Cybersecurity at the time of “hyper-supply-chains” and gatekeepers

An insight in the power sector

Ing. Prof. Vittorio Trecordi
Communications Networks for Electricity Systems @ PoliMi

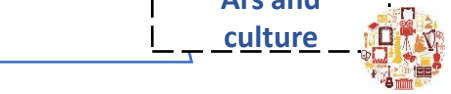
The challenge of hyper-supply-chains' security

ILLUSTRATIVE MODEL OF AN HYPER-SUPPLY-CHAIN

GATEKEEPERS

Data

Critical Assets | Know-how | ... | Financial Resources



Genius

Ars and culture

ILLUSTRATIVE MODEL OF A MODERN SUPPLY CHAIN

Raw materials

Energy

Water

Project lifecycle

Design | Source | Deploy | Operate | Dismiss

Component Manufacturing | Product Manufacturing | System Manufacturing | Technology Distribution | System Integration | ICT infrastructure operations | Cyber-physical infrastructure operations

Embedded Software | Support Software

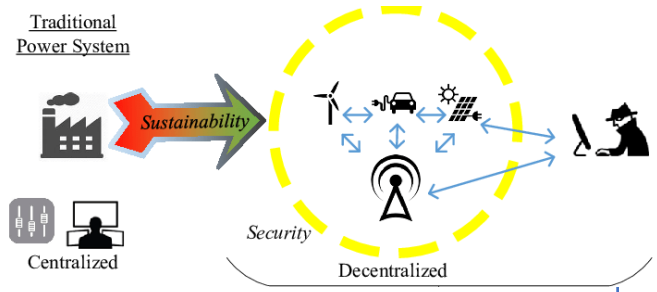
Software

Configuration | Integration | Customization

Maintenance (patching)

Globalization and complex **supply-chains relationships** and **dependencies** make the **surface of defense** extremely **wide** and with **vanishing and blurred areas of responsibility of different players**: the identification of appropriate **touch points (anchors)** and mapping of **responsibilities** (and **penalties**) is a key **challenge for regulation** (and **challenge for the players** in the business ecosystems)

Power sector is different



Peculiarities of the electricity sector

Electricity needed to run digital

Digital systems used for operating the grid need power feeds with quality and continuity

Real-time and availability requirements

Standard cybersecurity practices (authentication and encryption) are not matching requirements – in OT availability has apriority over integrity and confidentiality

Cascading effects

Outages and malfunctions can trigger blackouts in other sectors (telco, finance, transportation, healthcare, …) and countries

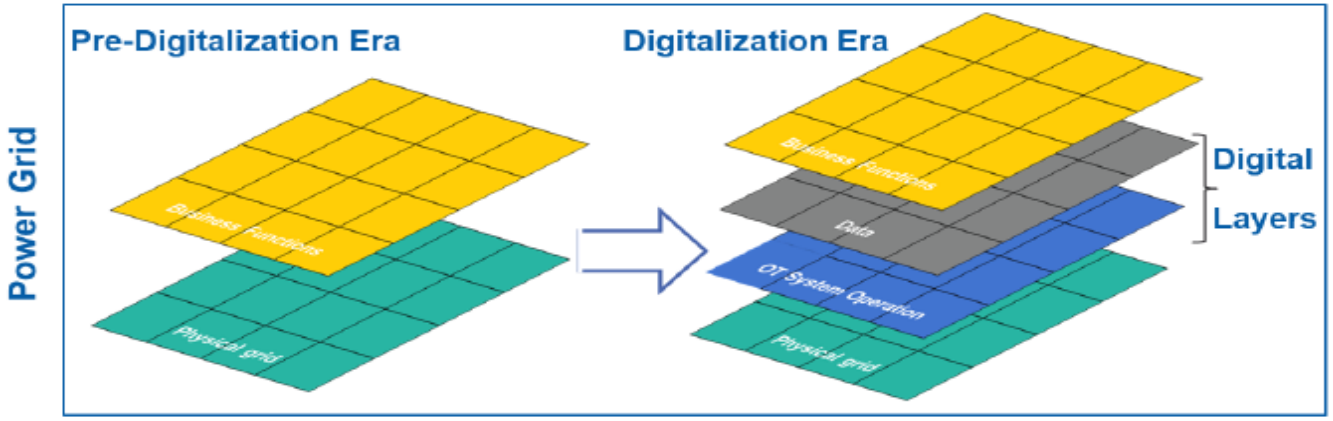
Technology mix

Risks from legacy long life-cycle components designed when cybersecurity was not an issue and from new IoT devices not made with cybersecurity in mind

Limits of ordinary cyber-defense approach

Control system in the energy sector that is under attack cannot be just disconnected from the network

Energy transition and digitalization is enlarging the surface of attack



"Security by design" is the new mantra

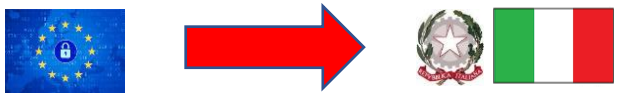
Harmonization of regulation is a crucial issue

EU GENERAL CYBERSECURITY LEGISLATION

CYBERSECURITY STRATEGY 2013 (updated 2020)	CYBERSECURITY PACKAGE 2017	NIS DIRECTIVE 2016 (Draft NIS 2 Dec. 2020)	EUROPEAN CRITICAL INFRASTRUCTURES DIRECTIVE 2008	CYBERSECURITY ACT 2019

Proposal for a Cyber Resilience Act 15/09/2022

The massive ongoing process of EU regulation for **horizontal** and **vertical** cybersecurity faces **harmonization issues** related to convergence and inter-relationship: **orientation** and **load challenges** for each player in the **supply-chain** facing **national regulation** and **compliance**



Proposed Directive on the resilience of critical entities (CER) 2020

Proposal for an Artificial Intelligence Act 21/04/2021

The EU toolbox for 5G security 2021

Radio Equipment Directive (RED) Article 3.3 Cybersecurity 12/01/2022

European Electronic Communications Code (EECC) 17/12/2018

EUCS – Cloud Services Scheme 22/12/2020

Candidate EUCC Scheme V1.1.1 25/05/2021

EU ENERGY-SPECIFIC CYBERSECURITY LEGISLATION

Regulation of the security of Gas supply 2017/1938	Clean Energy for all Europeans 2019	Electricity Regulation 2019/943	Recommendation on cybersecurity in the energy sector 2019/553	Network Code for cybersecurity aspects of cross-border electricity flows 2022
				Risk Preparedness Directive 2019/941