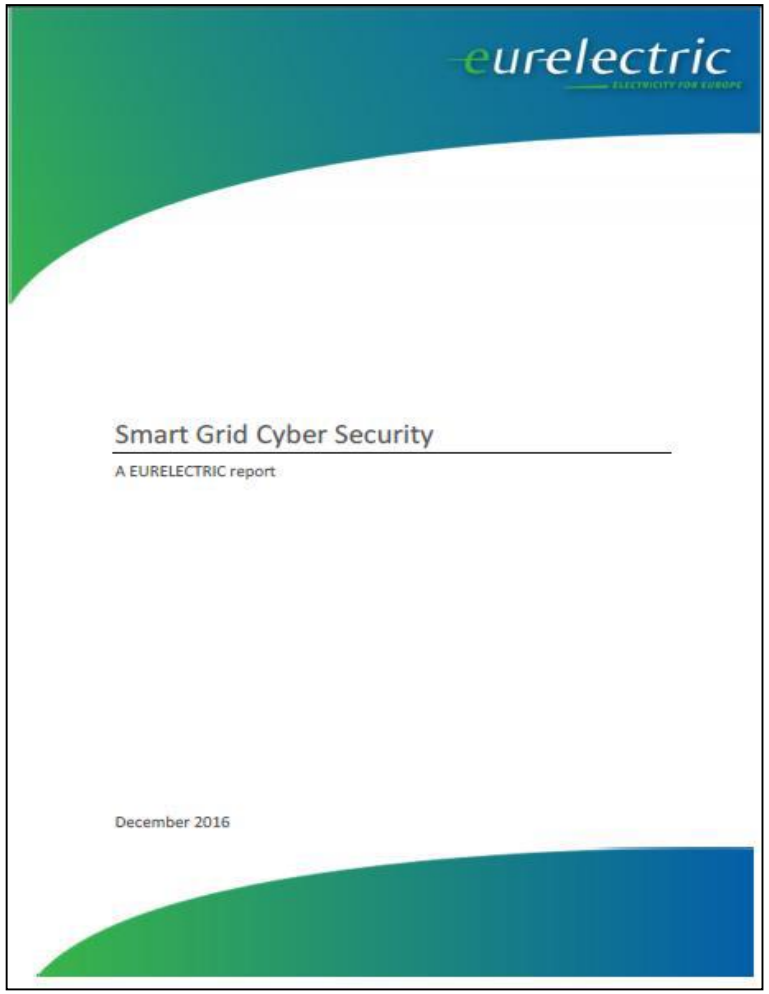
What needs to be done from a DSO perspective

- **Digitalization brings benefits** but also can present **risks** to our infrastructure.
- Regulatory framework and **incentives for investment** are needed.
- Enhance employee awareness and **cybersecurity culture**
- Empower **EU-DSO entity** in cybersecurity on equal footing with ENTSO-E
- Engage new threats coming from **IOT vulnerabilities**
- NIS Directive:
  - ✓ Need for homogeneous **speed of implementation** at all **Member States**
  - ✓ A minumun mandatory european **set of standards** and **cybercertification** including equipment **vendors**

Eurelectric work on cybersecurity



Dedicated report on Smart Grid Cyber Security

- Sector specific **threats and challenges**
- Current and potential **legislative frameworks**
- National & European **initiatives** on Smart Grid Cyber Security
- **Guidelines** for enhancing cyber security capabilities

eurelectric powering people

Background slides

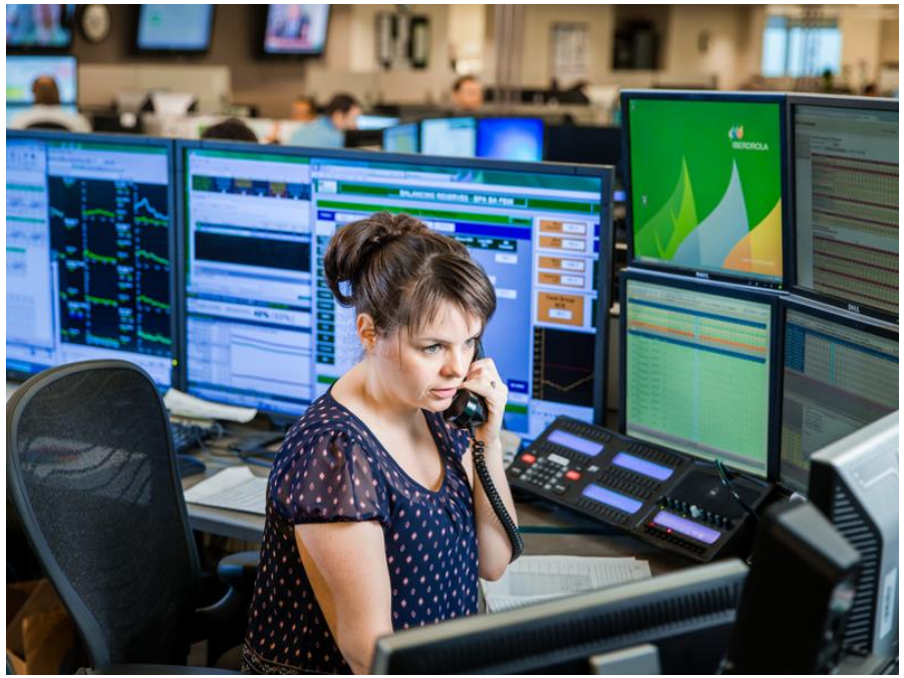
Case Study: Activities at Iberdrola

- Iberdrola is developing a **Cybersecurity Policy** for its global **DSO** business
- Using the best contractors
- Implementing the best standards
- Reinforcing AMI securitization at more ISO/OSI layers
- Developing its own Iberdrola **61850 standard** to widen vendor options
- **Hardening** and **ring fencing** legacy equipment
- Implementing **company-wide cyber governance** with a comprehensive internal organization
  - Covering **existing gaps** in current standards
  - **Deep defense** approach: multiple layers of protection for **OT**

Cybersecurity challenges for DSOs

REAL-TIME REQUIREMENTS

- The **distribution** sector operates **critical equipment** that needs to respond in real time
- The electricity industry has **specific equipment** and requirements (both **IT** and **OT**). General Purpose solutions are not always applicable. **Intensive and costly investment** R&D is needed
- Disclosure of **vulnerabilities** and incidents affecting the electricity sector should be extremely **confidencial**



Cybersecurity challenges for DSOs

INTERCONECTIVITY

- An outage in the electricity sector has **global consequences**. The whole system is **as strong as its weakest link**
- All **DSOs big and small must comply** with the same cybersecurity standards
- DSOs have specific equipment and requirements that require **investment in tailored solutions**.
- **Distributed Energy Resources** and smart appliances must be as **cybersecure** as the rest of the system

Cybersecurity challenges for DSOs

MIX OF LEGACY AND NEW TECHNOLOGIES

- The number of devices that make up the smart grid is **huge**
- The number of **smart consumers** and prosumers will **increase** in the distribution grid
- Unlike electronic devices, electrical equipment is **expensive** and have **long operating lives**. Patching legacy equipment may not be an option. **Complete renovation** may be necessary in many cases.