Energy Community
- Cybersecurity in the energy sector

MKD-CIRT Cybersecurity Conference

Regional critical sectors interdependence. Importance of information sharing in the region and internationally

Energy Community
Treaty

Mission

Extending the EU internal energy market

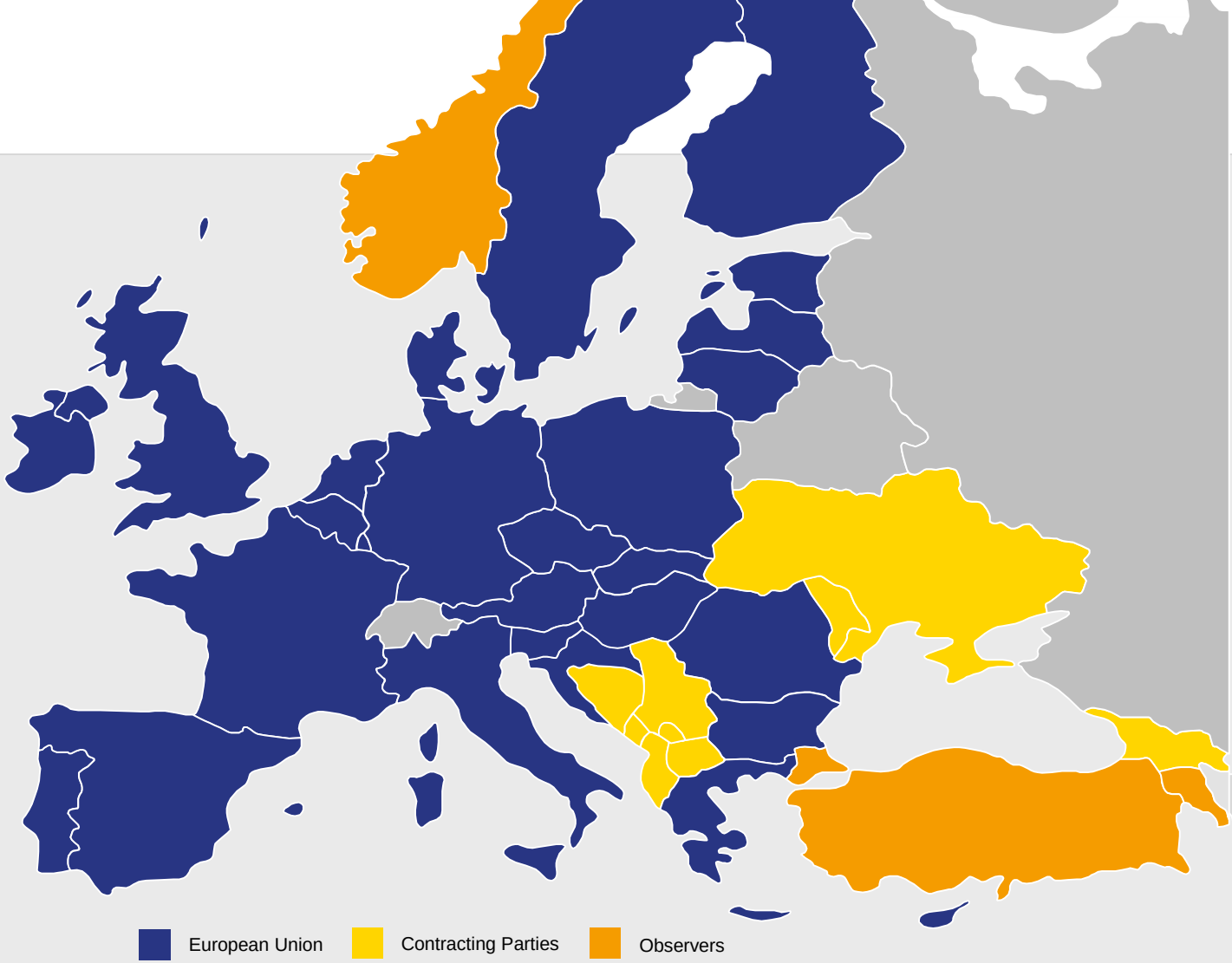
Target

Creating a regulatory framework to increase:

- competition in the energy markets
- security of supply
- investments in infrastructure
- environment and climate protection

Method

The Rule of Law



MINISTERIAL COUNCIL

PERMANENT HIGH LEVEL GROUP

} ***Political decisions***

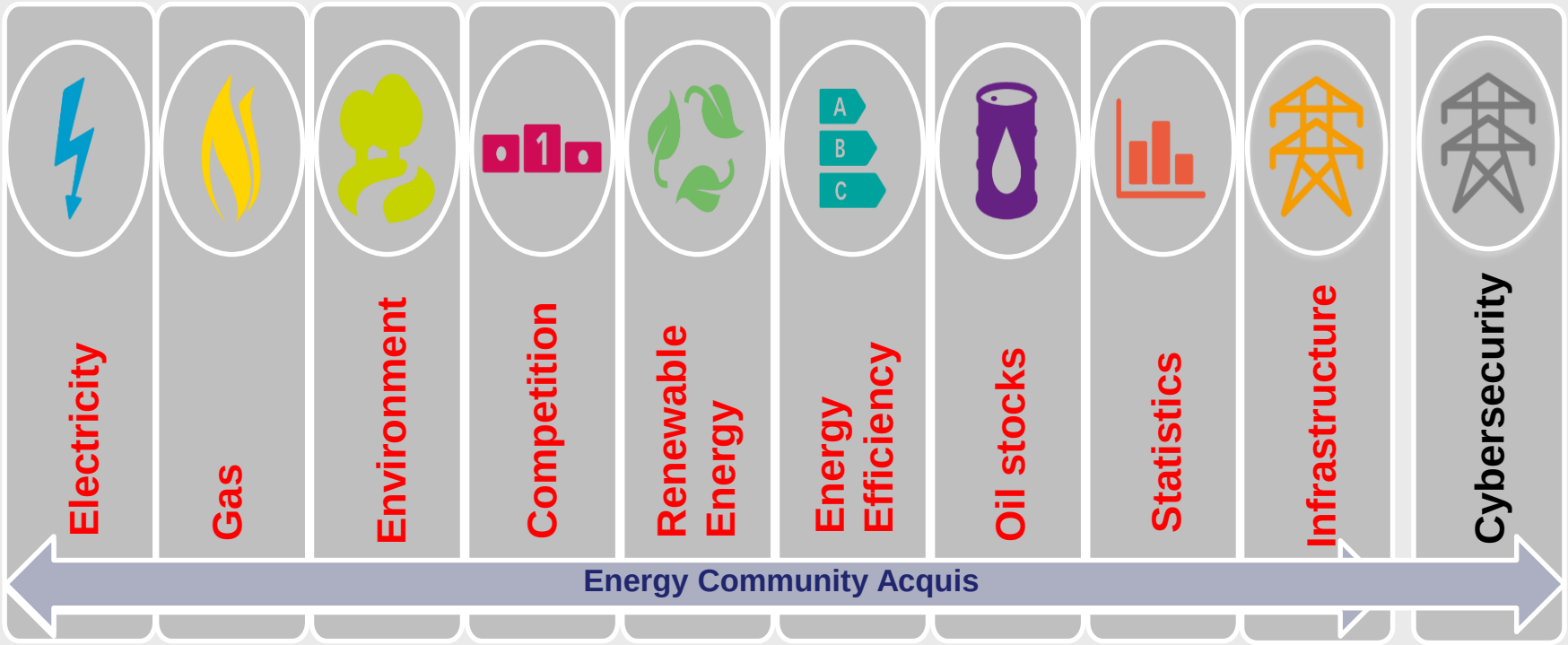
REGULATORY BOARD (ECRB) → ***Advisory body***

↳ *Working groups (EWG, GWG, RCWG)*

SECRETARIAT → *Monitoring, coordination, support*

ELECTRICITY FORUM | **GAS FORUM** | **OIL FORUM** | **SUSTAINABILITY FORUM**

Stakeholders' involvement


Electricity
Gas
Environment
Competition
Renewable Energy
Energy Efficiency
A
B
C
Oil stocks
Statistics
Infrastructure
Cybersecurity
Energy Community Acquis

Cyber threats in energy systems

❑ Sources of cyber risk in electricity networks

- Complex network topology
- Decentralization, volatility
- Diverse / mixed technologies, multiple standards
- Automated controls (SCADA, EMS, MMS, AGC…)
- Diverse communication channels / multiple access

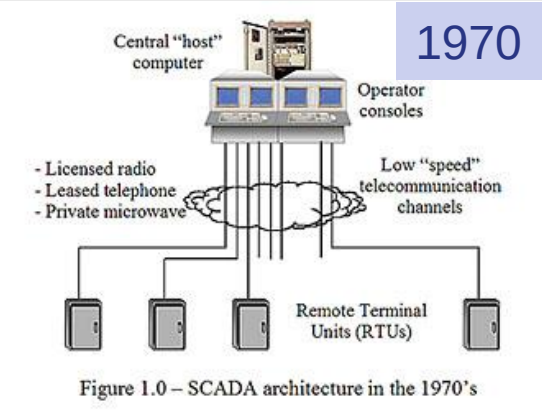


Figure 1.0 – SCADA architecture in the 1970's

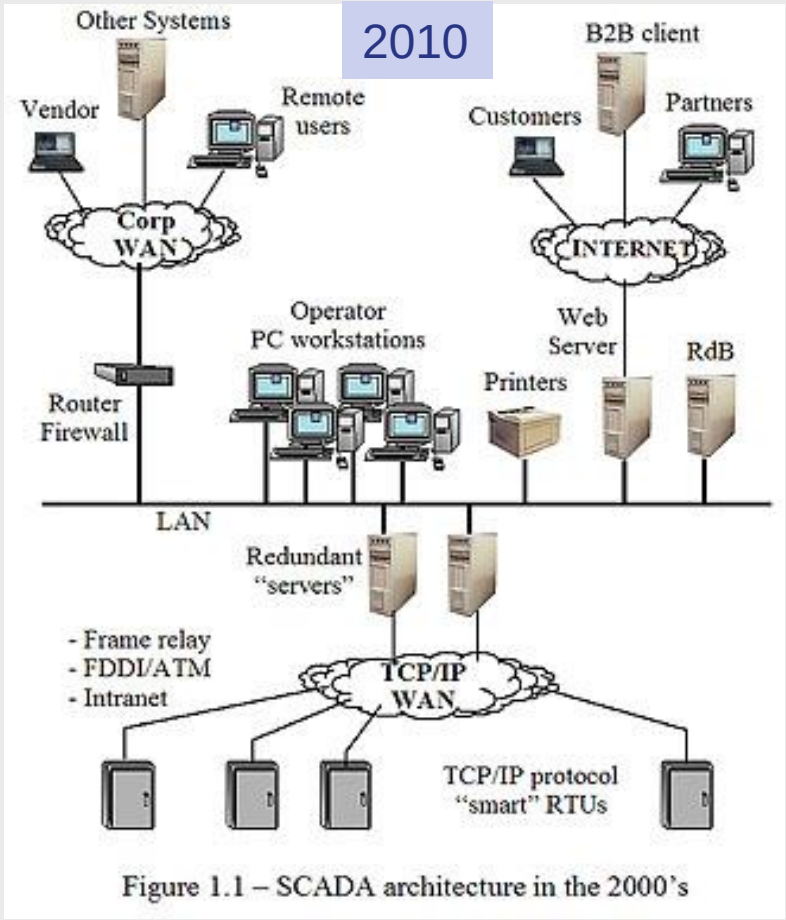
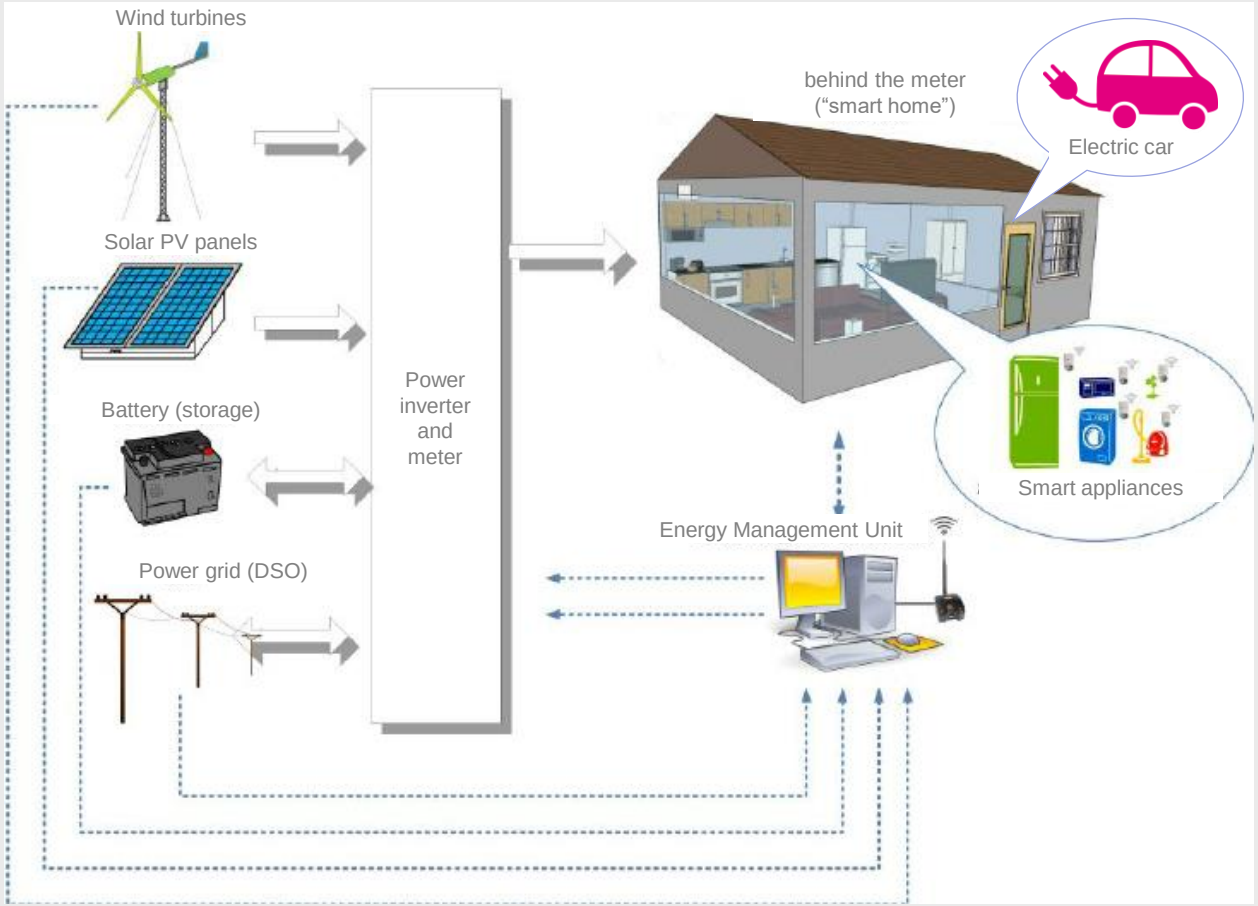


Figure 1.1 – SCADA architecture in the 2000's

Cyber threats in energy systems



❑ "Smart home" threats

- Smart meters – access and use of digital information
- "Smart" appliances behind the meter
- Diverse / uncertified technologies and applications
- Insufficiently applied or missing safety standards
- Data ownership and protection not defined or not enforced
- Lack of public awareness and knowledge how to alleviate risks

Cyber threats in energy systems

❑ Cyber incidents – Ukraine electricity grid

- *December 2015*
  - three Oblenergo (DSO) systems compromised: **Prykarpattya, Chernivtsi** and **Kiyvoblenergo** to lower extent
  - switched off 30 SS (225.000 citizens) for a period of 6 hours
  - 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 city demand for one hour
  - advanced, automated malware, swappable, adaptable and universal
  - simultaneous threat to multiple systems
  - (attacks were similar and related)

…the energy sector presents certain particularities that require particular attention - EC Recommendation C(2019)240, Staff Working Document SWD(2019)1240 :

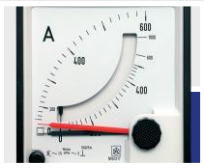
- **Real-time requirements** - some energy systems need to react so fast that standard security measures such as authentication of a command or verification of a digital signature can simply not be introduced due to the delay these measures impose.

- **Cascading effects** - electricity grids and gas pipelines are strongly interconnected across Europe and well beyond the EU. An outage in one country might trigger blackouts or shortages of supply in other areas and countries.

- **Combined legacy systems with new technologies** - many elements of the energy system were designed and built well before cybersecurity considerations came into play. This legacy now needs to interact with the most recent state-of-the-art equipment for automation and control, such as smart meters or connected appliances, and devices from the Internet of Things without being exposed to cyber-threats.

Cyber threats in energy systems

EU Legal framework - EC Recommendation on Cybersecurity



Real-time Requirements

- Use international standards
- Apply physical measures
- Classify/manage your assets
- Consider privately owned communication networks, or consider specific measures
- Split system into logical zones
- Choose secure communication and authentication

Cascading effects

- Evaluate interdependencies
- Ensure communication framework for early warnings and to cooperate in crisis
- Ensure level of security for new devices
- Consider cyber-physical spill overs
- Establish design criteria for a resilient grid

Technology mix

- Follow a cybersecurity-oriented approach when connecting devices
- Use international standards
- Establish monitoring and analysis capabilities
- Conduct specific cybersecurity risk analysis for legacy installations
- Collaborate with technology providers
- Update hardware and software

Clean energy for all Europeans package

	European Commission Proposal	EU Inter-institutional Negotiations	European Parliament Adoption	Council Adoption	Official Journal Publication
Energy Performance in Buildings	30/11/2016	Political Agreement	17/04/2018	14/05/2018	19/06/2018 - Directive (EU) 2018/844
Renewable Energy	30/11/2016	Political Agreement	13/11/2018	04/12/2008	21/12/2018 - Directive (EU) 2018/2001
Energy Efficiency	30/11/2016	Political Agreement	13/11/2018	04/12/2018	21/12/2018 - Directive (EU) 2018/2002
Governance of the Energy Union	30/11/2016	Political Agreement	13/11/2018	04/12/2018	21/12/2018 - Regulation (EU) 2018/1999
Electricity Regulation	30/11/2016	Political Agreement	26/03/2019	22/05/2019	-
Electricity Directive	30/11/2016	Political Agreement	26/03/2019	22/05/2019	-
Risk Preparedness	30/11/2016	Political Agreement	26/03/2019	22/05/2019	-
ACER	30/11/2016	Political Agreement	26/03/2019	22/05/2019	-

- **Electricity Directive** - references to cybersecurity:
  - Smart metering systems (Advanced Metering Infrastructure), as well as metering data communication and protection – apply the best available techniques for ensuring the highest level of cybersecurity protection
  - Tasks of TSO in development of data management systems

- **Electricity Regulation** - references to cybersecurity:
  - Tasks of ENTSO-E in promoting cybersecurity and data protection
  - Tasks of EU DSO Entity in development of data management and protection
  - Network Code for cybersecurity aspects of cross-border electricity flows including rules on common minimum requirements, planning, monitoring, reporting and crisis management
  - Rules concerning the tasks of the Regional Coordination Centres (RCC)

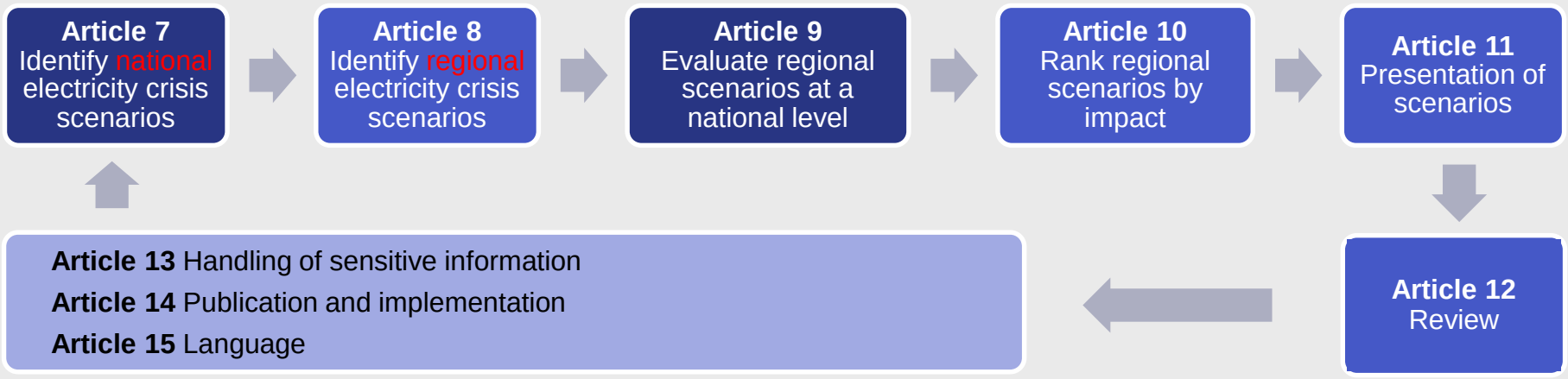
❑ Governance Regulation - relevance to cybersecurity:

- Energy Union five dimensions are promoted - (a) energy security; (b) internal energy market; (c) energy efficiency; (d) decarbonisation; and (e) research, innovation and competitiveness

❑ Risk-preparedness Regulation - references to cybersecurity:

- Complements the NIS Directive and CI Directive in the context of Security of Supply
- Cyber-incidents are properly identified as risk and that the measures taken to address them are properly reflected in the risk-preparedness plans and contributes to creating a comprehensive approach to the energy security
- Risk assessment methodology (also including malicious attacks) based on scenarios:
  - Simultaneous
  - Cross Border
  - At Regional Level
  - At National Level
  - All which goes beyond N-1 security criterion

❑ Risk Preparedness Regulation – methodology for identification of regional electricity crises scenarios



Challenge: Regulation

- does not facilitate effective trans-national cooperation

- **Country-level** regulations may forbid sharing of information
- Problems between **EU** and **NON-EU** members

Challenge: Organization

- "russian dolls" in network architecture

- **Complexity** of the ENTSO-E power system
- Connection of facilities (generators, loads) with extreme **diversity** in size and technology
- Large **stakeholder setup** – entanglement between large operators (TSO, RSC, DSO)

Policy:

- inter-TSO and - RSC cybersecurity measures

- **Security** – prevention control and compliance with standards
- **Resilience** – incident monitoring, detection, response and recovery

❑ Smart Grid TF Expert Group 2 - Cybersecurity Network Code for energy utilities

ToR – Step 1 Objectives for Network Code → **ToR – Step 2** Key areas for Network Code → **ToR – Step 3** Instruments used by Network Code → **ToR – Step 4** Recommendations on Network Code

- Harmonized Cybersecurity Baseline
  - Conformity to ISO 27001
  - Minimum Security Requirements
- Advanced Cybersecurity Implementation for OES
  - Protection of Current Infrastructure
  - Supply Chain Risk Management
  - Cross border and Cross Organisation Risks
  - Early Warning System
- Supportive elements
  - Crisis management
  - Supply Chain Security
  - Energy Cybersecurity Maturity Framework

NIS Directive - Cooperation Group on cyber security for the energy sector (AT is the leader)

- ENISA - role in the NISD CG
  - Assist MS and the EU Commission
  - Participate in the EU NIS Cooperation Group
  - Secretariat for CSIRTs Network
  - Elaborate advices and guidelines regarding standardization in NIS security
  - Organize exercises

EE - ISAC - European Energy – Information Sharing and Analysis Centre (23 members, 10 TF)

Physical Information Sharing Community

- Plenary meetings
- Community meetings
- Theme-based meetings
- Open House meetings

Digital Information Sharing Community

- Information requests
- Webinars
- White Paper

Domains on Information Sharing

- Vulnerabilities in IT and OT systems
- Threat / Risk analysis
- Incidents
- Best practices
- Alerts and notification
- Use of Standards
- Research topics

Interdependencies / opportunities and vulnerabilities as IT (Information Technology) and OT (Operational Technology) continue to converge and interoperate

- **REMIT** - EU Regulation on wholesale Energy Market Integrity and Transparency (EU) No 1227/2011
  - (23) The Agency (ACER) should ensure the operational security and protection of the data which it receives, prevent unauthorised access to the information kept by the Agency, and establish procedures to ensure that the data it collects are not misused by persons with an authorised access to them.
  - The operational security of the IT systems used for processing and transmitting the data therefore also needs to be ensured.
  - These rules should also apply to other authorities that are entitled to access to the data for the purpose of this Regulation.

❑ REMIT - EU Regulation on wholesale Energy Market Integrity and Transparency (EU) No 1227/2011

- (12) The Agency (ACER) shall ensure the confidentiality, integrity and protection of the information received … The Agency shall take all necessary measures to prevent any misuse of, and unauthorised access to, the information maintained in its systems.
- National regulatory authorities, competent financial authorities of the Member States, national competition authorities, ESMA and other relevant authorities shall ensure the confidentiality, integrity and protection of the information which they receive… and shall take steps to prevent any misuse of such information.
- The Agency shall identify sources of operational risk and minimise them through the development of appropriate systems, controls and procedures.

❑ Cost Recovery principles - to be applied in the context of implementation of cybersecurity measures and tendering of new (critical) infrastructures for regulated energy activities

Task Force - consisting of representatives from:

- competent authorities / single point of contacts of CPs
- ENTSO-E
- the CSIRT network
- TSO / security liaison officers (as applicable)
- the Secretariat
- the European Commission
- the ENISA (if possible)
- Observer and Participant countries
- relevant stakeholders (electricity)
- relevant IT environment (services)

ToR / work program / deliverables / a yearly report

Meetings

- twice a year or more, upon a motion of the Chairperson, the Chairperson of SoS CG, the Secretariat
- take part in meetings and activities of the SoS CG

Tasks

- **exchange information and best practice**, discuss modalities, on risks and incidents; on identification of operators and critical infrastructures, on awareness-raising, education programmes and training; research and development
- **discuss capabilities and preparedness of the CPs**, evaluate national strategies, assist CPs in building capacity
- **provide strategic guidance** for the CSIRTs
- **engage in discussions** with CPs and MSs on whose territory a potential critical infrastructure is located, and other affected CPs and MSs
- **support** operators of critical infrastructures with best practices, methodological guidelines
- **encourage the use of European or internationally accepted standards and specifications**; discuss them with relevant stakeholders and with relevant organizations

MC Procedural Act (29 November 2018)

on the establishment of Energy Community Coordination Group for Cybersecurity and Critical Infrastructure

(CyberCG)

- Domains (of critical infrastructure / essential services in):
  - Electricity / Natural gas / Oil / pollution and combustion emissions
  - Digital and electronic communications (services provided to energy operators)
- Stakeholders
  - Ministries (energy / climate / digital communications & information technologies), NRAs
  - Operators of critical infrastructure / essential services (Production / TSOs / DSOs)
  - National CSIRTs

MC Procedural Act (29 November 2018)

on the establishment of Energy Community Coordination Group for Cybersecurity and Critical Infrastructure **(CyberCG)**

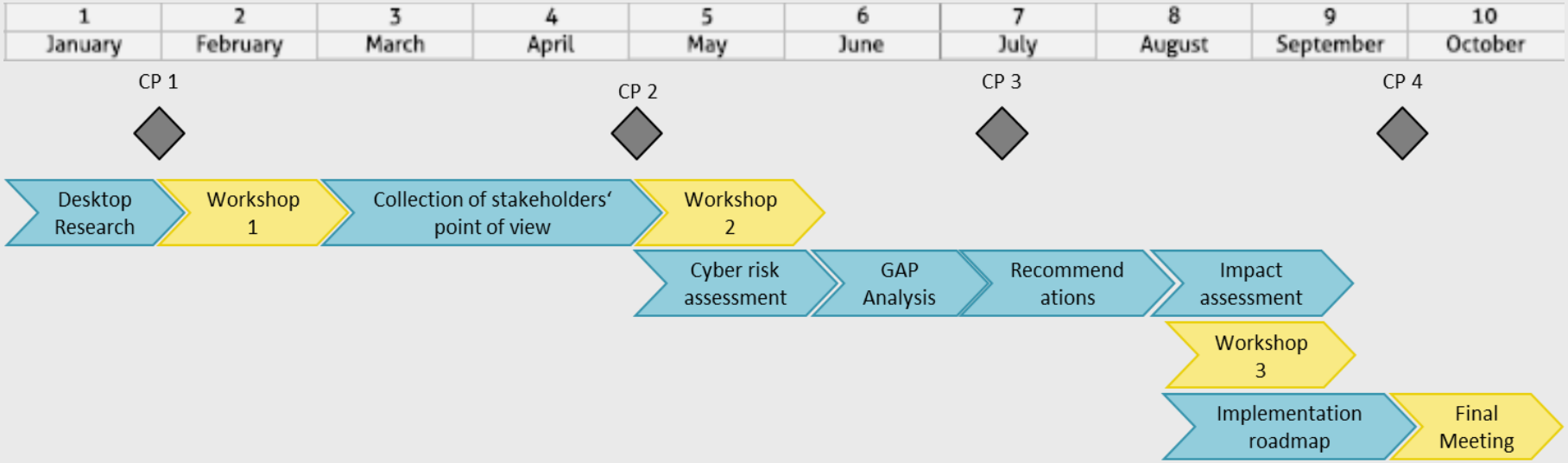
- Relevant EU *acquis* provisions
  - on Electronic communications networks and services - Directive 2002/21/EC
  - on Critical infrastructures (identification / designation / protection) - Directive 2008/114/EC
  - on Security of network and information systems - NIS Directive - Directive (EU) 2016/1148
  - European standardization in information security - Regulation No. 1025/2012/EU

MC Procedural Act (29 November 2018)

on the establishment of Energy Community Coordination Group for Cybersecurity and Critical Infrastructure **(CyberCG)**

- Tasks
  - establish administrative and operational environment (focal points / liaison officers)
  - communicate information (reports / strategies / measures) and knowledge (training / research and development / public awareness)
  - Develop and apply EU-coherent methodologies for risk assessment / security criteria / identification and designation of essential services and critical infrastructures,
  - apply EU technical standards on information security and relevant technologies,
  - establish a CSIRTs network (security incidents and threats / capacity building / blueprint for cooperation and early warning / mutual assistance)
  - facilitate cooperation with EU MSs / gaining observers' status in ENISA

- Domain: all EnC Contracting Partiers
- Scope: electricity / gas authorities, NRA, operators (TSO / DSO), producers, public domain
- Timeline:
  - Inception Report: 22 February 2019
  - First Workshop: 11 April 2019
  - Final Deadline: October 2019



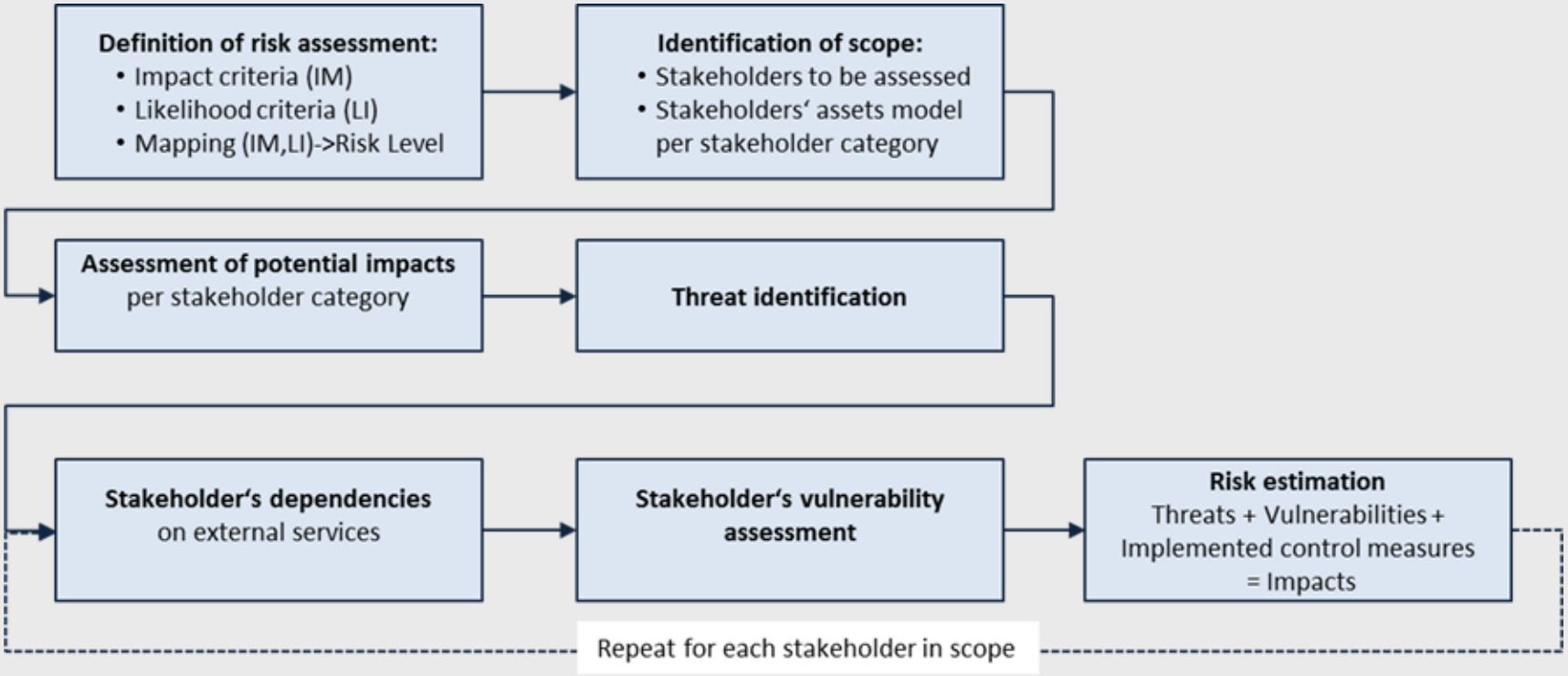
- Objectives
  - Assess the legal / regulatory environment and identify the regulatory gaps
  - Assess the potential cyber threats and risks
  - Identify the relevant provisions of the acquis and provide impact assessment of their implementation in the Energy Community
  - Propose the necessary measures on national level to improve cybersecurity
  - Propose a model for regional cooperation in managing cybersecurity risks and reporting incidents

- Task 1 (stocktaking) – identification and assessment
  - Existing cybersecurity environment (legal / policy / administrative / regulatory / enforcement / market)
  - Existing measures in place (pursuant to acquis / Council of Europe Convention on Cybercrime)
  - Existing cross-border cooperation (practices / initiatives / contingencies and potential synergies)
  - the ongoing projects (national / regional) and TA related to cybersecurity
  - cybersecurity standards and certification schemes applied in Contracting Parties
  - existing education and training programmes (expert / public domain) related to cybersecurity

- Task 2 (analysis) – identification of
  - the legal and regulatory gaps inconsistencies
  - gaps in cybersecurity standards

- Task 3 (recommendations)
  - Propose amendments, measures, and recommendations necessary to implement minimum common framework addressing cybersecurity of critical infrastructures
  - 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, participation in ENISA)
  - Provide recommendations how to align certification schemes and procedures
  - Propose mechanisms for research, education and training programmes (expert level and public domain)
  - Provide impact assessment for implementation of the proposed acts and measures
  - Develop a roadmap with the timing for the implementation

- Risk assessment Methodology



❑ CyberCG - Planned activities in 2019

- Establish a Working Group on Critical Infrastructures consisting of Ministries, NRA, Operators – a draft Work Plan shall be developed by 30 October 2019

- Establish a Working Group on Governance consisting of Ministries, NRA, CSIRTs – including cybersecurity legislation and technical standards (to the necessary level) – a draft Work Plan shall be developed by 30 September 2019

- Establish a permanent Discussion Panel (network) for CSIRTs – including CSIRT communication channels, coordination I n applied methodology and standards – target to establish an Energy CSIRT cooperation structure in the Energy Community – draft Work Plan shall be developed by 30 September 2019

- Develop a draft Program for training, education and capacity building for specific sectors – including (1) Policy authorities and NRA, and (2) CI Operators – draft proposal by 30 October 2019

- Cooperation with EC, ENISA, CEER, ENTSO-E / ENTSOG

❑ Athens Electricity Forum, 28-29 May 2019 https://www.energy-community.org/events/2019/06/AF.html

CONCLUSIONS

12. The Forum underlines that in an interconnected environment cybersecurity is a shared responsibility. To apply new technologies securely and reap the benefits of intelligent power grids, digitalisation of the energy system and internet of things, the Forum invites all actors to work together, exchange good practices and collaborate on the resilience and protection of their energy systems. The Secretariat shall support such cooperation through the established bodies, primarily the Cybersecurity Coordination Group, ECDSO-E and ECRB

13. The Forum invited regulators to adequately support cybersecurity in national regulatory cost recognition practise

simon.uzunov@energy-community.org
www.energy-community.org

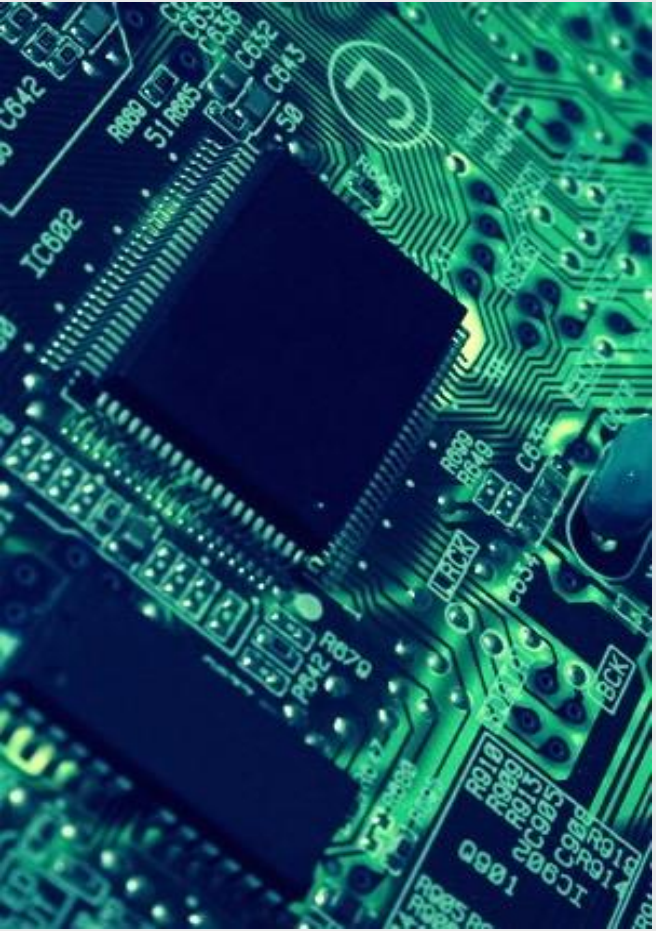
EC - Critical Infrastructure Directive 2008/114/EC

- 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

EC - 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

EC - 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