



European Union Agency for the Cooperation
of Energy Regulators

ACER Webinar on its Proposal for a Framework Guideline to Establish a Network Code on Cybersecurity

27 May 2021

9.30 – 12.00 CET

Online webinar

Public information

Opening

9:30 – 9:40

Christian Zinglensen, Director, ACER

AGENDA

09.20 - 9.30	Dial-in time	Starts promptly at 9.30
9.30 - 9.40	Opening	Christian Zinglensen, Director, ACER
9.40 - 11.05	Contents of the Framework Guideline: <ul style="list-style-type: none"> • Presentation on the Framework Guideline’s contents Øyvind Toftegaard, Seconded National Expert, ACER • Questions from the audience 	
11.05 - 11.15	Coffee break	
11.15 - 11.55	FG/NC Process: <ul style="list-style-type: none"> • Presentation on the Framework Guideline’s timeline Uros Gabrijel, Team Leader, System Operation & Grid Connection, ACER • Presentation on the adoption procedure for the Network Code Carina Carrillo Loeda, Legal Officer, European Commission • Presentation on the ENTSO-E/EU DSO preparatory work for the Network Code Andrea Foschini, Project Lead, ENTSO-E • Questions from the audience 	
11.55 - 12.00	Closing	Christophe Gence-Creux, Head of the Electricity Department, ACER

- Please be kindly reminded that your **mic is muted** throughout the webinar.
- Please keep your **video turned off** during the webinar.
- You may pose **questions via chat during the presentations**; all attendees will view all the questions.
 - After the agenda-items we will select relevant questions from the chat and ask presenters to address them.
- The slide pack will be shared with you after the webinar via email and on the ACER website.

The Framework Guideline's contents

9:40 – 11.00

Øyvind Toftegaard, Seconded National Expert, ACER

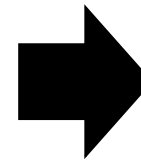
Part	Topic
Introduction	Cross border cybersecurity risk
Background	Legislation, preparatory work and ACER's role
Contents of the Framework Guideline	Measures proposed in the FG
Conclusion	Key takeaways and follow up
Q&A	Answering questions

Introduction

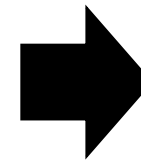
Cross border cybersecurity risk

The shift from physical to cyber risk

With the green shift and the technological development follows more complex ways to operate electric grids and the energy market.



The result is more effective and environmental friendly operation, but also more digital vulnerabilities and cyber-threats.



The modern electric grid, like the internet, is not limited by national borders. And so are threat actors.

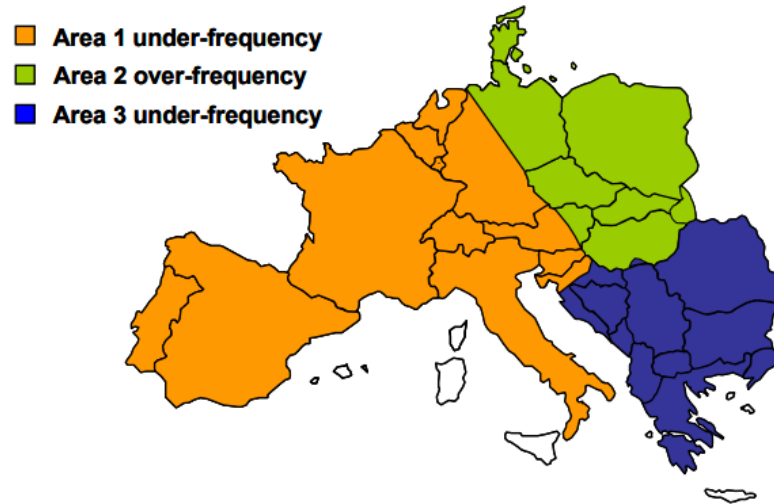


Cross border electricity cybersecurity risk



2003: Cascading effect of blackout in France and Switzerland led to blackout in Italy

-reigai.com



2006: Cascading effects of blackout in Germany led to blackout in several European countries

-entsoe.eu

 REUTERS

Ukraine's power outage was a cyber attack: Ukrenergo



2015: Digital attack led to blackout in Ukraine



2020: Digital attack assumed cause of blackout in India

Background

Legislation, preparatory work and ACER's role

To deal with cyber risk in general, EU has issued and proposed several regulations, such as:

- **The General Data Protection Regulation (2016)**
- **The Network and Information Security Directive (2016)**
- **The Network code on electricity emergency and restoration (2017)**
- **The Cybersecurity Act (2019)**
- **The Risk Preparedness Regulation (2019)**
- **The Directive on the resilience of critical entities (proposed 2020)**
- **The Network and Information Security Directive 2.0 (proposed 2020)**

Article 59, paragraph 2 of the Electricity Market Regulation (2019) empowers the Commission to adopt a delegated act to establish a network code on:

“sector-specific rules for cyber security aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management”

11 Feb – 14 May 2020, the Commission consulted stakeholders on the priorities for the development of network codes and guidelines for the period 2020-2023 in electricity:

“the results show[ed] strong support for the development of a network code for cybersecurity with 23 out of 27 stakeholders in favour”

On 28 January 2021, the Commission invited ACER to start drafting a framework guideline for the network code pursuant to Article 59, paragraph 4 of the Electricity Market Regulation, requesting:

“non-binding framework guidelines setting out clear and objective principles for the development of network codes relating to the areas identified in the priority list”

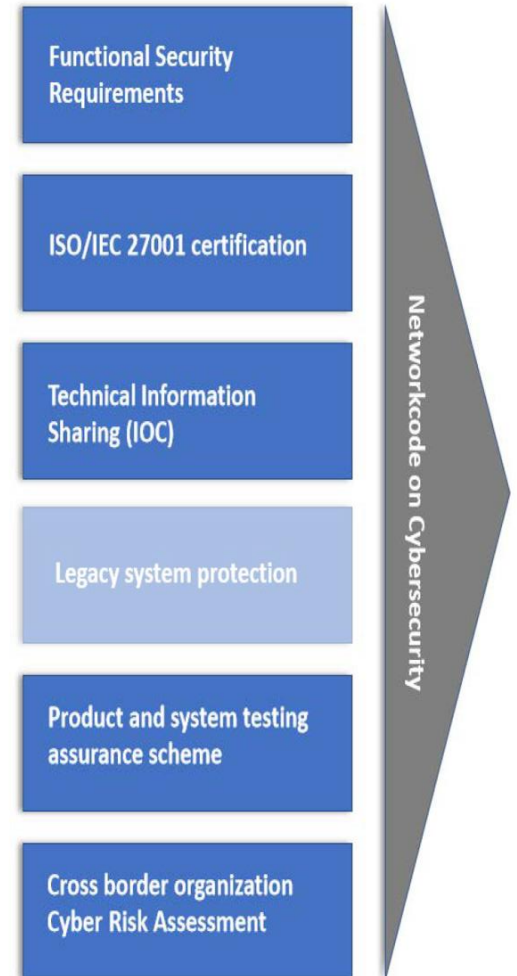
“Each framework guideline shall contribute to market integration, non-discrimination, effective competition, and the efficient functioning of the market”

Letter to ACER from the Commission

High-level objectives	Detailed main objectives	Additional objectives	Topics and work to consider
How to protect the energy systems based on current and future threats and risks	Clear scope and define entities to be subject to the NC	Crisis management	Real-time requirements of energy infrastructure components
How to support the functioning of the European society and economy in crisis situation	Governance for cybersecurity of cross-border electricity flows	Supply chain security	Cascading effects
How to create trust and transparency for cybersecurity in the supply chain for components and vendors used in the energy sector	Cross-border cybersecurity risk assessments	Joint exercises	Legacy and state-of-the-art technology
How to harmonise maturity and resilience for cybersecurity across EU with defined minimum level while favouring higher maturity	Uniform approach (rules) to mitigate identified cross-border risks	Peer reviews	Smart Grid Task Force Expert Group 2 report
	Minimum cybersecurity controls and requirements	Inspections	ENTSO-E/ DSO associations informal interim report
	Address supply chain and legacy technology risks	Coordinated inspections in the event of an incident	Revised NIS Directive
	Framework for effective sharing of security information	Other means of enhanced cooperation on cybersecurity	New Directive on the resilience of critical entities
	Cybersecurity maturity framework to assess implementation status		

Recap on work on the Framework Guideline

- **2019:** Smart Grid Task Force Expert Group 2 report
- **2020:** ENTSO-E/ DSO associations informal interim report
- **28 Jan 2021:** Invitation to ACER to draft framework guideline
- **4 Feb 2021:** Call for experts to the SOGC+ TF
- **Various dates:** Various meetings/updates
- **26 Apr 2021:** Request for comments on the Draft FG to:
 - SOGC+ TF
 - ACER EWG
- **30 Apr 2021:** FG proposal on public consultation



Contents of the Framework Guideline

Measures proposed in the FG

- Public consultation FG document published 30 April (comments to be submitted latest 29 June)
- Main headlines of the FG proposal:
 - Purpose: Safeguard cross-border electricity flows through sector-specific cybersecurity rules
 - Why: Increase in volatile and distributed production, demand response and digitalization
 - Scope:
 - Electricity undertakings (as defined in the Electricity Directive),
 - ENTSO-E, EU-DSO, ACER, NRAs,
 - Risk Preparedness NCAs, Electricity CS NCAs, CSIRTs, SOCs,
 - RCCs, and
 - Essential Service Suppliers.

Main content of the Framework Guideline

	Small and Micro Enterprises <50 Employees & <10 Mill Eur	Important Electricity Undertakings Minimum Security Requirements	Essential Electricity Undertakings Advanced Security Requirements
Basic cyber hygiene	Yes	Implicit	Implicit
Identification of critical products and processes		Yes	Yes
3-level risk assessment		Yes	Yes
Evaluation of critical assets and risks		Yes	Yes
Common security framework including verification of implemented requirements		Yes	Yes
Establish SOC or engage with MSSP		Yes	Yes
Security certification of essential products			Yes
Participation in cyber exercises			Yes

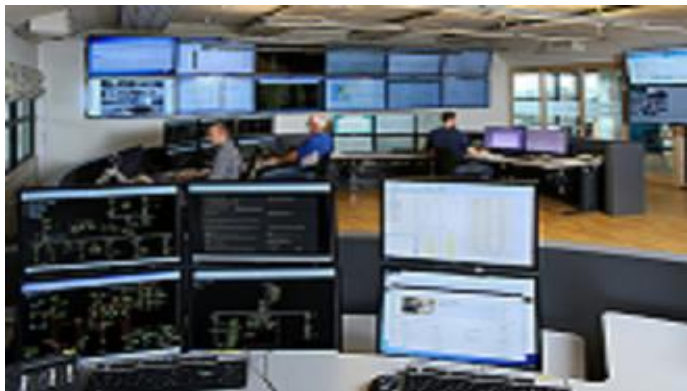
Asset inventory and cross border risk assessment (I)



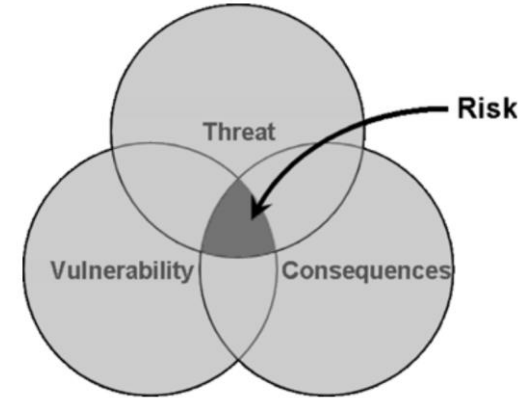
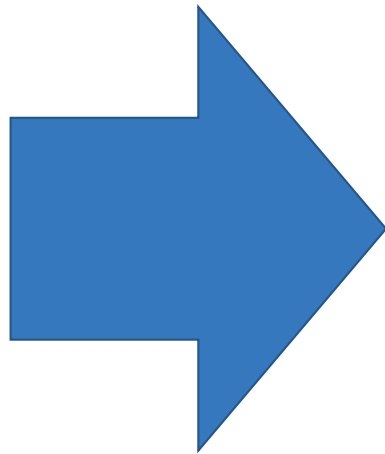
-electrical-engineering-portal.com



-ba.no



-tussa.no



		IMPACT LEVEL		
		Low	Medium	High / Very High
Threat Occurrence Probability	Low	Low Risk	Medium Risk	High Risk
	Medium	Low Risk	Medium Risk	High Risk
	High	Medium Risk	High Risk	High Risk

Legend



3 risk assessment levels:



1. Asset inventory and cybersecurity perimeter



European
waterfalls.com

2. Potential trans-national cybersecurity incident or attack scenarios



3. Scenarios that would likely disturb or impede cross-border electricity flows



Results shall be consolidated in a Cross-Border Electricity Cybersecurity Risk Assessment Report

Apply Electricity Cybersecurity Risk-Index (ECRI) Caps to classify Important and Essential Electricity Undertakings

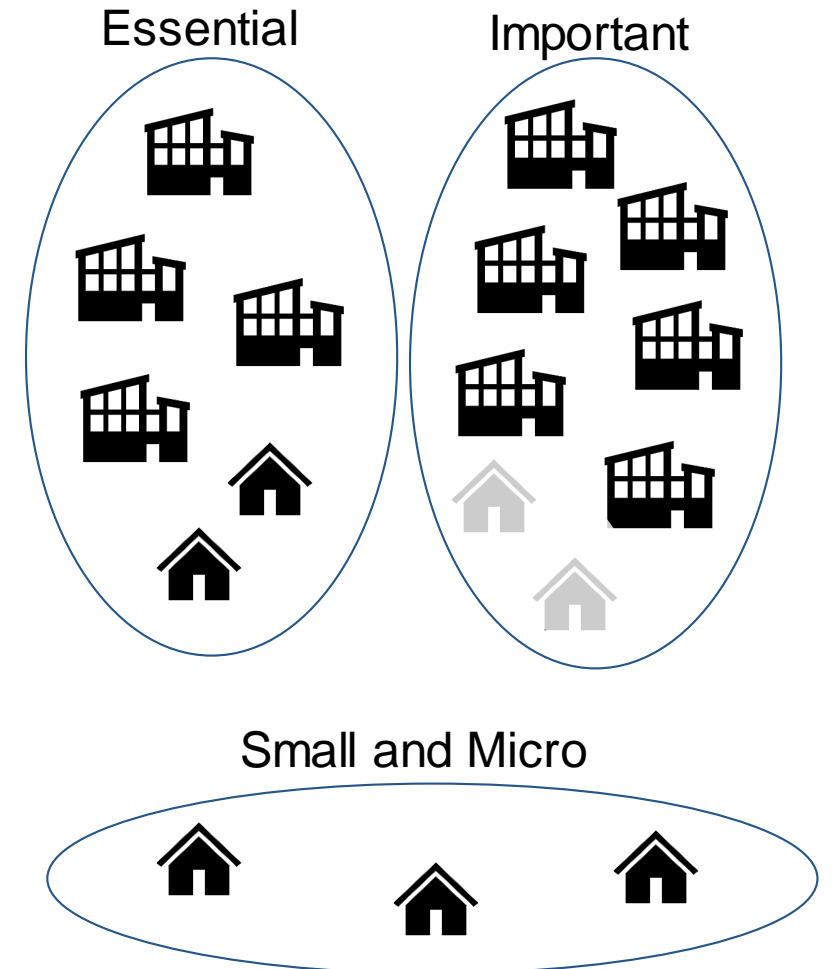
- ECRI score based on information asset inventory and risk assessment

Transitional measures for the classification of entities

- Transitional list of Essential and Important Electricity Undertakings

Small and Micro enterprises may be classified too

- Primary as Essential Electricity Undertakings
- Classification of small and micro enterprises not subject to ECRI Cap



To deal with cyber risk in general, EU has issued and proposed several regulations, such as:

- **Within a period of three months from the entry into force of the network code and in absence of common cybersecurity rules:**
A transitional list of national regulations of electricity cybersecurity and EU/International standards to be implemented by the important electricity undertakings or essential electricity undertakings in preparation for the implementation of the minimum cybersecurity standard or advanced cybersecurity standard
- **All Member States and all Electricity Undertakings shall be consulted and participate in drafting the list of principles to be implemented as minimum and advanced cybersecurity requirements**

The implementation of the security requirements shall be verifiable

1.



Or Other
Certifiable
Standard

2.

Peer Review

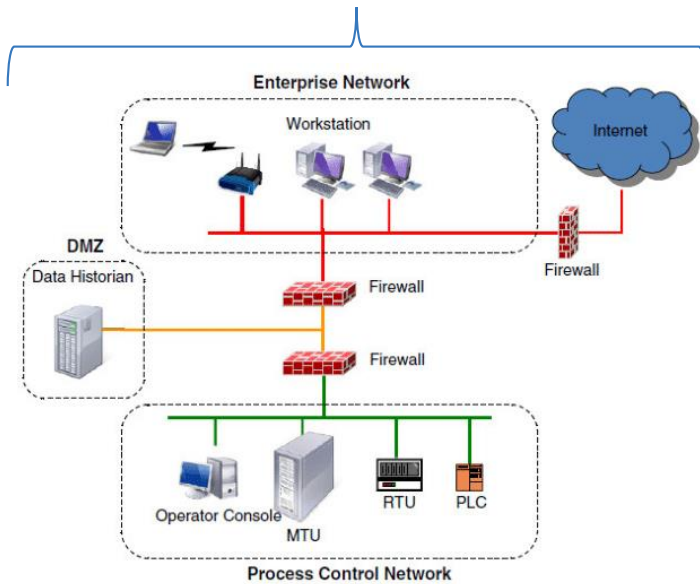
3.

Approved
National
Government
Schemes

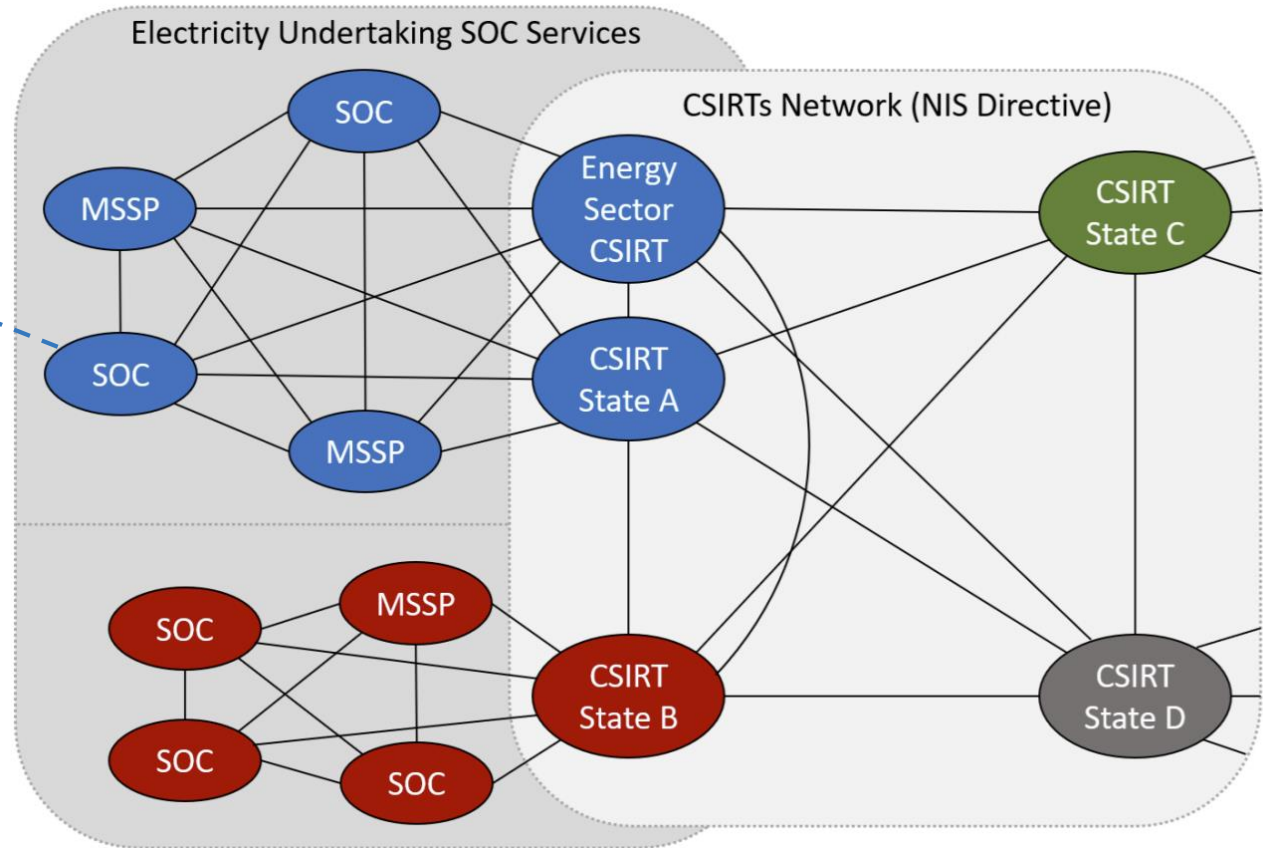
Information sharing, incident and crisis management



-mdscs.sa



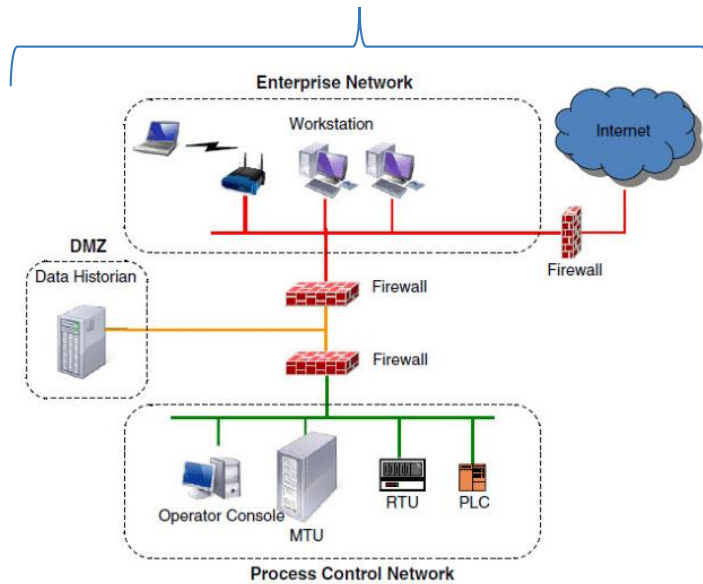
Rysavy, Ondrej & Rab, Jaroslav & Sveda, Miroslav. (2013)



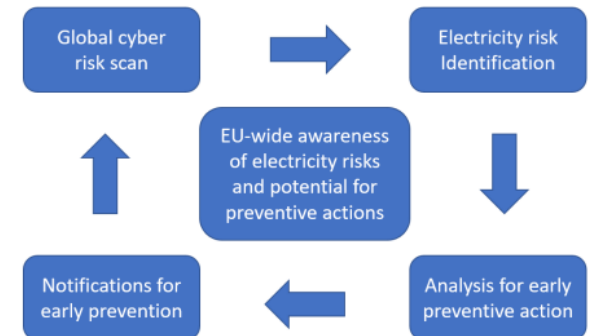
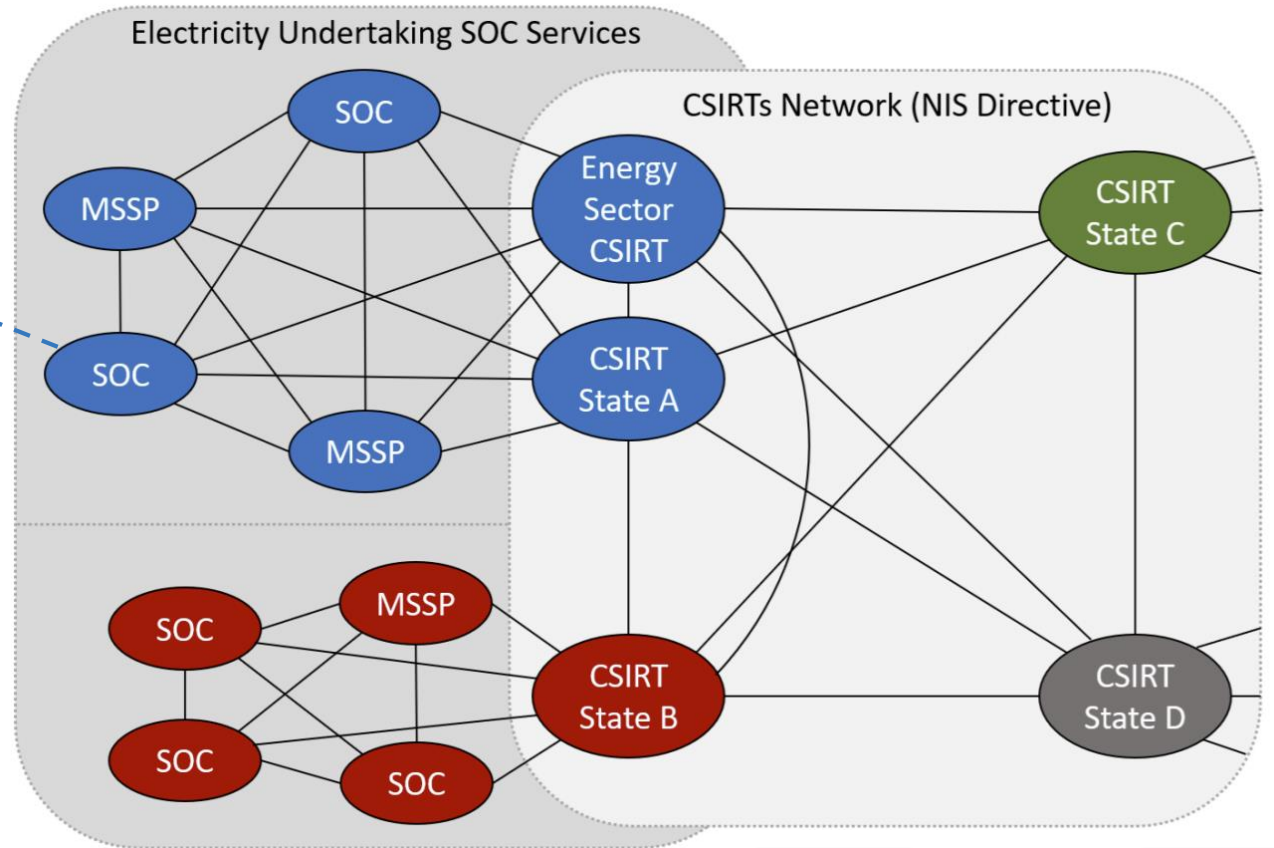
Information sharing, incident and crisis management



-mdscs.sa



Rysavy, Ondrej & Rab, Jaroslav & Sveda, Miroslav. (2013)





And Other
National
Schemes



Supply-chain security



+ Security requirements for essential
service suppliers

Participation in cyber exercises



-bladet.no



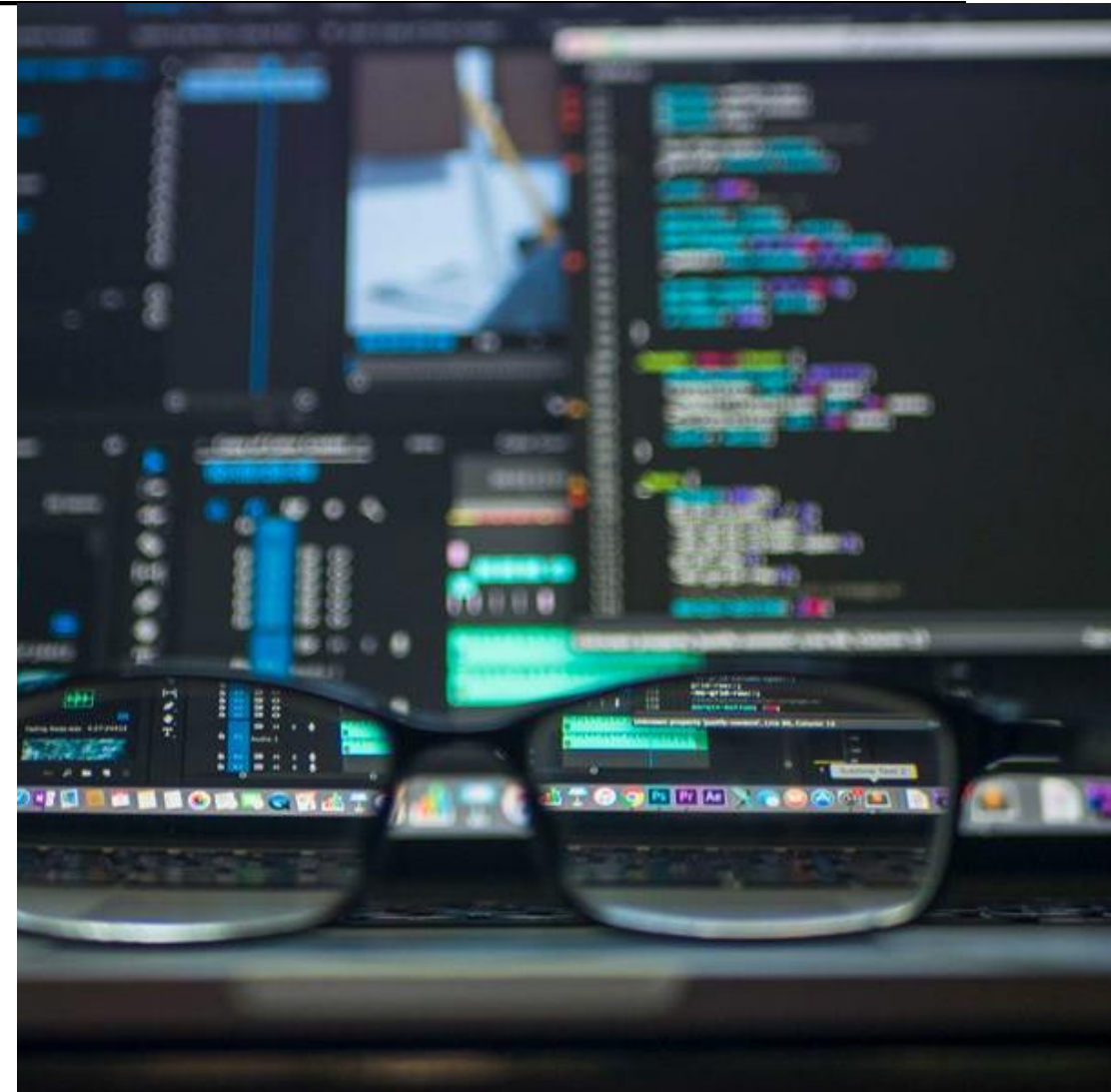
-tussa.no

An information protection scheme shall be established for protection of information exchanged in the context of the Network Code, including:

- **An information classification scheme**
- **General information protection rules**



- **Monitoring effectivity of security requirements**
By ACER, ENTSO-E and EU-DSO
- **Benchmarking with focus on cost-efficiency**
By ACER supported by NRAs
- **Reporting on security status and trends**
By ENTSO-E, EU-DSO and stakeholders



Conclusion

Key takeaways and follow up

- **June 2021:** More interaction with SOGC+ TF and ACER EWG
- **29 June 2021:** End of public consultation
- **July 2021:** Evaluation of responses and draft a final deliverable to the EC
- **July 2021:** EWG endorsement and BoR opinion before sending the FG to the Commission
- **Next steps:**
 - NC developed and consulted by ENTSO-E and EU DSO Entity
 - ACER goes through the proposed NC and sends recommendation to the commission
 - Comitology process and entry into force

-
- **We need sector specific cybersecurity legislation to prevent cross border cybersecurity risk**
 - **The FG will provide guidance to ENTSO-E and EU-DSO entity for the drafting process**
 - **The FG proposes mainly**
 - **Cybersecurity requirements for a wide scope of organisations**
 - **Cross border electricity cybersecurity risk assessment**
 - **A system for common cybersecurity requirements and its verification**
 - **A system for information sharing, incident- and crisis management**
 - **Advanced requirements in form certification of essential products and exercises**
 - **The next steps are to evaluate responses after the public consultation and draft a final deliverable**



Questions? –use the Q&A function



Was your question not answered? You can send us your questions:

DFG-NC-CS@acer.europa.eu



European Union Agency for the Cooperation
of Energy Regulators

 info@acer.europa.eu
 acer.europa.eu

 [@eu_acer](https://twitter.com/eu_acer)
 [linkedin.com/company/EU-ACER/](https://www.linkedin.com/company/EU-ACER/)

AGENDA

09.20 - 9.30

Dial-in time

Starts promptly at 9.30

9.30 - 9.40

Opening

Christian Zinglensen, Director, ACER

9.40 - 11.05

Contents of the Framework Guideline:

- **Presentation on the Framework Guideline's contents**
Øyvind Toftegaard, Seconded National Expert, ACER
- **Questions from the audience**

Coffee Break

11.05 - 11.15 **Coffee break**

11.15 - 11.55

FG/NC Process:

- **Presentation on the Framework Guideline's timeline**
Uros Gabrijel, Team Leader, System Operation & Grid Connection, ACER
- **Presentation on the adoption procedure for the Network Code**
Carina Carrillo Loeda, Legal Officer, European Commission
- **Presentation on the ENTSO-E/EU DSO preparatory work for the Network Code**
Andrea Foschini, Project Lead, ENTSO-E
- **Questions from the audience**

11.55 - 12.00

Closing

Christophe Gence-Creux, Head of the Electricity Department, ACER

The Framework Guideline's timeline

11.15 – 11.25

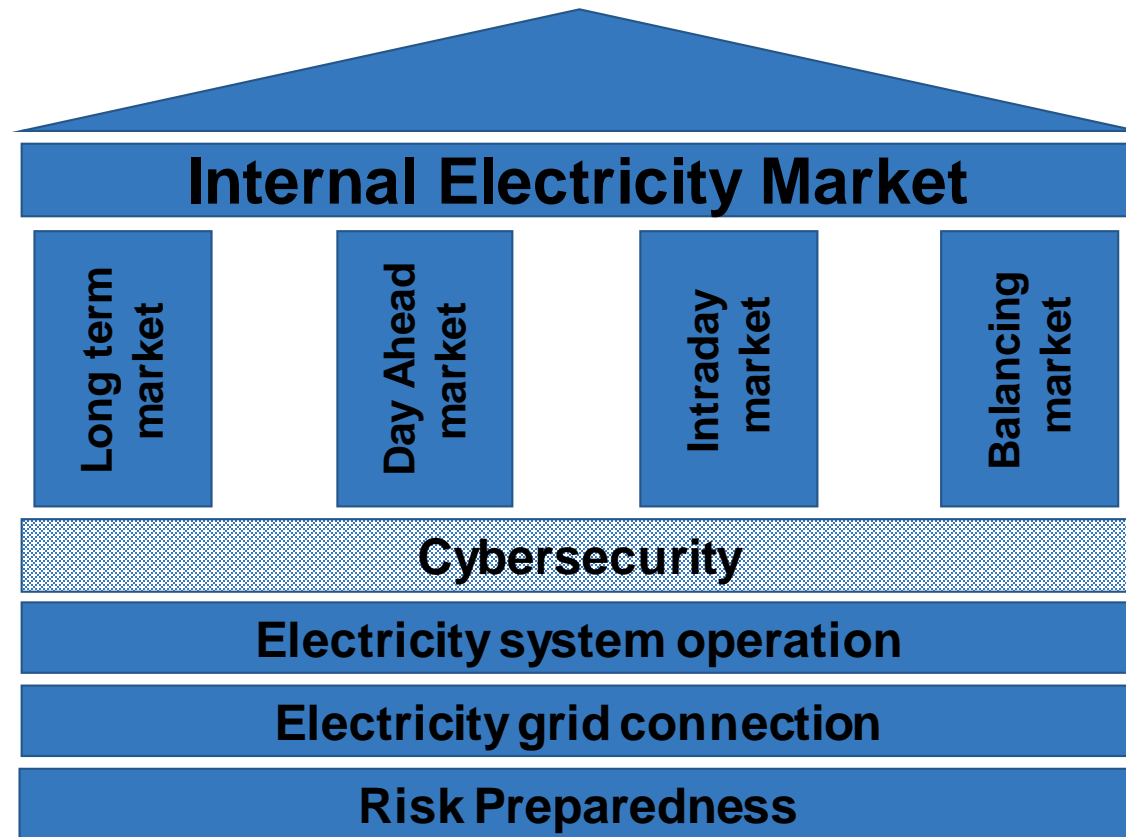
Uros Gabrijel, Team Leader, System Operation & Grid Connection, ACER

- Introduction
- Framework Guidelines / Network Codes – General Timeline
- Background
- Framework Guidelines on Cybersecurity - Formal Process

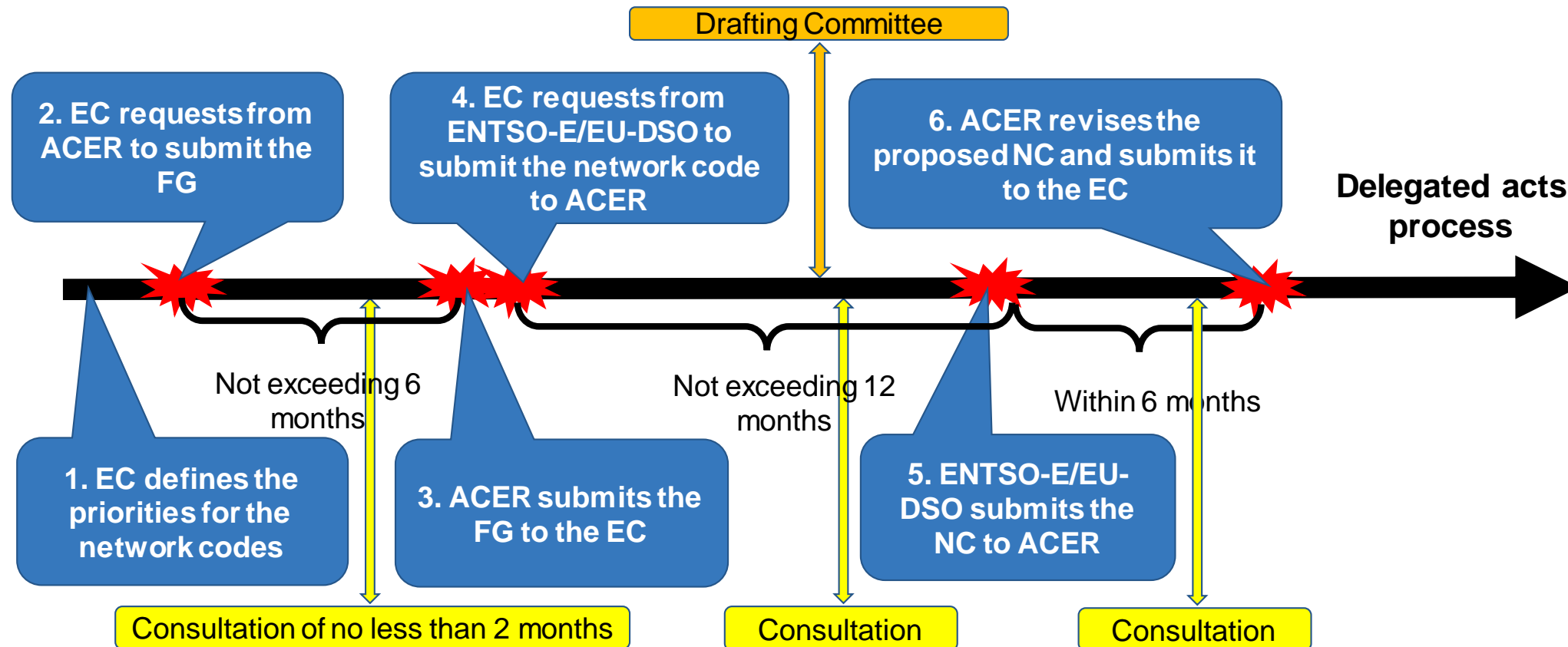
- Agency for the Cooperation of Energy Regulators
 - Regulation (EC) No 713/2009 established an Agency for the Cooperation of Energy Regulators (ACER)
 - A community body with legal personality
 - Purpose: “[...] to assist the regulatory authorities [...] in exercising at Community level the regulatory tasks [...] and to coordinate their actions”
 - Fully operational since March 2011

-
- Over time, ACER received additional tasks and responsibilities to better pursue the integration of the European Internal Energy Market
 - The latest provisions adopted in the [Clean Energy Package](#) (2019) strengthened ACER responsibilities regarding the coordination with NRAs and streamlined the development of the network codes by requiring ACER to revise proposed network codes before submitting them to the Commission

- ACER fosters a fully integrated and well-functioning Internal Energy Market



- General timeline as set out in Article 59 of [REGULATION \(EU\) 2019/943](#) (Electricity Regulation)



- Informal process
 - In 2019, the Smart grids task force expert group 2 published [recommendations](#) on the implementation of the Electricity Regulation
 - The Commission set up a drafting team of relevant stakeholders in February 2020
 - The [technical report](#) puts forward recommendations to the Commission and identifies areas that need to be addressed in the future network code on cybersecurity (February 2021)

- Formal invitation by the EC to draft the Framework Guidelines (FG): 28 January 2021
- [Public consultation](#) on ACER draft FG: from 30 April until 29 June 2021
- ACER to submit the non-binding FG to the EC within a reasonable period not exceeding six months upon the receipt of the invitation
 - The FG will be accompanied with Evaluation of responses to the public consultation

The adoption procedure for the Network Code

11.25 – 11.35

Carina Carrillo Loeda, Legal Officer, European Commission



ACER WEBINAR

Framework Guideline on Cybersecurity

27 May 2021

Commission delegated acts

Commission DA on Cybersecurity: Framework

- EMPOWERMENT: Article 59 (2) (e) EIM Regulation ((EU) 2019/943)
- Article 68 EIM Regulation + 2016 Interinstitutional agreement between EP/Council/Commission on Better Law Making.

Commission DA on Cybersecurity: Specificities for acts prepared by agencies

- Commission services drafting ex-novo v. draft received by Commission from Agencies (ACER).
- Implications for the adoption process of the delegated act by Commission.

Commission DA on Cybersecurity: Member States'/Council's/Parliament's experts (I)

- Commission involves experts through EXPERT GROUPS– up to MS to decide on experts sent. Electricity coordination group (includes also ACER/ENTSO-E/NRAs)
- Council and Parliament must receive all documents and invitations to meetings and be able to send experts.

Commission DA on Cybersecurity: Member States'/Council's/Parliament's experts (II)

- Role of the EXPERT GROUP:
 - No voting, not binding.
 - Closely taken into account by Commission-control by Council and Parliament via objection period.

Commission DA on Cybersecurity: Timing – after ACER's draft (I)

- Interservice consultation within the Commission.
- Send draft to expert group (number of meetings?): invitation +/-30 days before meeting; and documents (draft DA) 14 days before.
- 4 week public feedback? – Exceptions – if wide stakeholder consultation by Agency, avoid duplication.

Commission DA on Cybersecurity: Timing – after ACER's draft (II)

- Translation: depends on the length of document.
- Commission adoption by Written procedure.
- Transmission to EP/Council: Objection period: 2 months (+ 2 eventually or sooner if expression of no objection)
- OJ publication and entering into force.

Thank you

Carina Carrillo Loeda – Unit A5 DG ENER – Planning and legal affairs

The statements in this Power Point Presentation do not necessarily reflect the official views of the Directorate General for Energy or of the European Commission and, therefore, are not binding on them.

© European Union 2020

Unless otherwise noted the reuse of this presentation is authorised under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license. For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.



ENTSO-E/EU DSO preparatory work for the Network Code

11.35 – 11.45

Andrea Foschini, Project Lead, ENTSO-E

Network Code on Cybersecurity

27th May, Webinar: ACER Framework Guidelines



The network code on Cybersecurity aims to define a set of rule to strengthen the energy sector



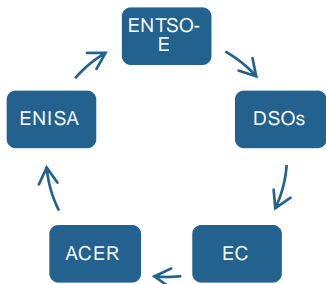
Togetherness & Strong Collaboration



Tailor Made for the Energy Sector



Promotes Security by Design



Strong Pool of Expertise



Timeline

Informal process lead by the European Commission

Since February 2020, an informal drafting team composed by ENTSO-E and four associations representing the DSO communities (GEODE, EURELECTRIC, CEDEC, E.DSO), under the leadership of EC, work on a set of focus areas for the Network Code on Cybersecurity.

- **19th February 2021** – delivery of the Final Interim Report to the EC
- **18th April 2021** – The EC published the Final Interim Report

Report: <https://europa.eu/!Xj84GG>

Web: <https://europa.eu/!JR39PR>

Formal process

- **June 2021** – EU DSOs Association operational
- **27th July 2021** – Starting of the Formal Drafting Process



Questions? –use the Q&A function



Was your question not answered? You can send us your questions:

DFG-NC-CS@acer.europa.eu



European Union Agency for the Cooperation
of Energy Regulators

 info@acer.europa.eu
 acer.europa.eu

 [@eu_acer](https://twitter.com/eu_acer)
 [linkedin.com/in/EU-ACER/](https://www.linkedin.com/in/EU-ACER/)



Closing



11.55 – 12.00

Christophe Gence-Creux, Head of the Electricity Department, ACER



European Union Agency for the Cooperation
of Energy Regulators

 info@acer.europa.eu
 acer.europa.eu

 [@eu_acer](https://twitter.com/eu_acer)
 [linkedin.com/in/EU-ACER/](https://www.linkedin.com/in/EU-ACER/)