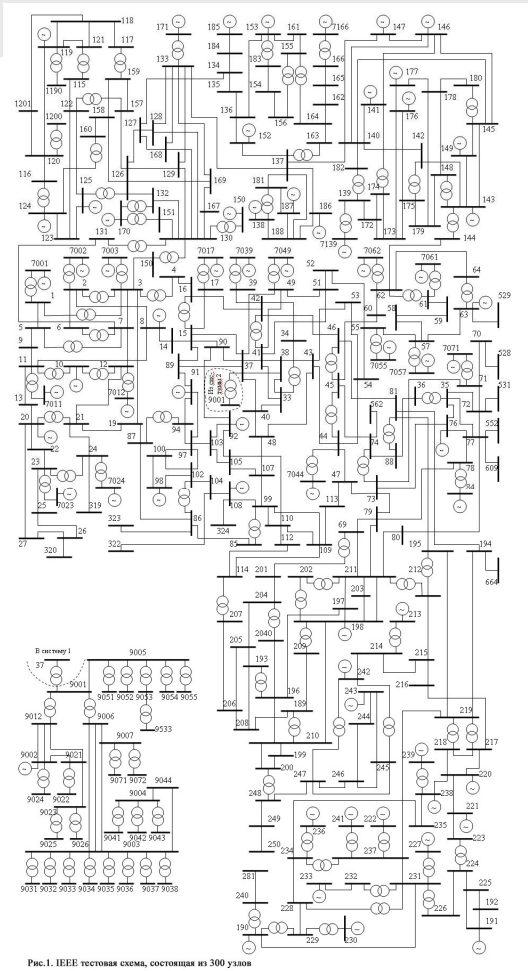


Рис.1. IEEE тестовая схема, состоящая из 300 узлов

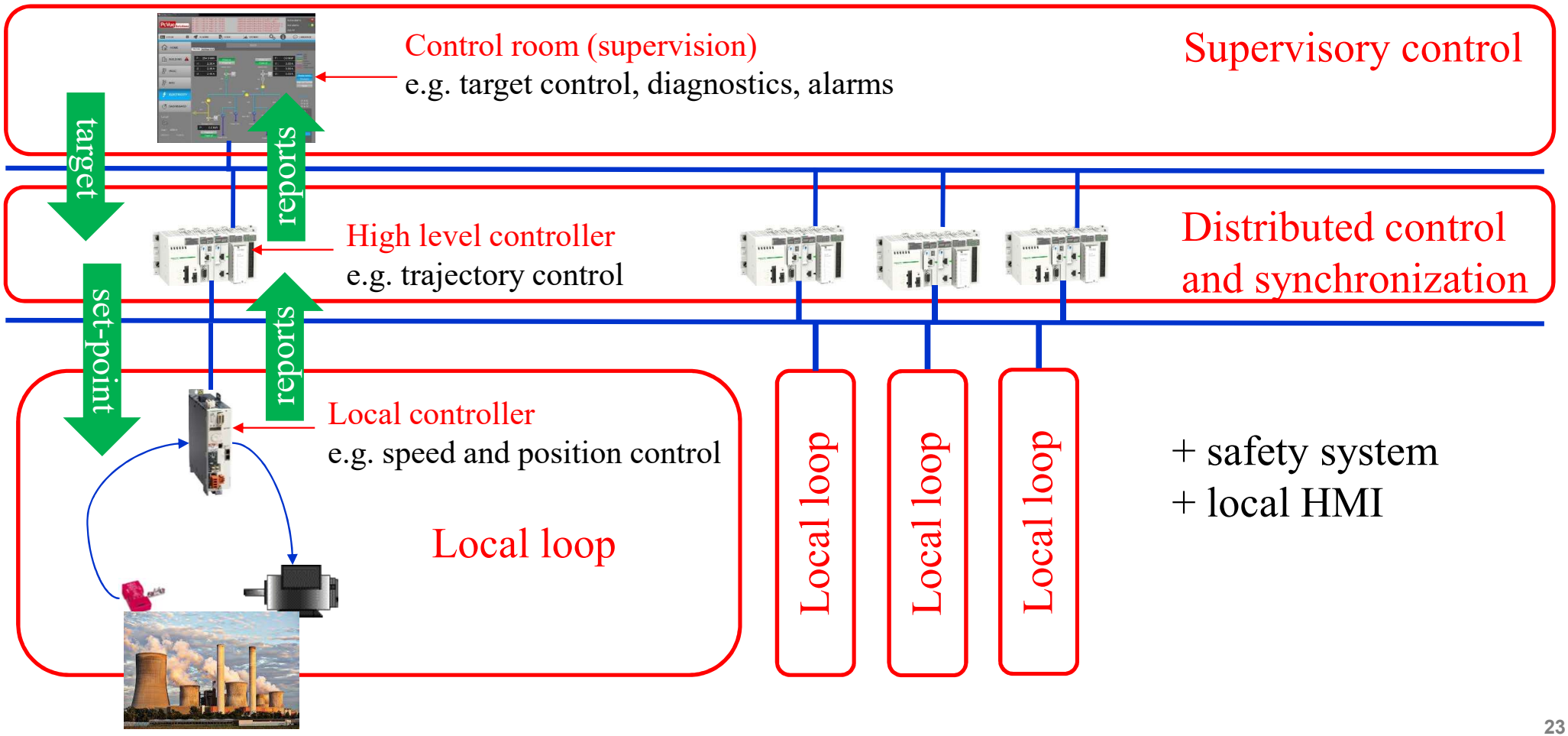
INDUSTROYER/CRASHOVERRIDE

- System recognition via an OPC server
- No protocol syntax or semantics violation
- Loss of view
- Loss of control
- Physical system damage

SCADA CYBERSECURITY AWARNESS

- **Basic**
  - Understand threat/vulnerability/attacks concepts
  - Understand risk and risk mitigation
  - Understand SCADA and industrial networks
  - Understand security objectives and controls
- **Advanced**
  - Be able to use the security controls of an industrial device
  - Understand data networks security controls
  - Be able to compare industrial security solutions
- **Expert**
  - Evaluate the security of a device/network/systems
  - Propose security system plan

THE SYSTEM APPROACH AND COMMUNICATION



SYSTEM APPROACH

- **Everything, including communication system is part of the control function**
  - ► Communication protocols are control oriented
- **There is strong interdependence between control elements**
  - ► Some control functions are distributed
- **Security deployment has to be global**
  - ► System oriented not global oriented
- **The final target of the control function is the physical process integrity**
  - ► Physical process model has to be taken into account