Cybersecurity Initiatives in the Energy Community

Regional Conference
Cybersecurity: Cooperation and Information Exchange

Energy Community

Mission:

Extending the EU internal energy market

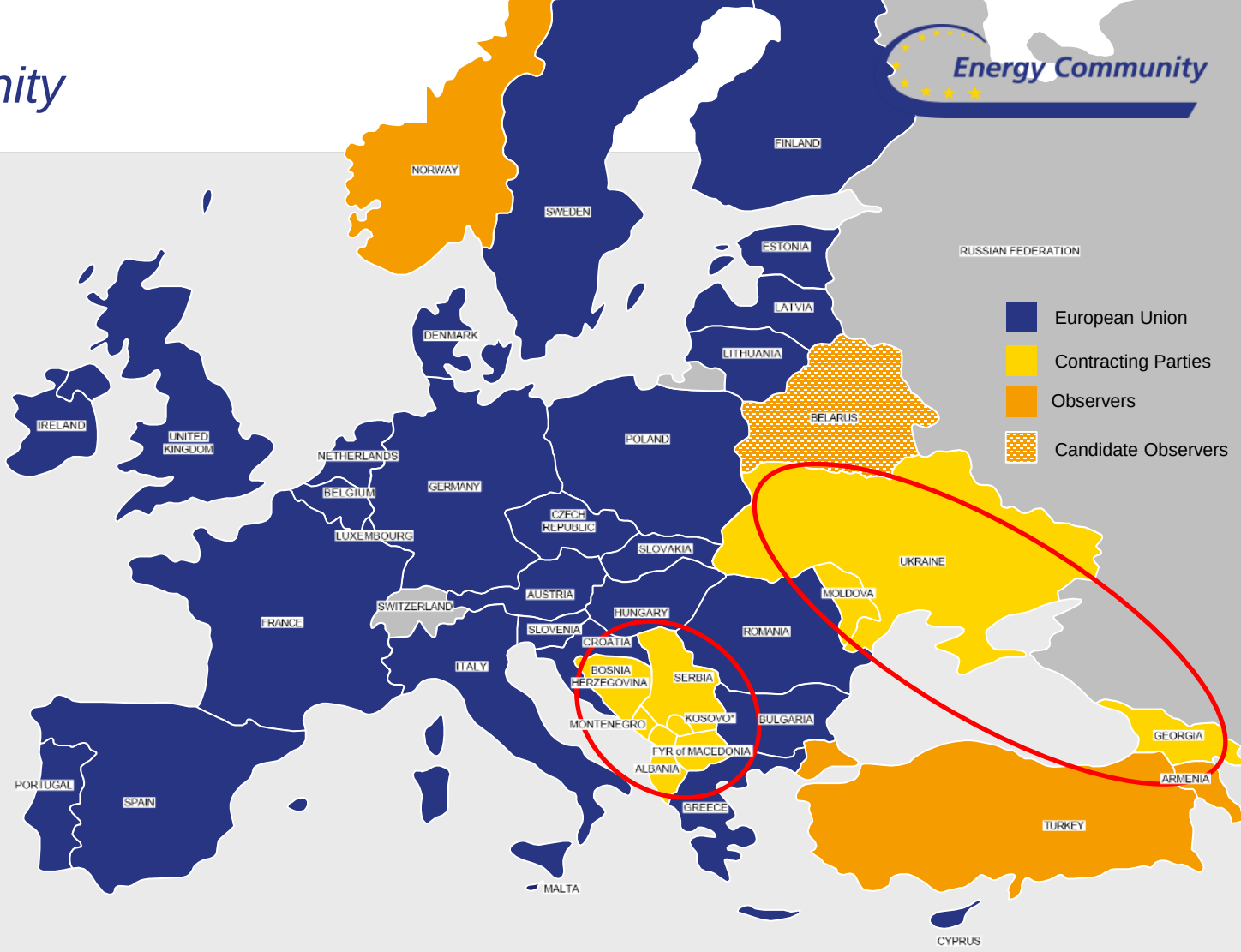
Why?

Creating a single regulatory and market environment to:

- *increase regulatory certainty,*
- *enhance security of supply,*
- *increase competition in the energy markets*

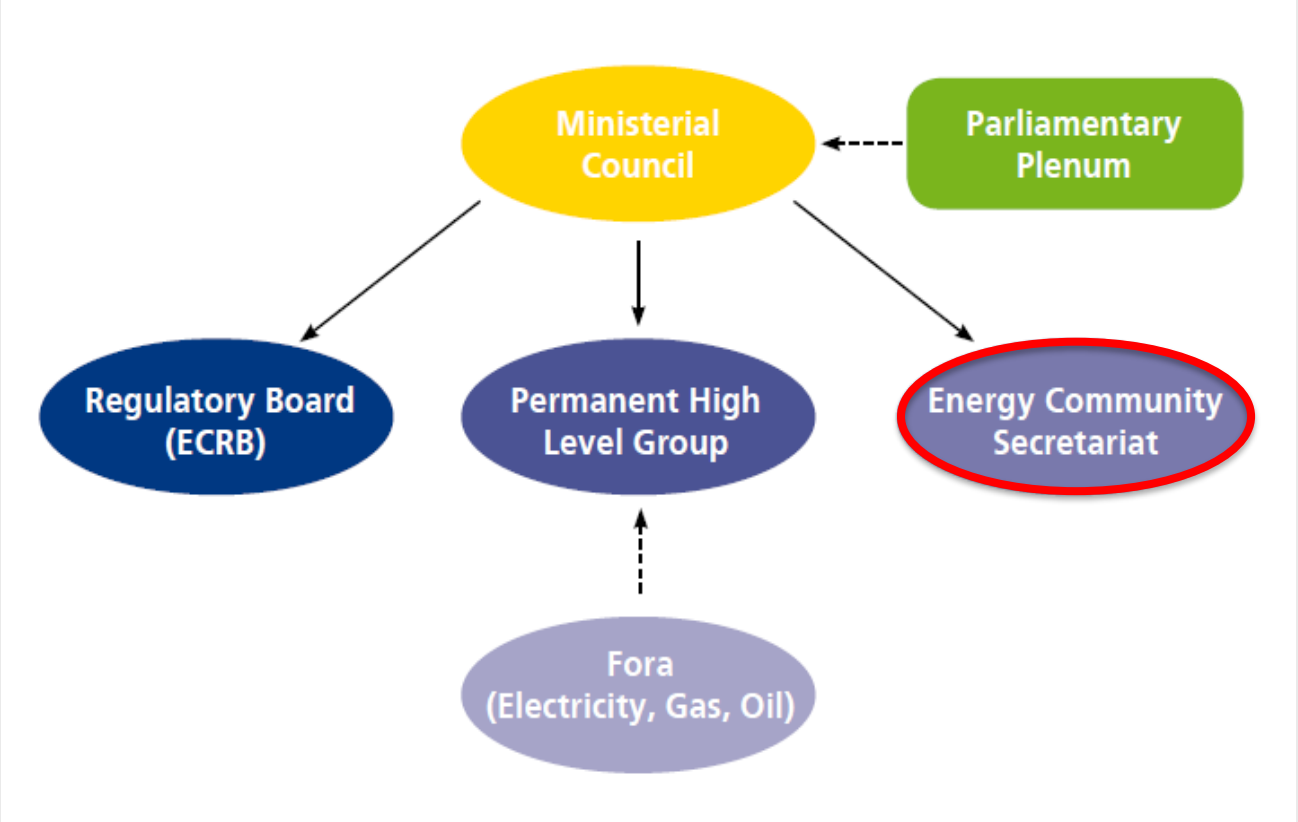
How?

By the Rule of Law



Legal Framework

- *Electricity*
- *Gas*
- *Security of Supply*
- *Energy Infrastructure*
- *Energy Efficiency*
- *Renewables*
- *Environment (partly)*
- *Climate (partly)*
- *Oil stocks*
- *Statistics*
- *Competition*



Cyber threats in energy systems

❖ Main cyber risk in electricity networks

- Complex topology
- Diverse technologies
- Automated controls (SCADA, EMS, MMS, AGC…)
- Diverse communication channels

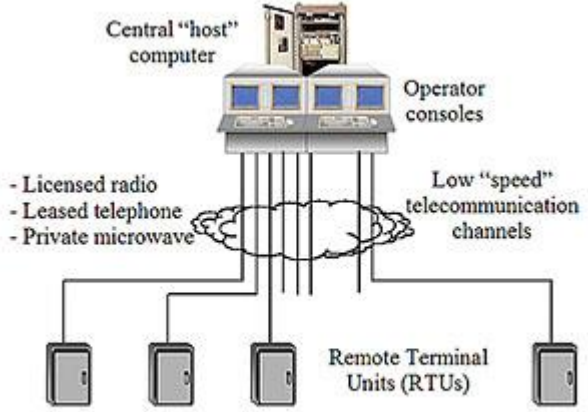


Figure 1.0 – SCADA architecture in the 1970's

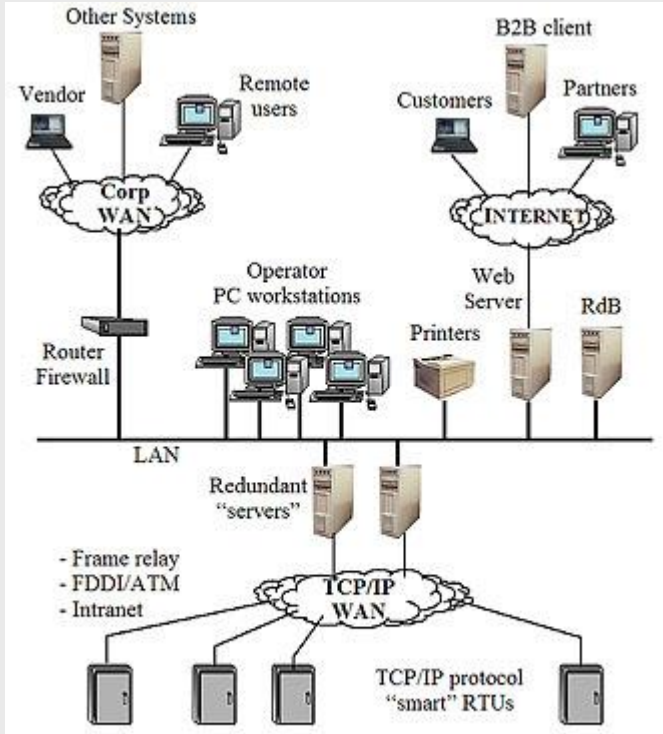
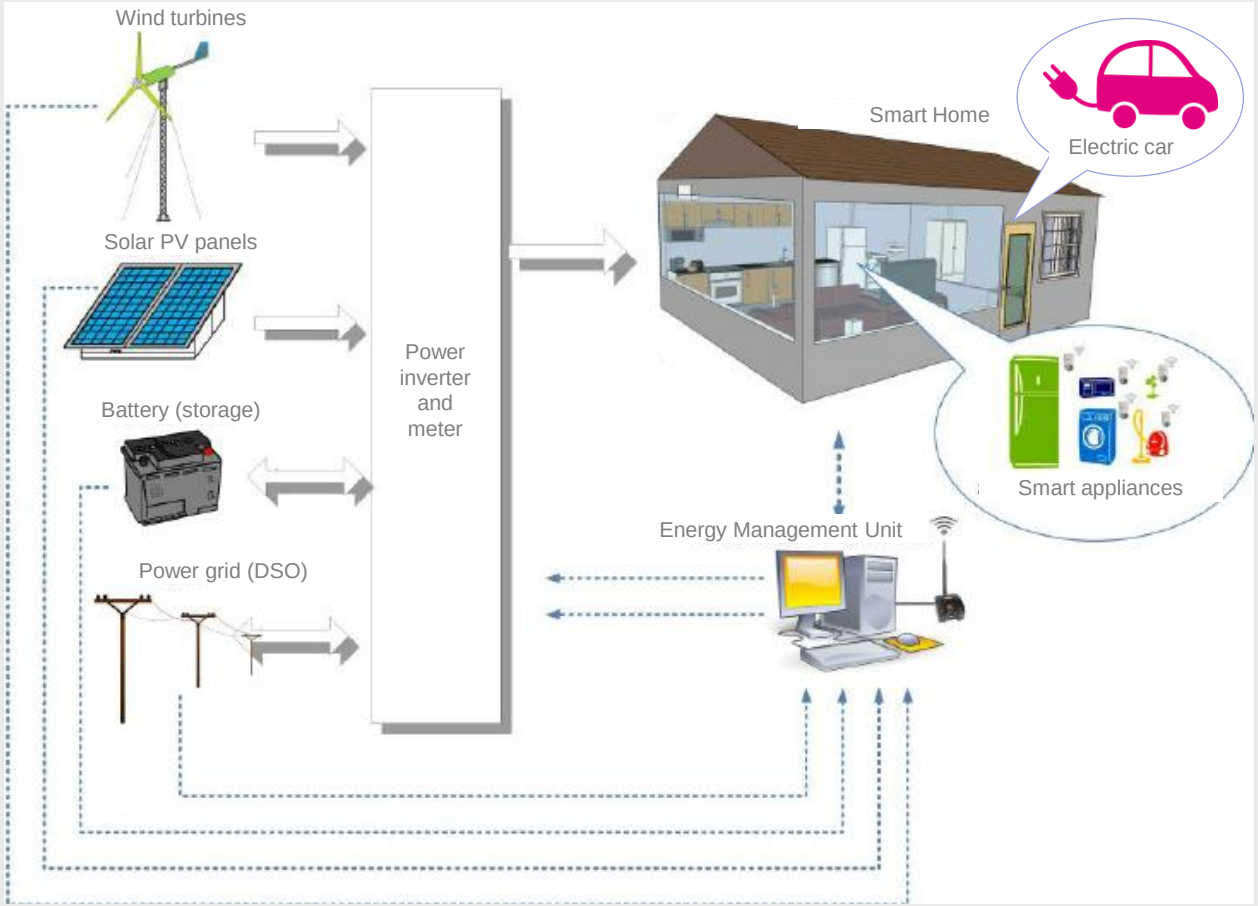


Figure 1.1 – SCADA architecture in the 2000's

Cyber threats in energy systems



❖ “Smart home” threats

- Smart meters – access and use of data
- “Smart” devices behind the meter
- Expanding market for end-user products
- Diverse unreliable technologies and applications
- Insufficient or missing safety standards
- Data ownership and protection not defined or not implemented

Cyber threats in energy systems

❖ Security challenges in the energy sector

- Moving towards interconnected, digitalized and decentralized systems
- Proliferation of highly interactive but poorly secured (“user friendly”) information and communication technologies
- Outsourcing and renting of infrastructures and services
- Increased interdependency and exchange of data among market players
- Protection concepts and design rules of energy facilities not adequate to modern threats
- Dependence on foreign technologies (intregrity and compatibility of components)
- Cross-border interconnected energy network – the “weakest link” and “cascade” effects
- Constraints imposed by security measures – in contrast to real-time-availability requirements
- Availability of human resources and their competences
- Evolving cybercrime business models, growing powers / interests of cybercrime communities
- Diverse ownership structures and related rights and decisions

Cyber threats in energy systems

❖ Cyber attack example (**Ukraine** electricity networks)

- **December 2015**
  - three Oblenergo (DSO) systems compromised: **Prykarpattya** – switched off 30 SS (225.000 citizens) for a period of 6 hours; **Chernivtsi** and **Kiyvoblenergo** to lower extent
  - imposed vast damage on systems and data

- **December 2016**
  - Ukrenergo 330 kV Transmission SS **Kiyv North** - SCADA system compromised causing blackout for 1/5 of Kiyv demand for one hour
  - advanced, automated malware, swappable, adaptable and universal
  - simultaneous threat to multiple systems
  - attacks were related

Critical Infrastructure Directive 2008/114/EC

- Critical Infrastructure: an asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people and the disruption or destruction of which would have significant impact in a MS as a result of the failure to maintain those functions
  - **European Critical Infrastructure (ECI)** – significant impact on at least two MSs (CPs)
  - ECI sectors: Energy (Electricity, Gas and Oil), and Transport
- Identification of ECI
  - **Criteria** - Sectoral, cross-cutting and trans-boundary, corresponding **Thresholds** (severity of impact),
- Designation of ECI (bilateral / multilateral)
  - Potential / suspected ECI, level of impact, **discussions**, reporting (EC), informing the operator, discretion principles
- Operator Security Plan
  - **Identification** of assets / threat scenarios – **risk** analysis / vulnerability and potential impact / security **measures**
  - Periodic **review**, supervision, Community measures and compliance with agreed **criteria**
- Security Liaison Officers – communication mechanisms
- Threat assessment and reporting (EC), common methodologies, classified information

NIS Directive (EU) 2016/1148

- Build sufficient capacities at national level
  - Adopt a national NIS strategy
  - Designate national competent authorities, single contact points and Computer Security Incident Response Teams (CSIRTs)
- Identify critical infrastructure, operators of essential services (**OES**), and relevant digital service providers
- Build structures for cross-border cooperation and exchange of information
  - At strategic level - creating a Cooperation Group of national authorities
  - At operational level - creating a network of national CSIRTs

NIS Directive (EU) 2016/1148

- Cumulative conditions for identification of **OES**
  - provision of a service essential for critical societal / economic activities
  - provision of that service depends on network and information systems
  - an incident would have significant disruptive effects on the provision of that service
- Security and Notification Requirements imposed on OES
  - take technical and organizational measures
    - ✓ to secure networks and systems
    - ✓ to prevent and manage risks
    - ✓ to handle incidents and minimize their effects
  - notify incidents
- Monitoring and enforcement powers

❖ PHLG Recommendations (March & June 2018)

- Create a Cooperation Group between CPs and MSs
- Put in place common certification conditions across the Energy Community
- Eliminate regulatory gaps
- Initiate cooperation on the establishment of research and education programmes
- Develop a common crisis management and rapid emergency response mechanism, inter alia through Title III or Title IV measures
- Step-up public-private cooperation in cybersecurity

Cybersecurity in the Energy Community

❖ Study on Cybersecurity in energy

- Timeline
  - Deadline for tenders: 20 September 2018
  - Start of activities: (31 October 2018)
  - Completion: within 10 months
- Contracting Parties to:
  - Work closely with the consultant
  - Provide all the necessary data
  - Engage the relevant actors in the energy sector

❖ Study on Cybersecurity in energy

- Objectives
  - Identify and assess key weaknesses, risks and exposure to cyber threats in the energy systems
  - Identify the existing regulatory framework and regulatory gaps for cybersecurity governance
  - Identify the relevant provisions of the NIS Directive and the Directive on European critical infrastructure and provide an impact assessment of their implementation in the Energy Community
  - Propose the necessary measures to improve cybersecurity in Contracting Parties (national level)
  - Propose a model for regional cooperation in managing cybersecurity risks and reporting incidents as well as a common cooperation platform, common certification framework and common framework for research, education and training programmes
  - Explore the possibility for the participation of Contracting Parties in the work of the European Union Agency for Network and Information Security (ENISA).

❖ Study on Cybersecurity in energy

- Task 1
  - Identify the current legal and policy framework and administrative and regulatory rules and environment including competent authorities and law enforcement authorities relevant for cybersecurity in the domain of energy. In particular assess:
    - ✓ National strategies related to cybersecurity
    - ✓ Resilience measures including crisis prevention, monitoring and notification of incidents
    - ✓ Security requirements applicable in the energy and dependent sectors
    - ✓ Mechanisms for cross-border incident and crisis management
    - ✓ Public-private initiatives related to cybersecurity and existing training and education programmes
  - Assess whether Contracting Parties have measures in place transposing the NIS Directive, the Directive on European critical infrastructure and the Directive on attacks against information systems
  - Assess whether Contracting Parties took measures to implement the Council of Europe Convention on Cybercrime
  - Identify the current institutional framework for enhancing cybersecurity (authorities, market participants, CSIRTs)
  - Identify the existing cross-border cooperation initiatives
  - Identify the ongoing projects and technical assistance related to improving the governance on cybersecurity
  - Identify existing cybersecurity standards and certification schemes in Contracting Parties
  - Identify existing education and training programmes related to cybersecurity
  - Identify cyber threats and risks to which Contracting Parties are exposed

❖ Study on Cybersecurity in energy

- Task 2
  - Based on the analysis of Task 1, identify the legal and regulatory gaps, inconsistencies and diverging provisions in the Contracting Parties' existing legal, regulatory and institutional frameworks
  - Identify and prepare an overview of the gaps in cybersecurity standards between the Contracting Parties and standards applicable in the EU
- Task 3
  - Propose amendments, policies, measures, procedures and recommendations necessary to implement minimum common framework addressing cybersecurity of critical infrastructure in the Energy Community
  - Propose cooperation mechanisms in the Energy Community (criteria for the identification of large-scale cybersecurity incidents, cross-border cooperation, relevant actors and standard operating procedures)
  - Provide recommendations how to align certification schemes and procedures as well as research, education and training programmes
  - Provide ipact assessment of the implementation of the proposed acts and measures in the Energy Community
  - Develop a roadmap with the timing of the implementation of the proposed provisions and measures

❖ Implementation of NIS Directive

- PHLG (March 2018) Conclusions:
  - Acknowledged the necessity to build cybersecurity capabilities and risk management and incident reporting culture in the Energy Community
  - ECS to explore the incorporation of the **NIS Directive**, take steps and discussions for identification of suitable provisions, and prepare a proposal with adaptations and appropriate timing
  - Recommended to eliminate regulatory gaps and develop cooperation structures, certification framework and research and education programs

- PHLG (June 2018) Conclusions:
  - Discussed the options for establishment of organizational framework for high level of security of information systems and critical infrastructure within the Energy Community Security of Supply Coordination Group and defining the roles of the key actors
  - Underlined the necessity to integrate such structures in the European framework
  - To explore the possibilities for participating of the Energy Community and the Contracting Parties in the ENISA