Cyber security considerations for the energy sector: a perspective from the electricity sector

Laurent Schmitt

ENTSO-E

Florence Forum 30-31.5.2018

Cybersecurity implications of the Energy sector evolutions

Decarbonization

Decentralization

New Prosumer IoT

requires

Digitization

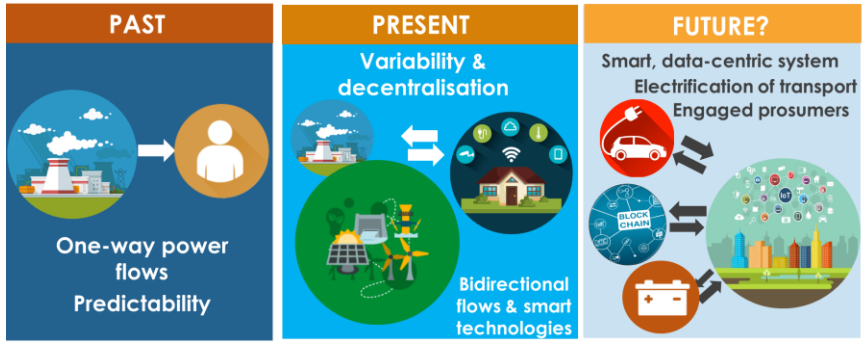
is enabled by

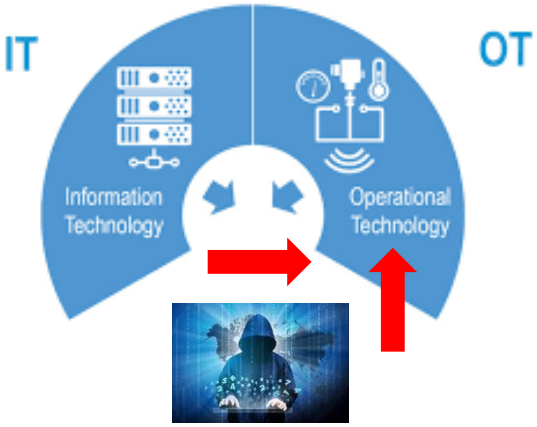
Interconnectivity & interoperability

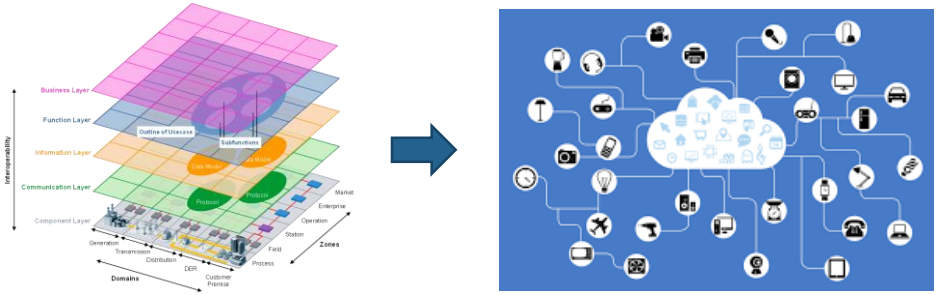
increases

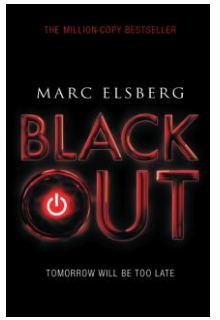
Cyber security risk

Grid Digitization : just started, significantly accelerating









New Cyber risk preparedness required

Power System Cyber risks

Risk specificities

Massive and hybrid asset base

Real-time and cascading consequence chain

Dramatic financial and societal impacts of large disruption

"*Major cyber attack on the US power system could cost up to US$ 1.000 billion.*"
Lloyd's analysis - 2015

New approach required

- Cyber security by design for solutions
- Shared awareness across all TSOs and RSCs (and DSOs in the future
- Pan-European attack pattern anticipation

New tightened ENTSO-E Cybersecurity approach

New expertise

- MOUs with **ENCS, ENISA, ACER & CENELEC**
- Strengthened implication into **EC SmartGrid Taskforce / EG2**
- New ENTSO-E Cyber Strategy Paper

New tools

- Roll-out of the **Integral Security Framework (Sep 2017)**
- New cooperation tool **for Cyber Incidents** (2018-19)

New Infrastructures

- New robust security plans e.g. **CGM Security Plan (Oct 2017)**
- Evolve Electronic Highway into new E-SCN (COMO) architecture