POLICY
TECHNOLOGY
MARKET

ENERGY STORAGE

Global Conference

Brussels, 14-16 October 2025

2025

Session 2.8 Why Cybersecurity Matters for your Projects: Responsibilities and Obligations?

POLICY TECHNOLOGY MARKET
ENERGY STORAGE Global Conference
Brussels, 14-16 October 2025

Michaela Kollau
European Commission

Maarten Hoeve
European Network for Cyber Security

Aakash Sharma
Sungrow

Stéphane Alaimo
Saft

Moderator:

Patrick Clerens
Secretary General / Energy Storage Europe

Session 2.8 Why Cybersecurity Matters for your Projects: Responsibilities and Obligations?

Michaela Kollau

Policy Officer

European Commission

Cybersecurity in the energy sector

Energy Storage Global Conference 2025

Michaela Kollau, European Commission, DG ENER,
Unit F4: Energy security and safety
15 October 2025

European Commission

Cybersecurity in the energy sector

A policy perspective

EU’s horizontal Security Framework

Critical Entities Resilience Directive (CER)

NIS 2 Directive

Cyber Resilience Act (CRA)

Cybersecurity in the energy sector

- **Cybersecurity Network Code for cross-border electricity flows**
- **NZIA – implementing Act on criteria on cybersecurity in auctions for RES**
- **Risk assessment related to wind energy – Action#5 of the European Wind Power Action Plan**
- **Risk assessments related to solar**

COMMISSION IMPLEMENTING REGULATION (EU) 2025/1176

of 23 May 2025

specifying the pre-qualification and award criteria for auctions for the deployment of energy from renewable sources

Article 5

Cybersecurity and data security (pre-qualification criteria)

Pre-qualification criteria related to cybersecurity and data security shall require bidders to:

(a) take appropriate and proportionate technical, operational and organisational measures that reflect the principles of security by design and by default to ensure the security of the renewable energy installation's network and information systems including, where relevant, measures listed in Article 21(2) of Directive (EU) 2022/2555;

(b) where, 9 months or more before the publication of an auction within the scope of Article 26 of Regulation (EU) 2024/1735, the bidder is subject to the jurisdiction of a third country requiring the bidder to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited or there is a public statement on behalf of the Union or the Member State carrying out the auction that threat actors operating out of the territory of that third country have carried out malicious cyber activities or campaigns, present a cybersecurity plan outlining how the bidder guarantees the security of the installation and of the overall system and more specifically take the necessary technical, operational and organisational measures to ensure that data used for or generated in their business activities related to the auction are stored in and not transferred outside the European Economic Area;

(c) ensure and demonstrate, where the bidder relies on suppliers for the supply of ICT products used in the renewable energy installation or ICT services related to its operation, that the suppliers take the measures referred to in point (a) and where those suppliers meet any of the two conditions set in point (b) for bidders, that those suppliers also take the measures referred to in point (b);

(d) ensure that an operator established in the European Economic Area maintains operational control of the installation.

Review energy security framework

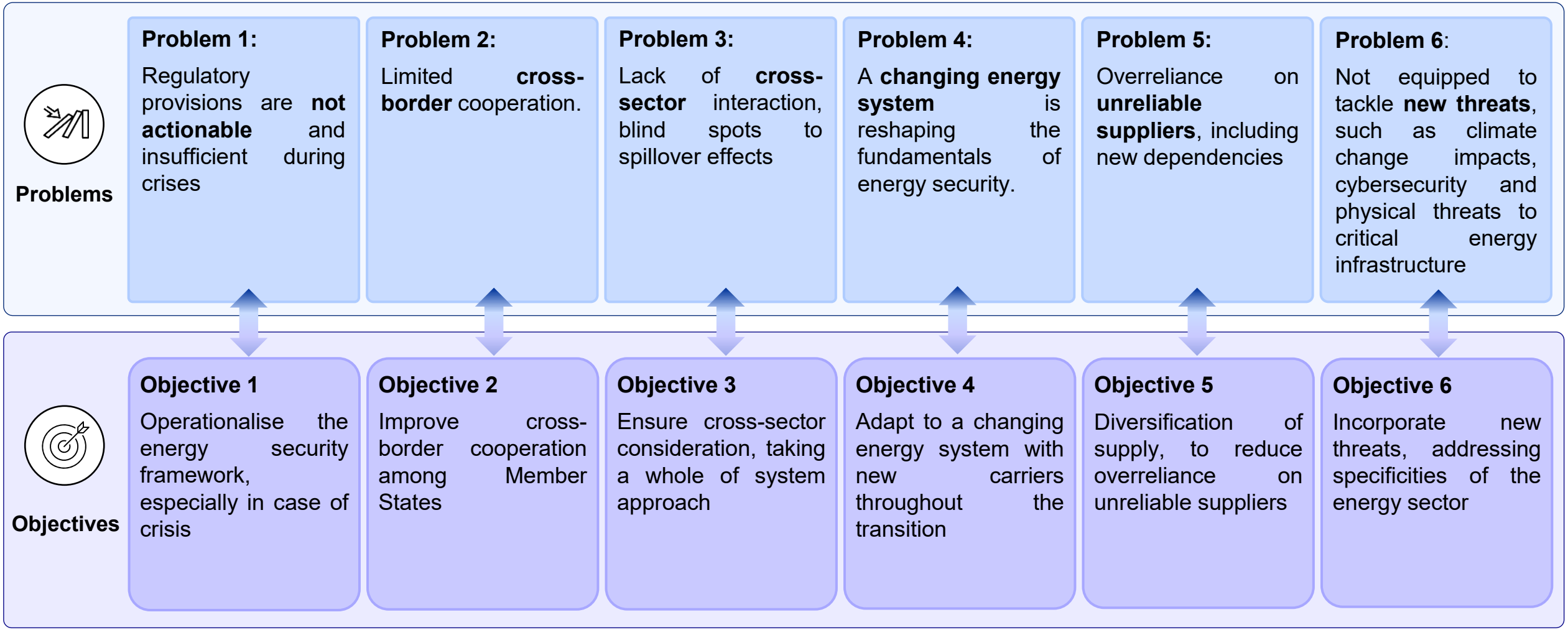
Status update

Why a revision?

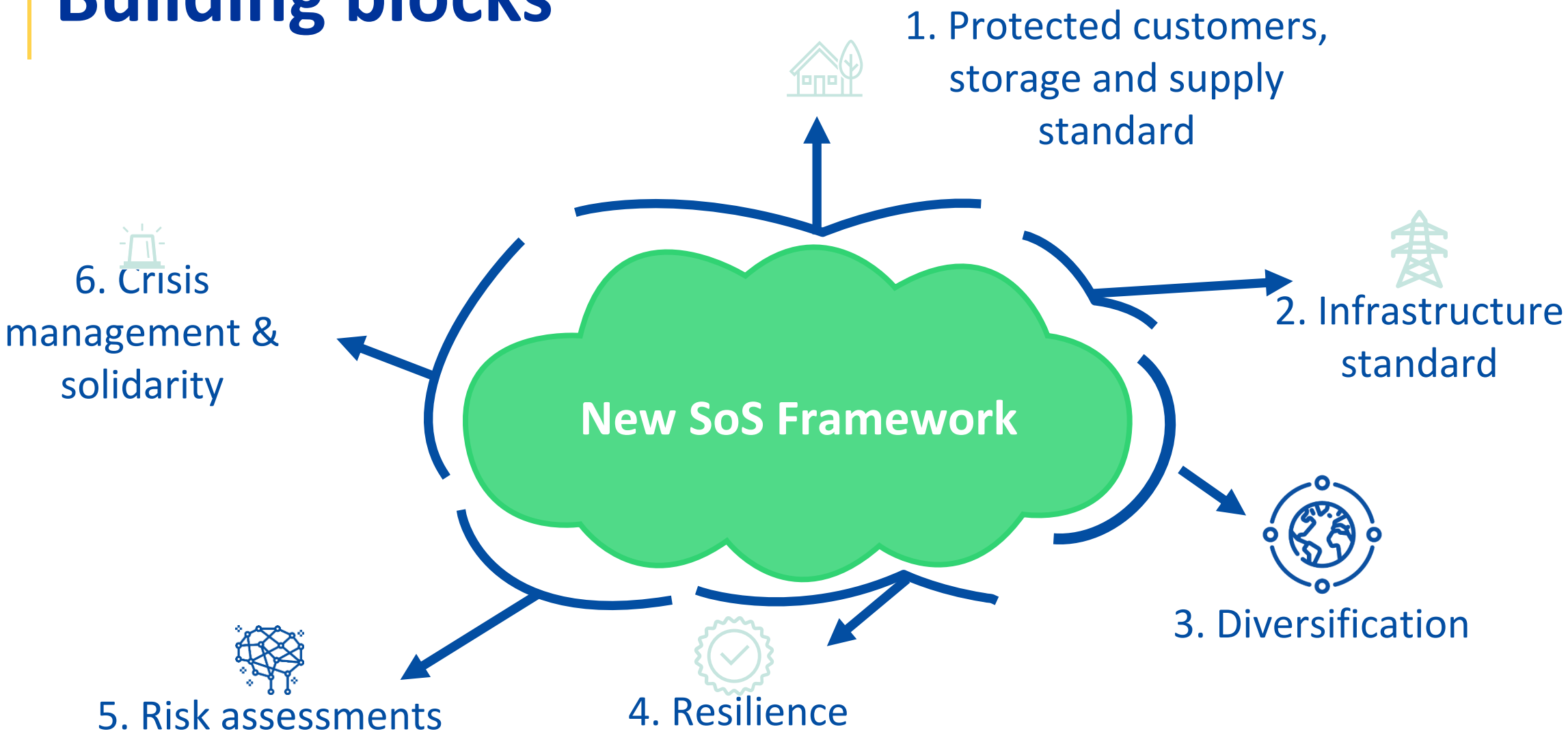
Main reasons to act: emerging challenges and weaknesses

- → Competitiveness
- → Cumbersome framework
- → Lack of cross-sector interaction
- → Limited cross-border cooperation
- → A changing energy system
- → Climate change adaptation
- → New threats (cyber and physical)
- → Dependencies and geopolitical turbulences

Problems and objectives



Building blocks



Timeline

Sep-Nov 2024

Fitness check - Public consultation

Call for evidence for legislative proposal

Sept - Oct 2025

29 Sept 2025

Stakeholder workshop

Joint ECG-GCG on the revision

9 Oct 2025

Oct 2025

End of consultant's study

Adoption of the legislative proposal

1st half 2026

Fill in copyright information.

Thank you

Session 2.8 Why Cybersecurity Matters for your Projects: Responsibilities and Obligations?

Marteen Hoeve

Director Technology

European Network for Cyber Security

Risk: disruption of grid through storage

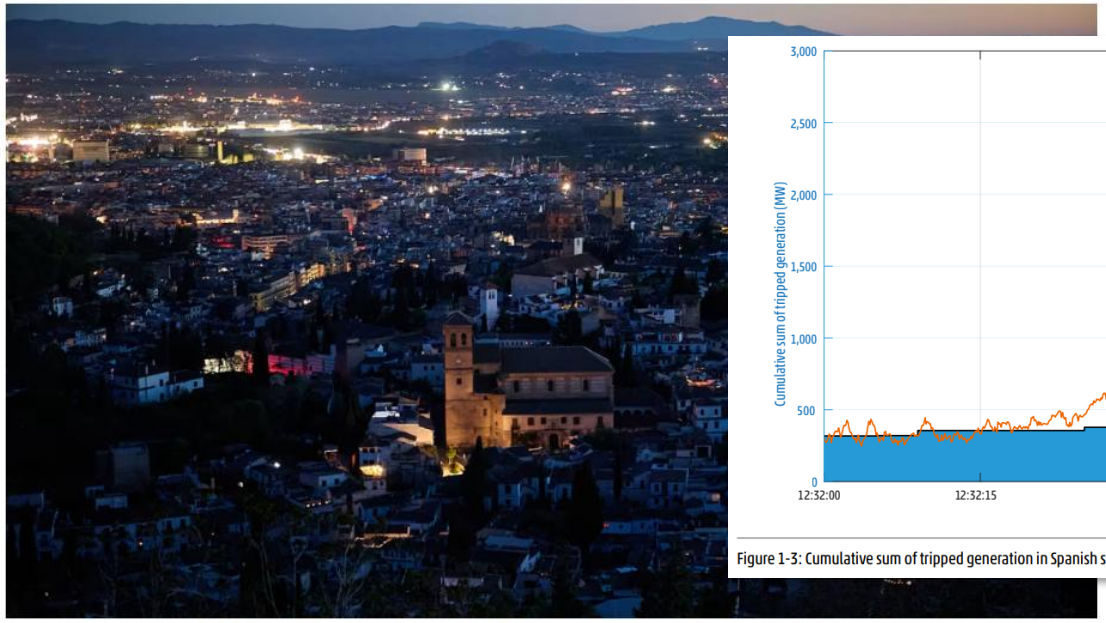
CNN World Sign In

World / Europe

Spain says April blackout was caused by grid failures and poor planning, not a cyberattack

Story by the Associated Press

3 min read · Updated 9:09 PM EDT, Tue June 17, 2025



A general view of the city of Granada, with the Alhambra, is plunged into darkness during the power outage that affects Spain nationwide in Granada, Spain on April 28, 2025. Fermin Rodriguez/NurPhoto/Getty Images

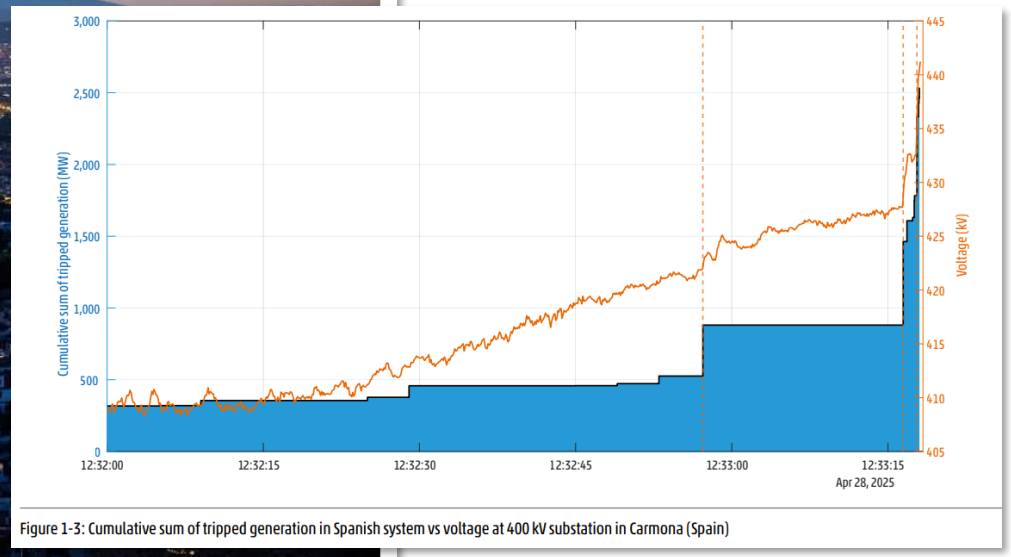


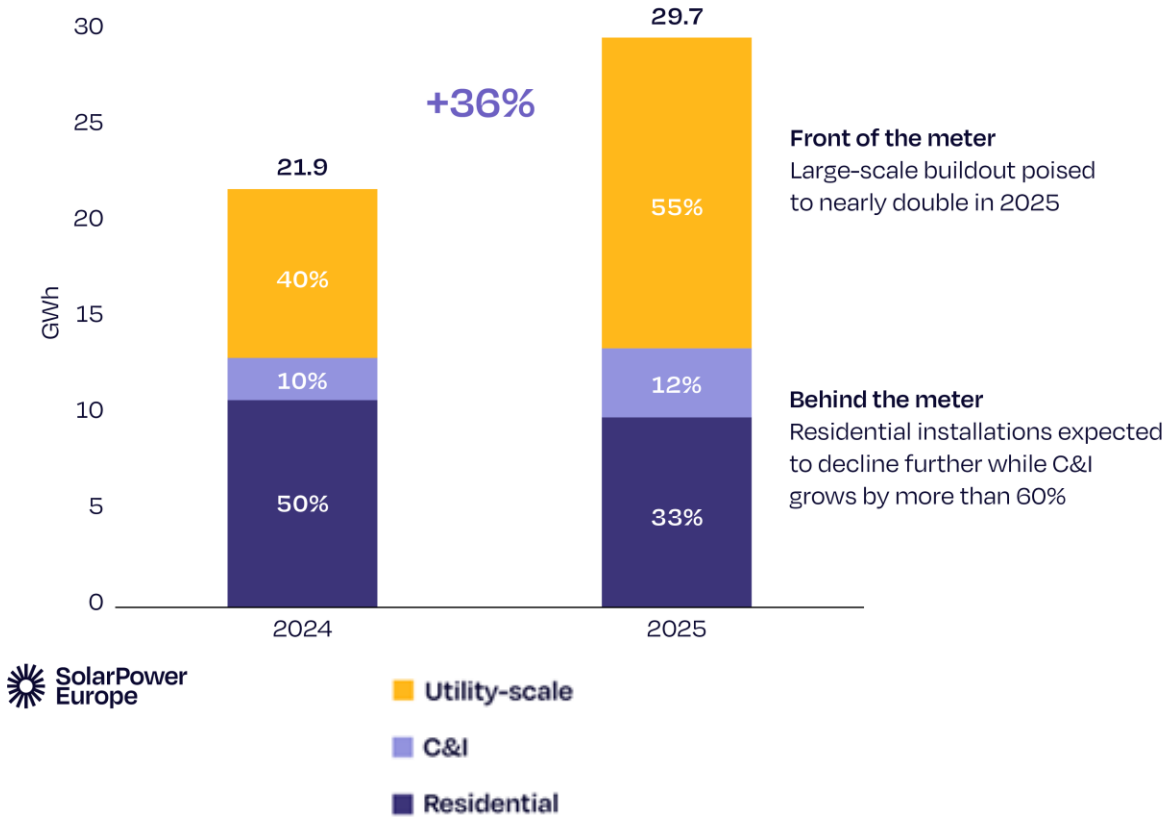
Figure 1-3: Cumulative sum of tripped generation in Spanish system vs voltage at 400 kV substation in Carmona (Spain)

Source: ENTSO-E

Mitigation: segmented approach

European annual battery market expansion set to speed up again in 2025, driven by utility-scale

Europe annual BESS installed capacity 2024-2025



- Mitigated as for traditional utilities
- Covered by NIS2 / NCCS

- To be mitigated by manufacturers
- Gaps in legislation

Session 2.8 Why Cybersecurity Matters for your Projects: Responsibilities and Obligations?

Aakash Sharma

Product Certification Manager

Sungrow

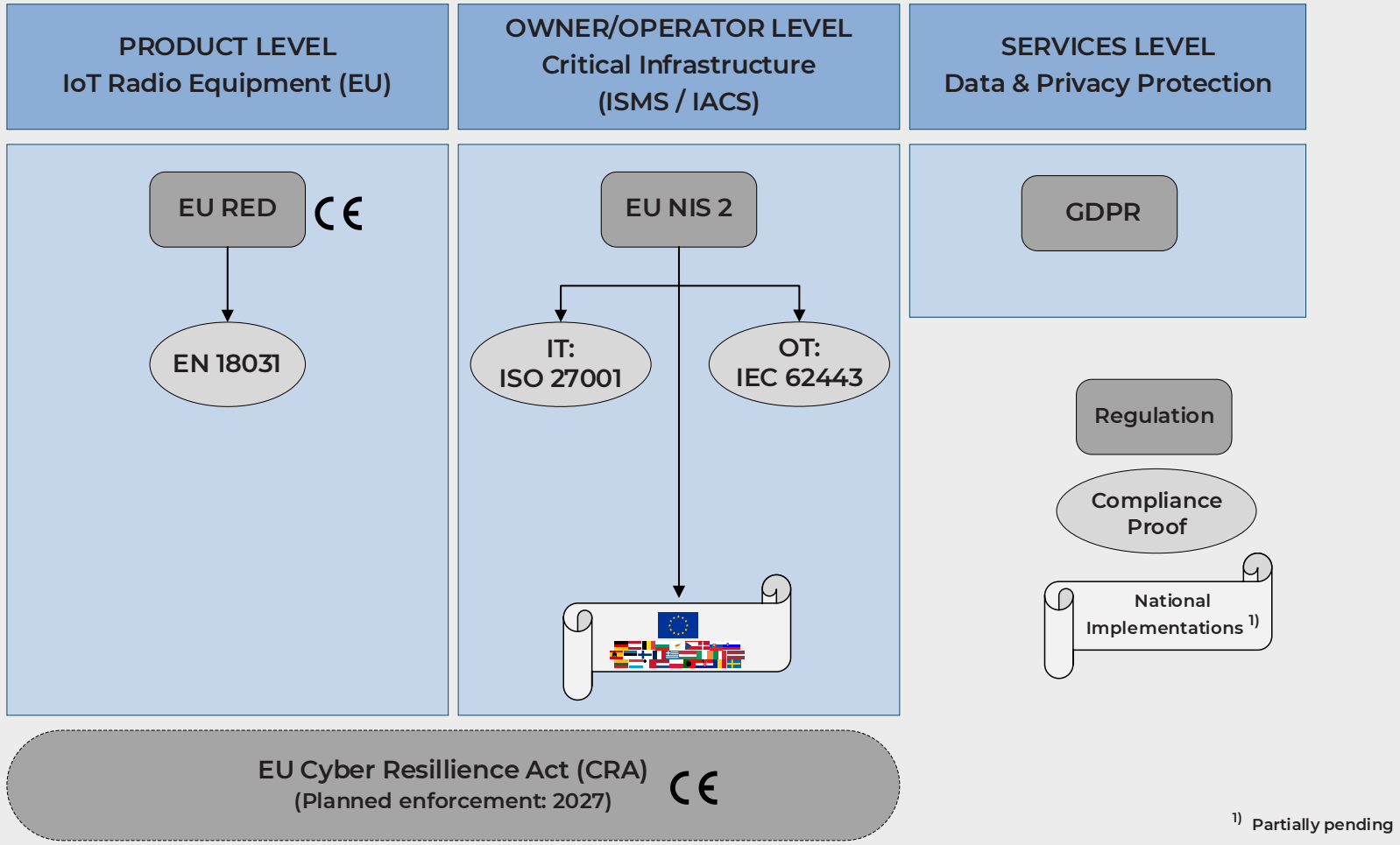
SUNGROW
Clean power for all

POLICY TECHNOLOGY MARKET

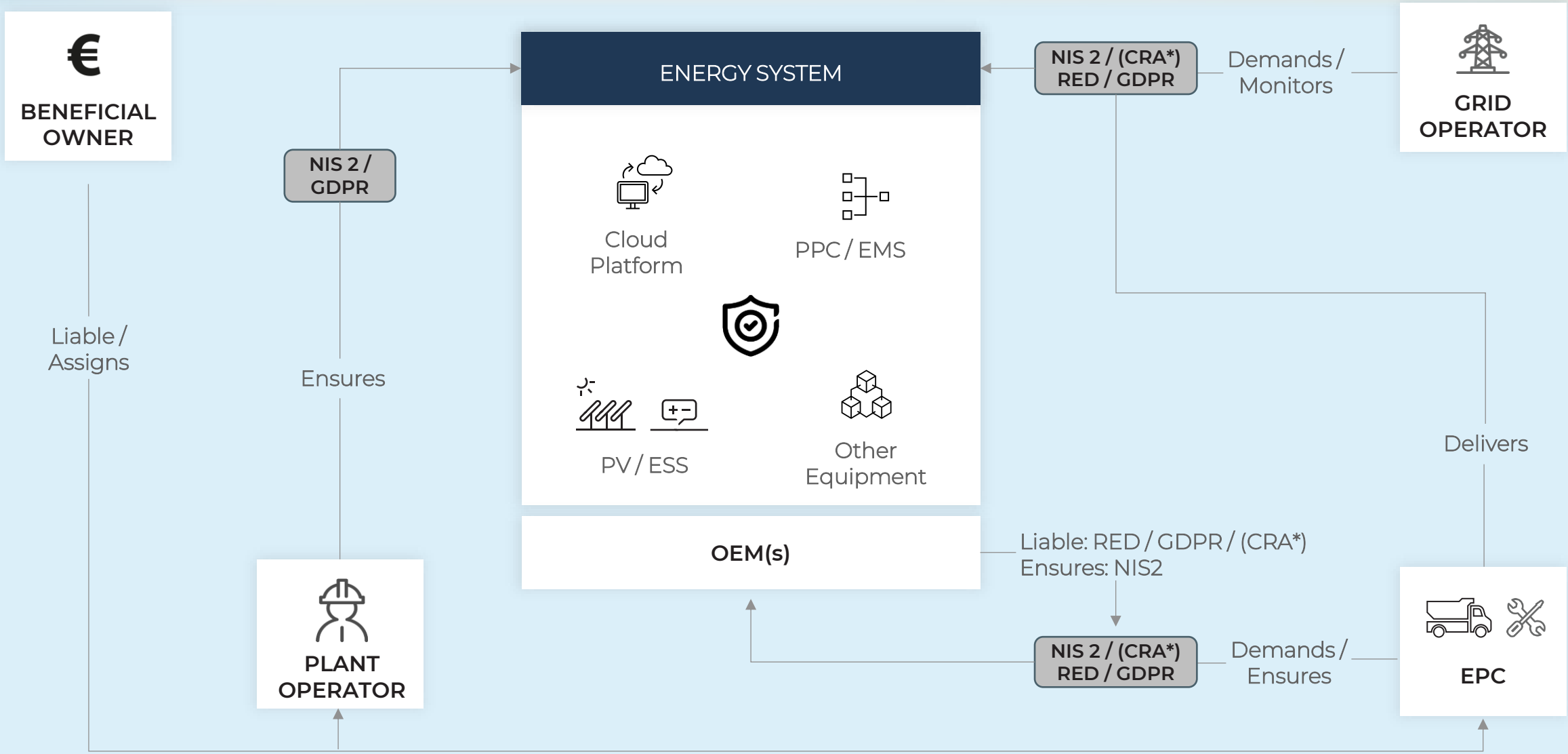
ENERGY STORAGE Global Conference
Brussels, 14-16 October 2025

Contents

Cyber Security Regulations



Stakeholder Obligations



* Planned enforcement of CRA: 2027

Key Regulatory Challenges

Regulatory Overlap	• Intersecting Scope • Duplicated Compliance Efforts
Divergent National Implementation & Enforcement	• Varying Thresholds • Patchwork of Rules Management
Fast Innovation vs Slow Regulatory Processes	• The Speed Mismatch • Evolving Technology

POLICY
TECHNOLOGY
MARKET

ENERGY STORAGE
Global Conference
Brussels, 14-16 October 2025

THANK YOU!

a.sharma@sungrow-emea.com

www.linkedin.com/in/aakasharma1/

Session 2.8 Why Cybersecurity Matters for your Projects: Responsibilities and Obligations?

Stéphane Alaimo

Head of Digital Product Developments

Saft

POLICY TECHNOLOGY MARKET

ENERGY STORAGE Global Conference

Brussels, 14-16 October 2025

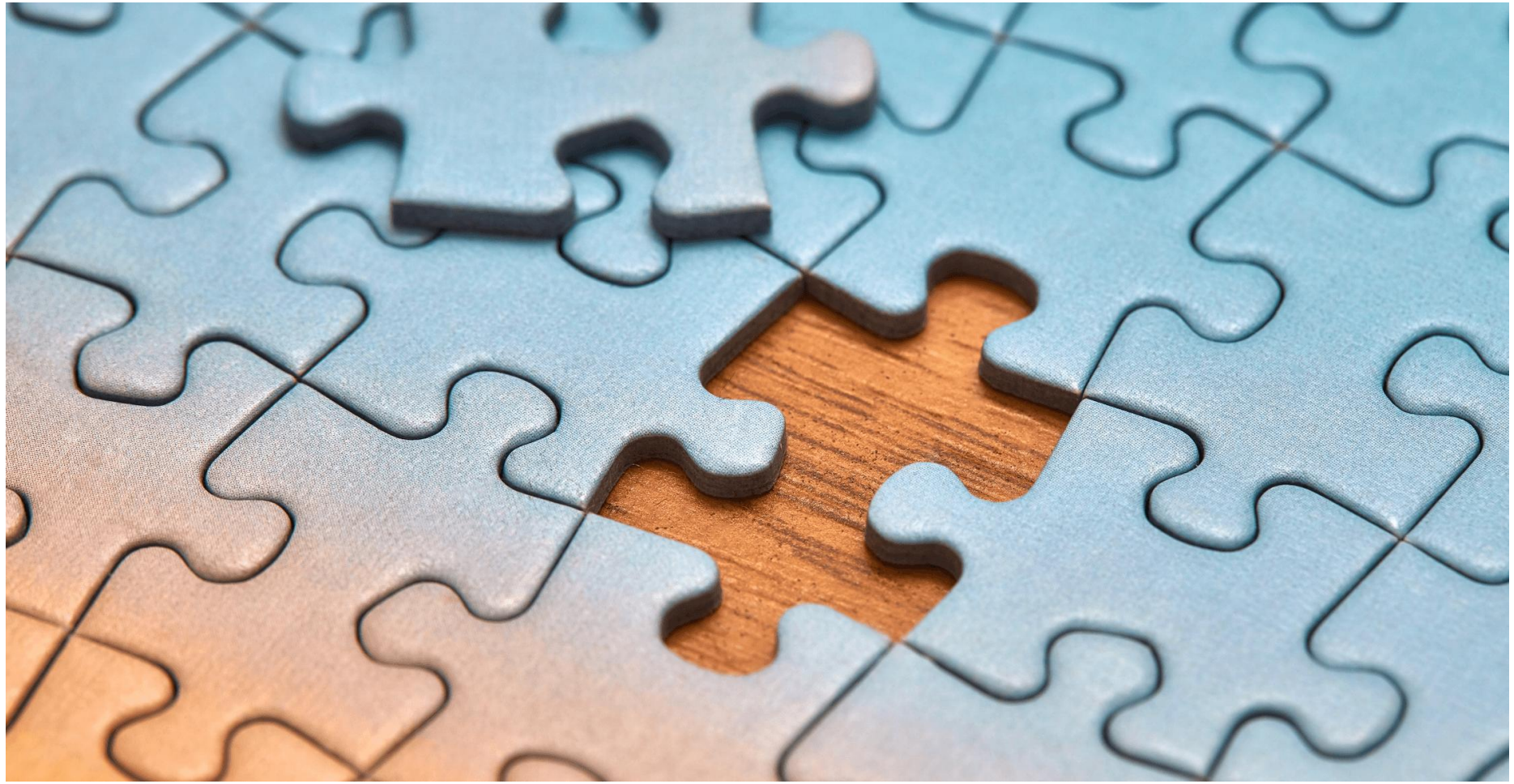
TotalEnergies

The path to Battery Security in Europe

ESGC Brussells
October 2025
Stéphane ALAIMO

saft

The missing piece of the puzzle



Battery systems are critical infrastructure

- The European grid won't survive without energy storage
- Batteries systems are connected digital systems
- Cyber-threats on electricity networks are booming

Regulatory Timeline – USA vs Europe

United State

- 2008: **NERC CIP** : comes into force for bulk connected
- 2014: **NISTIR 7628** Guidelines for Smart Grid Cybersecurity
- 2016: NERC CIP : Inclusion of supply-chain controls
- 2025: NERC CIP : Explicit requirements for energy storage > 20MVA

European Union

- Before 2025: Local initiatives
- 2025: **NCCS** Network Code on Cybersecurity (TSO and DSO)
- 2026: **NIS 2** Directive on network and information systems
- 2028: **CRA** Cyber Resilience Act

Proposed path

- No need of another standard.

- Leverage the **CRA** with:
  - Batteries classified as **Critical assets,** with third-party certification
  - Adopt or adapt **IEC 62443** as harmonised baseline standard

Why IEC 62443

People & Organization

Strategic security

Security awareness and personel trainings, roles and responsabilities, corporate policy…

Process

Secure by design

Secure development Lifecycle with Thread & Risk analysis, Configuration and change management, Requirements traceability, Security testing and monitoring, Vulnerability management…

Technology

Defense-in-depth

Access control, Authentification, layer Hardening, Detection & monitoring

IEC-62443-4-1

IEC-62443-4-2

Secure batteries.
Secure the Energy Transition