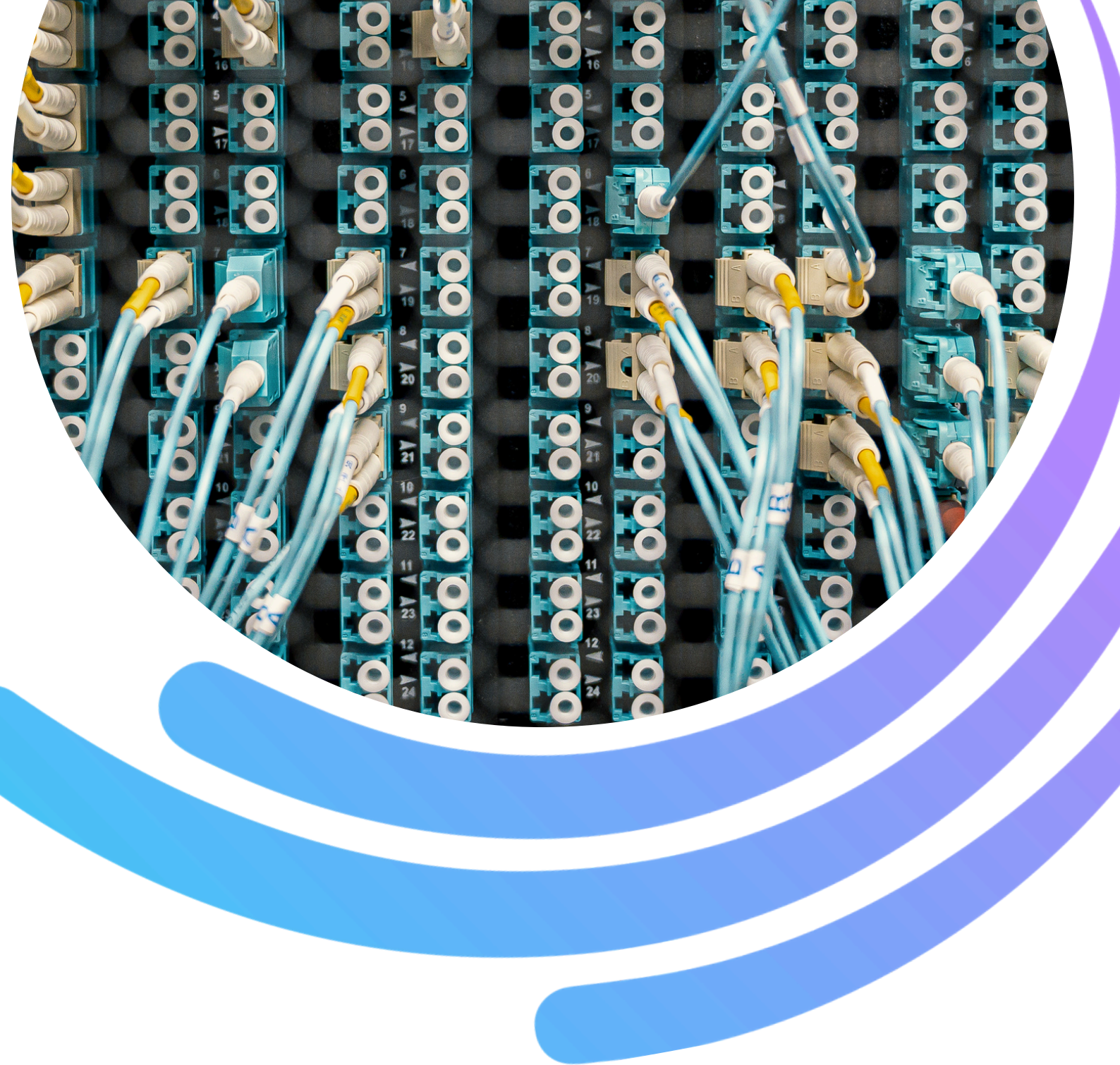




Cybersecurity in Battery Energy Storage Systems:

**Roles, Responsibilities, and
Regulatory Gaps Across
the Value Chain**

September 2026, Brussels



**energy
storage
europe**

Cybersecurity in Battery Energy Storage Systems: Roles, Responsibilities, and Regulatory Gaps Across the Value Chain

Recommendations for EU policymakers and industry

Table of Contents

1. Introduction.....	8
2. BESS Landscape, Value Chain & Cyber Functions	9
2.1 Battery Energy Storage System Definition	9
2.2 Core Hardware Components.....	10
2.2 Key Software and Communication Layers	12
2.3 Why This Architecture Creates Cybersecurity Complexity	12
2.4 Key Actors in the BESS Value Chain.....	13
2.5 Lifecycle Phases.....	14
2.6 Deployment Models & Risk Classification.....	14
3. Responsibility Mapping Across the Lifecycle & Actors.....	18
3.1 Responsibility Matrix	18
3.2 Technology Responsibilities (CRA + CSA).....	19
3.3 Process Responsibilities (NIS 2 + NCCS).....	20
4. Regulatory Mapping & Accountability	22
4.1 Primary Legislative Pillars and Interactions	22
4.2 Key Definitions Under the Framework.....	22
4.3 Applicability Matrix.....	23
5. Challenges & Gaps	27
5.1 Coordination Opportunities Within the Existing Framework	27
5.2 Harmonisation Failures and Their Consequences.....	27
5.3 Specific Gaps Requiring Urgent Resolution	27
5.4 Transparency Around Emerging ITC Supply Chain Risk Management.....	28
6. Recommendations.....	29
6.1 Recommendations for the Industry	29
6.1.1 Asset Owners and Operators.....	29
6.1.2 OEMs and System Integrators.....	29
6.1.3 EPCs and Installers	30
6.1.4 System Operators, Aggregators, and Service Providers	30
6.2 Policy Recommendations for the EU.....	30
7. References and Sources.....	32

Glossary of Terms

BESS: Battery Energy Storage System

BMS: Battery Management System - monitors, protects, and manages battery cells and packs, typically across cell, module, and system levels, to ensure safe, reliable, and efficient operation.

CADA: Cloud and AI Development Act

EMS: Energy Management System - orchestrates dispatch, scheduling, and grid interaction

CRA: Cyber Resilience Act - EU regulation requiring security-by-design for products with digital elements (full effect December 2027)

CSA 2.0: Cybersecurity Act 2.0 - proposed update to the EU Cybersecurity Act, expanding ENISA mandate and certification schemes

ECII: Electricity Cybersecurity Impact Index - used under NCCS to classify BESS by grid criticality

HBOM: Hardware Bill of Materials - complete inventory of physical components and their origins

IAA: Industrial Accelerator Act - EU initiative supporting clean-tech manufacturing scale-up

MFA: Multi-Factor Authentication

NCCS: Network Code on Cybersecurity - EU implementing regulation for electricity sector cybersecurity

NIS 2: Network and Information Security Directive 2 - EU framework for critical infrastructure cybersecurity (transposition deadline October 2024)

OEM: Original Equipment Manufacturer

O&M: Operations & Maintenance

PCS: Power Conversion System - converts electrical power between different forms (e.g., DC to AC, AC to DC, voltage/frequency conversion), including components such as inverters. DC battery power to AC grid power (includes inverters)

SBOM: Software Bill of Materials - complete inventory of software components, libraries, and dependencies

SPV: Special Purpose Vehicle - a legally independent entity often used to hold a single energy asset

SRA: Secure Remote Access

TSO / DSO: Transmission / Distribution System Operator

VPP: Virtual Power Plant - aggregated fleet of distributed energy resources

Executive Summary

Energy Storage Europe welcomes the European Commission's growing focus on cybersecurity in the energy sector and supports the direction of travel across the Cyber Resilience Act (CRA), the Network Code on Cybersecurity, and the proposed Cybersecurity Act (CSA) 2.0. Yet raises concerns that require targeted corrections to ensure these frameworks deliver on their **security objectives without inadvertently slowing battery storage deployment.**

Battery Energy Storage Systems (BESS) actively regulate the grid in real time. They are not inherently more vulnerable than other grid-connected technologies; but their combination of deep cyber-physical coupling, multi-vendor architectures, and third-party control dependencies creates a governance challenge where control-layer failures can escalate rapidly to grid-stability events. With BESS hitting 50 GW installed with 200 GW projected by 2030, **cybersecurity risks are no longer isolated asset-level concerns.**

The current EU framework does not yet provide a coherent approach to BESS cybersecurity risks. Important accountability gaps remain, particularly for legacy assets, outsourced operations, special purpose vehicle structures, and manufacturers without an EU legal entity. Divergent implementation of NIS2 and inconsistent connectivity requirements across Member States increase compliance costs, create unnecessary complexity, and slow project deployment. This is particularly burdensome for battery storage; a technology manufactured at scale through highly standardised global supply chains. As the supply chain framework under the Cybersecurity Act 2.0 continues to develop, the **Industry calls for a clear, risk-based, and component-level approach to cybersecurity requirements, with proportionate obligations and realistic implementation timelines that support both resilience and investment.**

This paper call for four targeted actions:

- **Reclassify Battery Management Systems, Power Conversion Systems, and Energy Management Systems as Critical products under the Cyber Resilience Act;**
- **Mandate harmonised technical requirements for battery storage connectivity at distribution level;**
- **Publish joint NIS 2 and Network Code on Cybersecurity implementation guidance;**
- **Provide industry with early clarity on CSA 2.0 supply chain scope and timelines.**

Focus: The Questions This Paper Aims to Answer

1. How does the cybersecurity risk profile of BESS differ from solar PV and other distributed energy resources?
2. Which BESS components create the highest cyber-physical risk: BMS, PCS, EMS, SCADA, cloud platforms, communications protocols, or remote-access systems?
3. Which actors should be accountable for cybersecurity across the BESS lifecycle: OEMs, system integrators, EPCs, asset owners, O&M providers, aggregators, TSOs, DSOs, cloud providers and investors?
4. How should cybersecurity obligations differ between utility-scale, co-located renewable, C&I, residential, and aggregated residential BESS fleets?
5. Are current EU frameworks, NIS 2, CER, CRA, NCCS, CADA and CSA 2.0, sufficient for BESS, or do they still rely too heavily on generic assumptions?

The Consequences of Fragmented Cybersecurity Governance

Cyber incidents can become grid incidents: A control algorithm failure during [testing at a 100 MW battery storage installation in Estonia tripped two interconnectors and destabilised the Baltic grid](#). Caused by a software error rather than a cyberattack, it illustrates the grid-stability consequences that deliberate manipulation of the same control layer could produce. The threat context makes this relevant: the [European Union Agency for Cybersecurity \(ENISA\)](#) recorded more than 200 energy-sector cyber incidents globally in 2023, more than half targeting Europe.

The attack surface is growing faster than governance can track it: The highest-risk components are those that translate digital commands into physical action: Battery Management Systems, Power Conversion Systems, Energy Management Systems, supervisory control systems, substation gateways, communications protocols, cloud platforms, and remote-access tools.

ENISA has [confirmed](#) these layers are already the primary targets in energy-sector incidents across all technology types.

Deployment costs rise through fragmented national requirements and late retrofits: NIS 2 obligations are not harmonised across the EU, and ENTSO-E is still conducting the risk assessment under the [Network Code on Cybersecurity](#). This leaves battery storage operators without a consistent baseline for compliance. Fragmented connectivity requirements force market-specific configurations, raising costs and slowing deployment. The broader transition involves an estimated €3.4 to €4.3 billion in annual equipment costs, with potential compliance savings of €15.3 billion over five years.

ICT supply chain security moves into the focus of policymakers: Since 2025, the Commission has taken a series of concrete steps: initiating supply chain reviews for wind and solar under the NIS Cooperation Group, introducing [Title IV](#) on Security of ICT Supply Chains in the proposed Cybersecurity Act revision, and conditioning EU financing on the exclusion of power conversion systems from high-risk suppliers. These developments have direct implications for battery storage, yet industry currently lacks clarity on how they apply to storage-specific components and supply chains. Technical cybersecurity requirements and supply chain risk governance address different problems: they should be developed in a coherent and mutually reinforcing manner, so that progress on one does not delay or undermine the other.

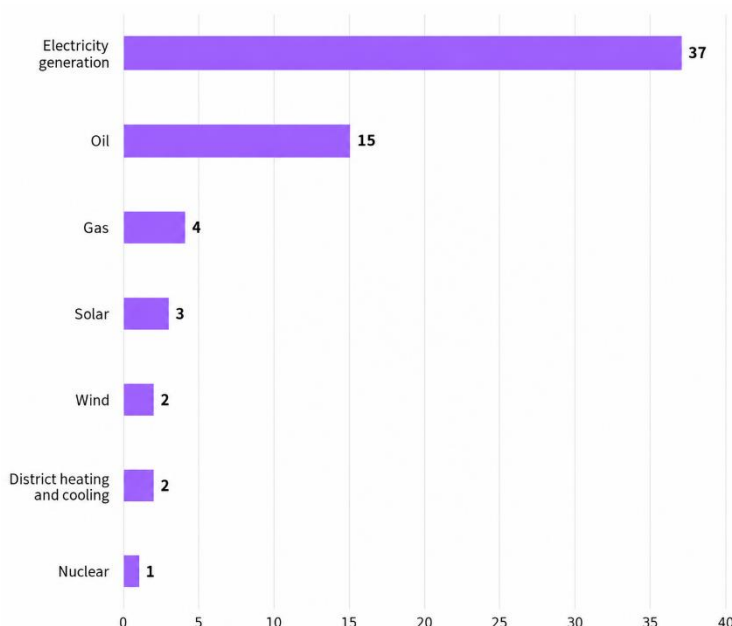


Figure 1: In Q1 2026, electricity operators accounted for 37 incidents (56.1% of energy-sector activity), followed by oil at 22.7%. Source: ENISA.

1. Introduction

The European Union has made substantial progress in strengthening the cybersecurity and resilience of critical infrastructure. The [NIS 2 Directive \(2022/2555\)](#), the [Cyber Resilience Act \(2024/2847\)](#), the [Network Code on Cybersecurity \(Commission Delegated Regulation \(EU\) 2024/1366\)](#), and the proposed revision of the [Cybersecurity Act](#) reflect a clear policy direction: digital systems supporting essential services must be secure, resilient, and subject to defined accountability. However, there is a risk that this regulatory architecture does not keep pace with the highly digital nature of a fast-growing and innovating sector such as energy storage. Regulatory frameworks must evolve in lockstep with technological change and the growing complexity of actors, systems, and interfaces across the energy industry.

As distributed energy resources emerged and scaled, **solar photovoltaic systems became the primary reference case for distributed energy cybersecurity policy**, including through the NIS Cooperation Group's supply chain review under Article 22 of NIS 2. Photovoltaic systems introduced inverter-based generation, remote monitoring, and grid-edge connectivity. But they remain largely unidirectional: they generate and export, with limited real-time grid interaction.

Battery storage is different: active, bidirectional, software-intensive resources that charge and discharge within milliseconds. They are explicitly designed to provide the services that keep the system stable in real time: frequency containment, balancing, reserve provision, congestion management, inertia-like services, black start, support islanding, and system restoration. Unlike other distributed energy resources, **the primary purpose of battery storage is not energy generation but flexibility, stabilisation, and regulation of the power system. This creates a distinct cybersecurity profile:** deeper cyber-physical coupling, greater control depth, higher communication intensity, and stronger dependence on third-party optimisation, aggregation, cloud platforms, and remote access. The same dynamic applies to other grid-forming and grid-connected devices with real-time control functions; including smart meters, demand-response platforms, substation automation systems, and the digital control layers of conventional generation assets.

To address the complex system management architecture of battery storage, responsibilities across the value chain, from project development and financing through design, integration, commissioning, operation, maintenance, and decommissioning, **must be clearly and consistently assigned**. Several questions around responsibility remain unresolved:

- Which entities are responsible for cybersecurity at each stage of the battery storage project lifecycle, from development and financing through to construction; and how should applicable legislation be applied?
- Who is responsible for firmware updates across multi-vendor systems; and who controls and audits remote access in outsourced operations and maintenance arrangements?
- Who owns vulnerability disclosure when a flaw is discovered in an embedded Battery Management System, Power Conversion System, Energy Management System, or SCADA component?
- How should responsibilities shift between utility-scale, co-located, commercial and industrial, and residential configurations?

This paper addresses these issues by clarifying cybersecurity roles and responsibilities across the battery storage value chain. It aims to support industry and policymakers in adapting EU cybersecurity frameworks to the specific risks created by battery storage, and to provide industry actors with practical guidance on procurement, contracting, risk management, and implementation.

2. BESS Landscape, Value Chain & Cyber Functions

This section introduces the principal components of a Battery Energy Storage System (BESS), the key actors across the value chain, the lifecycle phases through which responsibilities shift, and the deployment models that shape regulatory classification. It provides the technical and structural foundation for the responsibility mapping and regulatory analysis that follow.

2.1 Battery Energy Storage System Definition

Before mapping cybersecurity responsibilities across the value chain, it is necessary to establish what falls within scope. A BESS is a multi-component assembly, and the components within scope determine which actors bear obligations, which regulatory instruments apply, and where accountability gaps arise. For the purposes of this paper, a BESS encompasses the following principal elements:

- Battery cells, modules, and packs, with cells comprising cathode and anode active materials, electrolytes, separators, and current collectors
- Battery Management Systems (BMS) and Battery Thermal Management Systems (BTMS)
- Power Conversion Systems (PCS), including inverters
- Energy Management Systems (EMS) and supervisory control and data acquisition systems (SCADA)

Although the elements listed above are defined as part of a BESS in [Energy Storage Europe's position paper on the Industrial Accelerator Act](#), the following cybersecurity-relevant components are also considered within scope for the purpose of this paper:

- Battery housing and containers, and the electrical systems and protection equipment required for grid connection
- Auxiliary systems, including HVAC, fire protection, auxiliary power, and communications
- Balance of plant components, including transformers, grid connection, and protection equipment

Different pieces of legislation regulate these components separately, increasing the risk of inconsistencies, overlaps, and gaps. For example, the [Industrial Accelerator Act](#), introduces a definition of stationary battery energy storage systems drawn from the [Net Zero Industry Act](#), but that definition covers only the electrochemical core. Power Conversion Systems, Energy Management Systems, and SCADA (the components most directly relevant to cybersecurity risk) fall outside the Union origin requirements and are addressed only through a general cross-reference to the proposed Cybersecurity Act revision, creating an asymmetry with other technologies covered by the IAA and a risk of inconsistency with the parallel supply chain framework being developed under that revision.

Energy Storage Europe's [position paper](#) on the Industrial Accelerator Act, calls for a revised definition that explicitly covers the full system, including Power Conversion Systems, Energy Management Systems, battery housing, SCADA, and electrical systems and protection, mirroring the system-level approach already applicable to photovoltaic systems under the NZIA. The position paper also calls for an amendment to the Implementing Act on the basis of Article 46(7) NZIA to add these elements as recognised main specific components, subject to a careful impact assessment, and for alignment of any Union origin requirements with this broader definition, including with Delegated Regulation (EU) 2025/1463.

2.2 Core Hardware Components

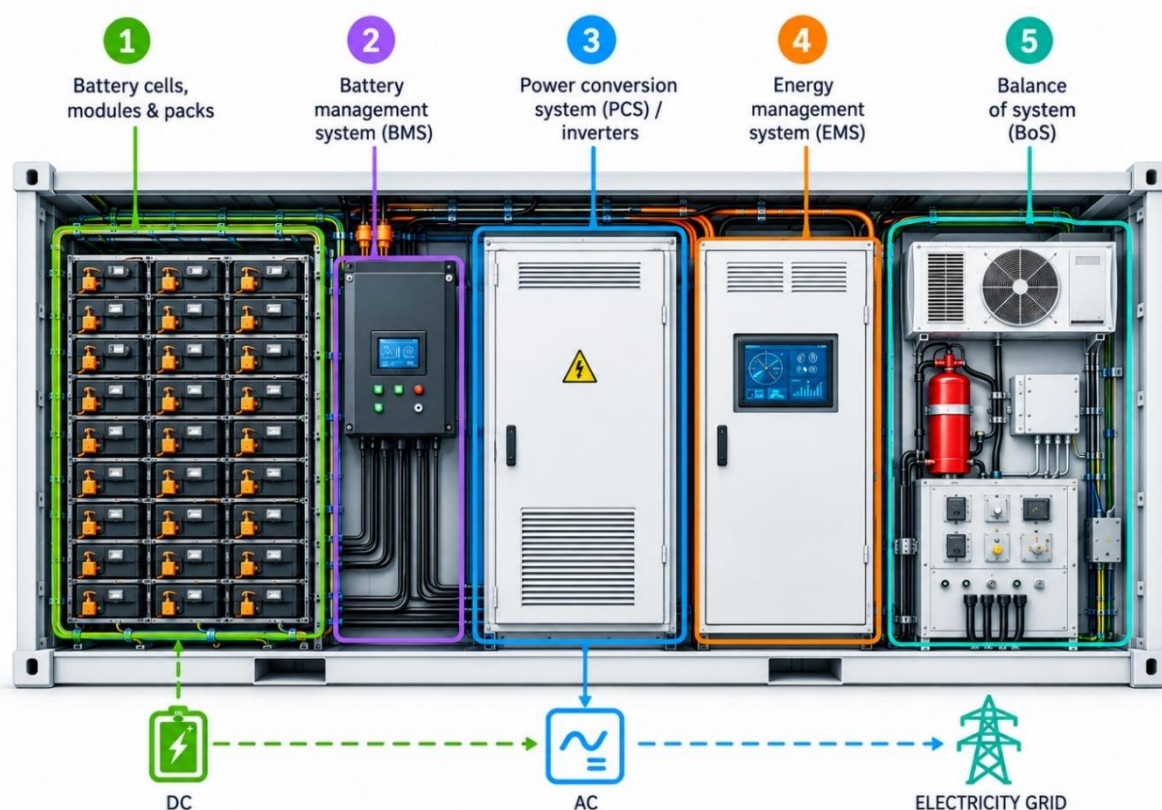


Figure 2: Main components of a utility-scale BESS container.

- 1. Battery Cells, Modules, and Packs:** The electrochemical foundation of the system. Cells are grouped into modules and packs. While largely mechanical and electrical in nature, battery packs increasingly include embedded sensors and firmware with the potential for remote control access.
- 2. Battery Management System (BMS):** Software-driven hardware that monitors cell voltage, temperature, and state of charge; protects against overcharge and thermal runaway; and communicates battery status to the EMS. [Studies](#) find that the BMS is among the highest-priority components for cybersecurity scrutiny: a compromised BMS could result in unsafe operating conditions of masked failures.
- 3. Power Conversion System (PCS) / Inverters:** Converts direct current (DC) from the battery to alternating current (AC) for grid injection, or vice versa during charging. The PCS responds to grid commands in real time and is the primary interface between the BESS and the electricity network. PCS firmware vulnerabilities or attacks on PCS could allow manipulation of active and reactive power output, directly affecting grid frequency and voltage.
- 4. Energy Management System (EMS):** The 'brain' of the BESS, orchestrates scheduling, dispatch, and market participation. The EMS communicates with the grid operator, aggregator platforms, and market systems. It is typically cloud-connected and highly networked, making it a highly critical attack surface.
- 5. Balance of System (BoS):** Supporting hardware including thermal management, fire suppression, switchgear, and monitoring sensors. Increasingly software-integrated and networked to the EMS. This includes additional applications and interfaces such as SCADA for substation operation or a Power Plant Controller (PPC) that may be used to monitor and control major components in the plant such as transformers, high level control of battery strings, and interface with protection devices.

DC BLOCK

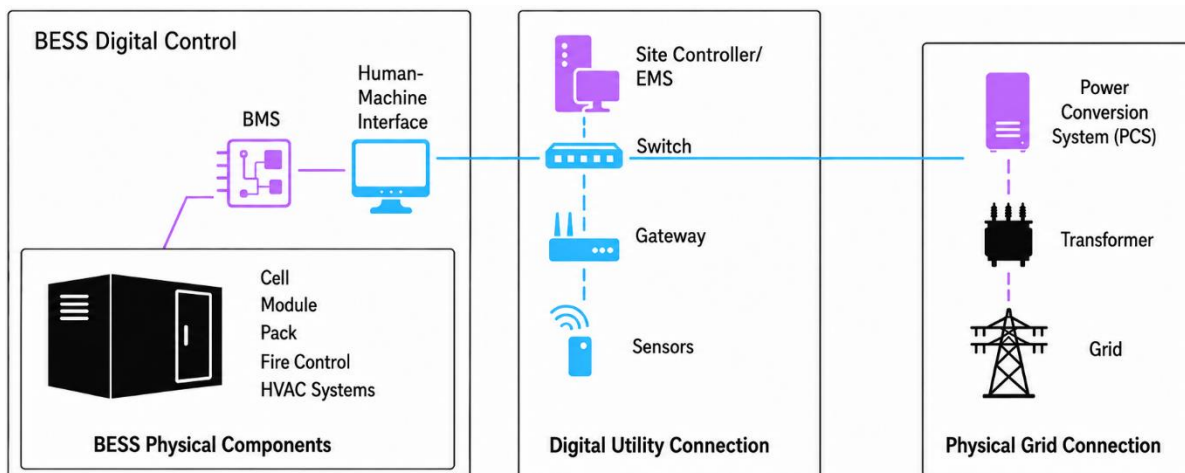


Figure 3: Components Of a Modern Battery Energy Storage System: Dc Block Structure. Purple Components Have the Highest Level of Criticality of Cyber and Physical Threats. Blue Components Have a Medium Level of Criticality.

Source: Adapted from [Securing Battery Energy Storage Systems from Cyberthreats: Best Practices and Trends for Protecting Critical Energy Infrastructure](#). The Brattle Group and Dragos, 2025

AC BLOCK

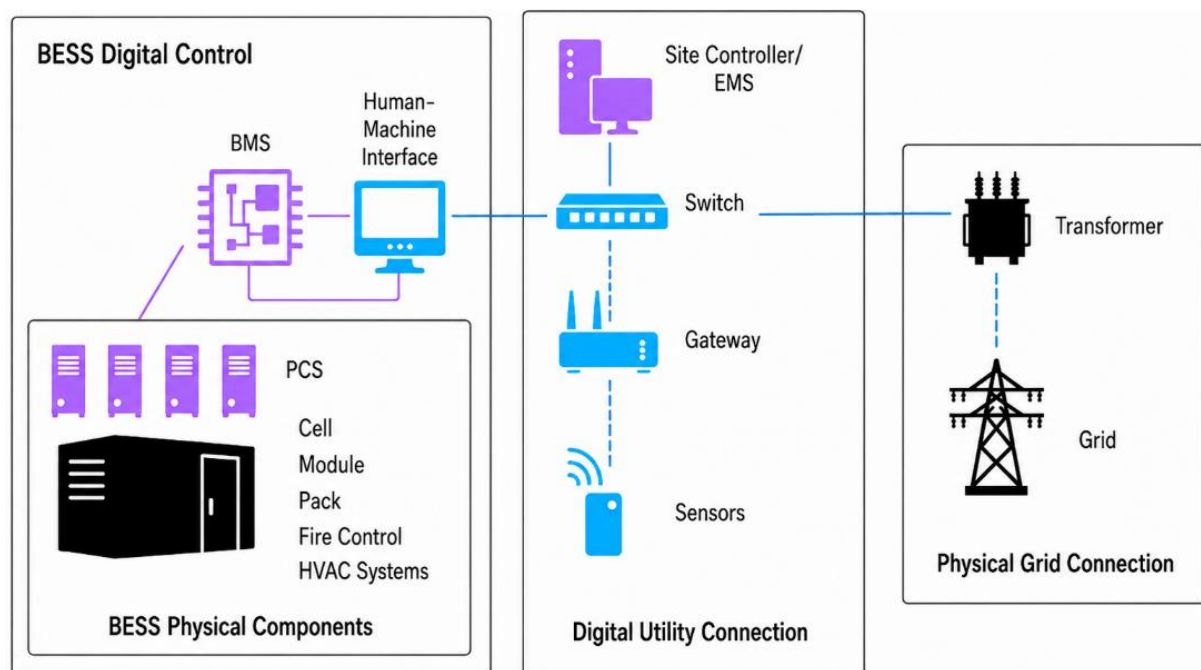


Figure 4: Components Of a Modern Battery Energy Storage System: AC-block architecture. Purple Components Have the Highest Level of Criticality of Cyber and Physical Threats. Blue Components Have a Medium Level of Criticality.

Source: Adapted from [Securing Battery Energy Storage Systems from Cyberthreats: Best Practices and Trends for Protecting Critical Energy Infrastructure](#). The Brattle Group and Dragos, 2025

2.2 Key Software and Communication Layers

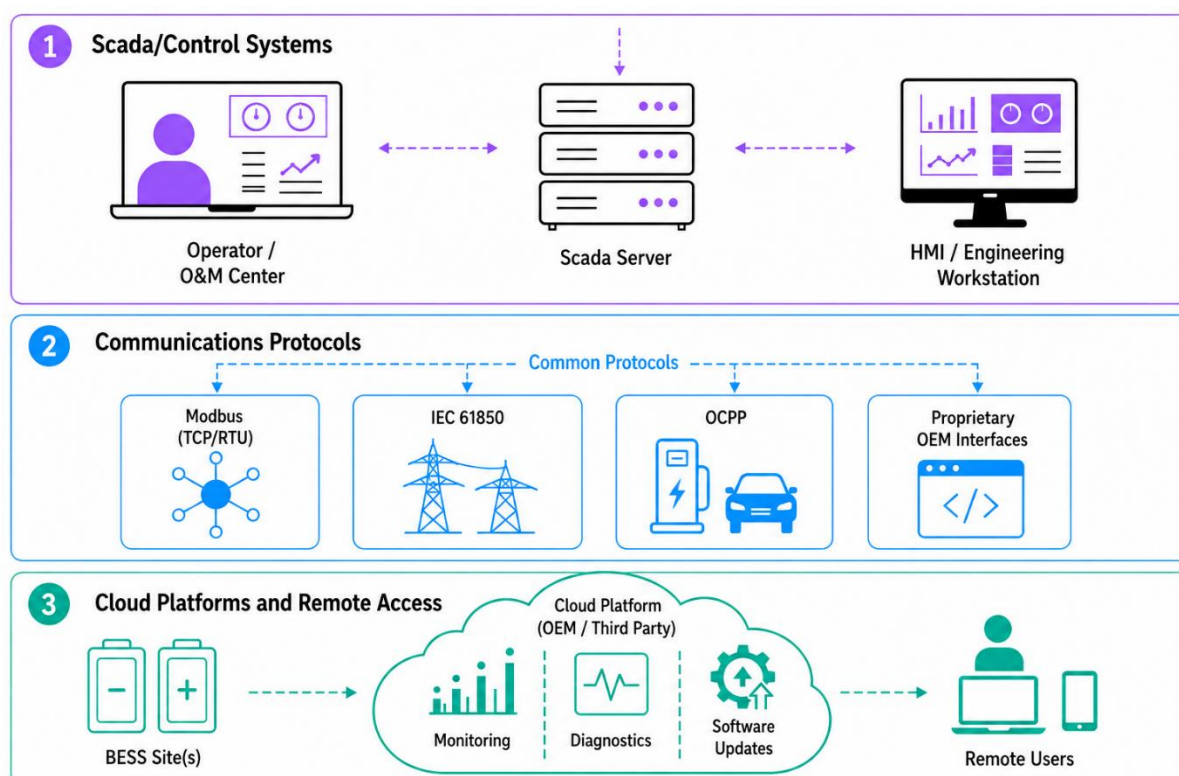


Figure 5: Key software and communication layers in a BESS deployment: SCADA/control systems, communication protocols, and cloud platforms and remote access.

- 1. SCADA/Control Systems:** Supervisory control and data acquisition systems used for real-time monitoring and remote operation, often managed by the asset owner, O&M provider, or grid operator. These environments are frequently characterised by operational technology security weaknesses common across the energy sector: weak credential management, excessive user privileges, insufficient network segmentation, exposed services, and inadequate monitoring.
- 2. Communication Protocols:** BESS systems communicate using protocols such as Modbus, IEC 61850, IEC 104, OCPP, and proprietary OEM interfaces. Each protocol carries distinct security characteristics and exposure risks.
- 3. Cloud Platforms and Remote Access:** Many BESS systems connect to OEM or third-party cloud platforms for monitoring, diagnostics, trouble shooting and software updates. Remote access is operationally necessary, but represents one of the most common attack vectors in OT environments.

2.3 Why This Architecture Creates Cybersecurity Complexity

Some features of BESS architecture make cybersecurity governance particularly challenging:

Multi-vendor environments: A single installation may integrate a BMS from one manufacturer (considering that nowadays BMS are deeply embedded in cells, therefore, the manufacturers coincide), PCS from another, an EMS from a third party, cloud services from a fourth, and a separate SCADA vendor. No single actor has end-to-end visibility of the system, and no single regulatory instrument currently assigns accountability across this entire stack. Each plant also involves a bespoke integration of hardware and software to function as a single

coherent system, which means individual components cannot easily be substituted or upgraded retroactively once the system is commissioned.

Grid-forming capability: Modern utility-scale battery storage systems provide frequency response, synthetic inertia, and black-start services. A security failure therefore does not affect only the asset owner: it can directly affect system operators and grid stability across borders.

Note on what this means for policymakers:

Battery storage systems are multi-component, multi-actor, grid-relevant systems. The central implication for cybersecurity legislation is structural: a component-level approach is insufficient. Responsibilities must be defined at the system level, with clarity on which actor is accountable at each layer of the architecture and at each stage of the asset lifecycle. Without this, gaps between instruments designed for individual components, a manufacturer's product, an operator's network, a cloud provider's platform, will leave the overall system without a responsible party for cross-cutting functions such as firmware updates, remote access governance, and vulnerability disclosure.

Regulatory frameworks must therefore address operational integrity alongside data security, covering the key hardware and software components described above as well as the processes surrounding them.

2.4 Key Actors in the BESS Value Chain

The following table identifies the primary actors involved in the BESS lifecycle, their principal regulatory trigger under current EU frameworks, and their core cybersecurity function. Detailed regulatory obligations are elaborated in the following section. All references on the CSA 2.0 are based on the current available [proposal](#) published by the European Commission on 20 January 2026.

Actor	Primary Regulatory Trigger	Core Function in Cybersecurity
OEMs (BMS, EMS, PCS)	CRA Article 13	Ensuring "security-by design"
	NIS2	Important entities as manufacturer of electrical components
	CSA 2.0 Title IV	Compliance on implementation of Chapter IV on Security of ICT Supply Chains
System Integrators	CRA Article 13(15)	Ensuring individual components form a compliant, secure system before deployment
	NIS2	Important entities as manufacturer of electrical components
	CSA 2.0 Title IV	Compliance on implementation of Chapter IV on Security of ICT Supply Chains
Asset Owners / Operators	NIS 2 Article 3 & 21	Responsible for "all-hazards" risk management and service-level resilience
	CSA 2.0 Title IV	Asset owners are subject to the CSA 2 Title IV as critical entities under the NIS2 and procuring entities towards which the mitigation measures in art. 103 apply
TSOs / DSOs	NIS2	Identifying High/Critical impact entities and overseeing cross-border grid stability
	NCCS Article 24	High-impact and critical-impact entities within the European electricity sector.

	CSA 2.0 Title IV	Compliance on implementation of Chapter IV on Security of ICT Supply Chains
Aggregators / Optimisers	NIS 2 Annex I	Managing fleet-wide digital risks and providing market flexibility
Service Providers (Cloud/ICT)	CSA 2.0 Title IV	Subject to supply chain vetting and "High-Risk Supplier" designations
	Cloud and AI Development Act	Cloud service providers will be subject to assurance levels and Union origin requirements in public procurement potentially extendable to private actors as well (modalities still unclear)

2.5 Lifecycle Phases

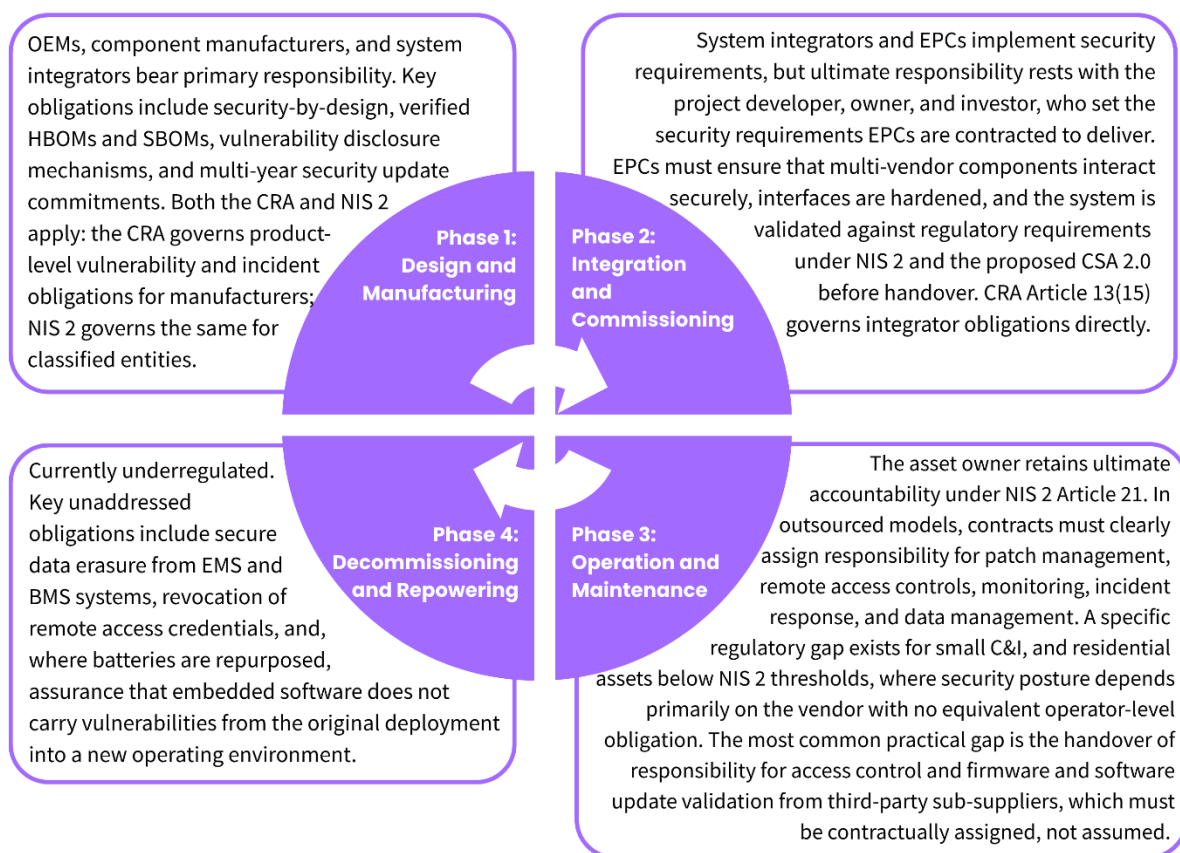


Figure 6: Cybersecurity responsibility across the BESS lifecycle: design and manufacturing, integration and commissioning, operation and maintenance, and decommissioning and repowering.

2.6 Deployment Models & Risk Classification

Cybersecurity obligations for infrastructure are scaled according to potential impact. This happens under the NCCS based on the Electricity Cybersecurity Impact Index (ECII); or under the CER and national implementing legislation based on asset size and services provided, which classifies BESS installations by their potential impact on grid stability and cross-border energy flows. Similarly, BESS installations can be categorised as follows:

Utility-Scale Standalone BESS: Operators/Asset Owners are typically classified as 'Essential Entities' under NIS 2 if they exceed the size threshold (50+ employees, or €50m+ turnover) or have significant cross-border

impact. Plants are sometimes considered critical infrastructure, however they often also fall below single plant thresholds and can make up a significant portion of the installed capacity, depending on the country. The entities responsible for the plants are generally subject to the most stringent NIS 2 Article 21 obligations and NCCS entity designation.

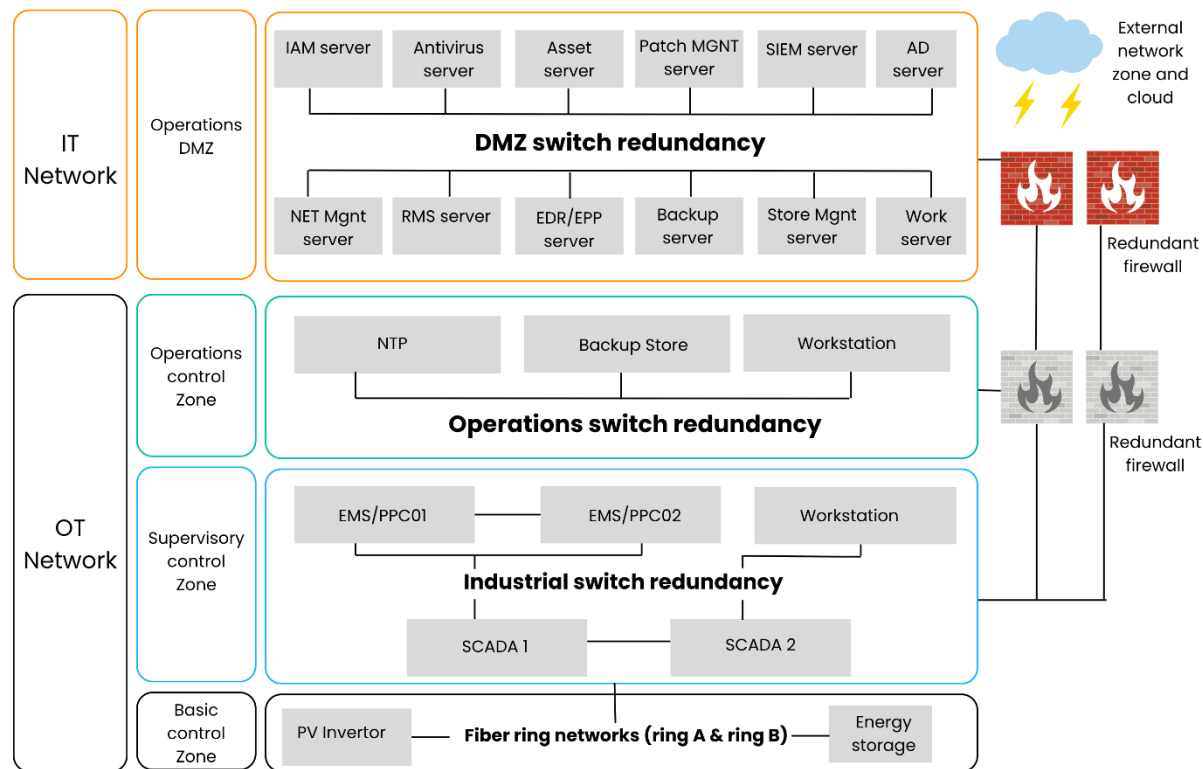


Figure 7: Reference network architecture for a utility-scale standalone BESS, with segmentation into IT, DMZ and OT zones separated by redundant firewalls.

Co-Located with Renewable Generation: Classification depends on asset size and grid connection. If the combined plant exceeds relevant thresholds, it may trigger critical infrastructure designation. Asset owner or operator is often classified as an essential entity. Co-location introduces additional attack surface: a breach at the PV inverter level could propagate to the BESS EMS.

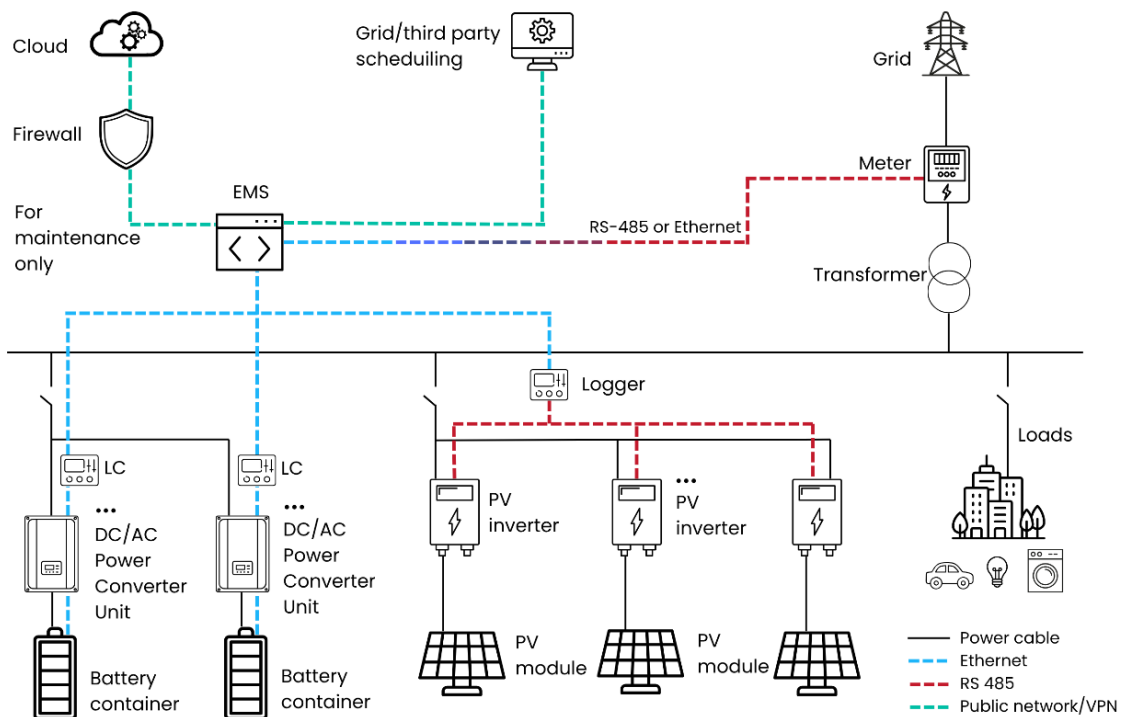


Figure 8: Co-located BESS and PV plant: the EMS coordinates battery and PV inverters and is the shared point where a compromise could spread between the two systems.

Commercial & Industrial (C&I) BESS: Asset owner or operator may not be a regulated entity under NIS 2, it varies largely dependent on the specific business use case.

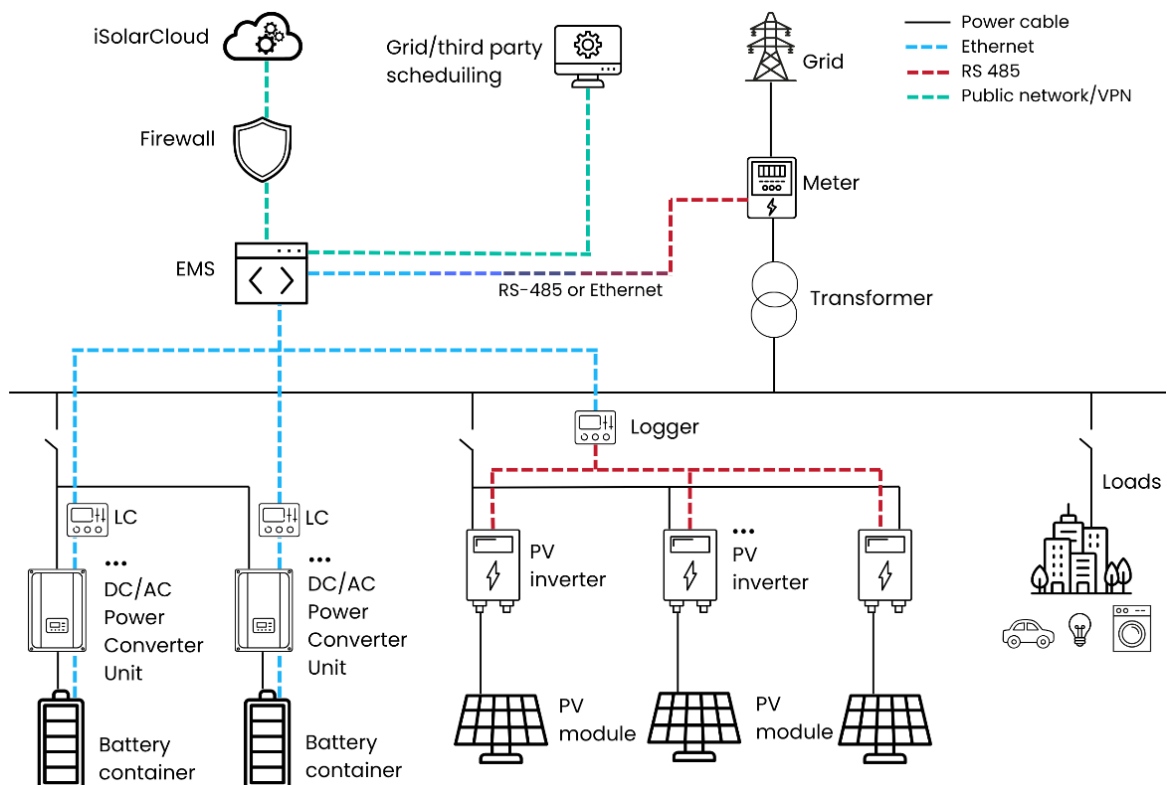


Figure 9: Commercial and industrial BESS behind the meter, with a vendor cloud platform and third-party scheduling connected to the site EMS.

Residential BESS: Generally, fall into the CRA 'Default' category, requiring only self-assessment for hardware components. However, the aggregation of large residential BESS fleets through VPP platforms raises systemic risk concerns that the current residential classification does not adequately address. Any extension of cybersecurity obligations to aggregated residential BESS fleets must respect the mass-produced nature of these products and apply requirements at the type-of-entity or product-category level, not on a project-by-project or fleet-by-fleet basis. Disproportionate requirements risk raising costs for consumers and slowing the deployment of distributed storage.

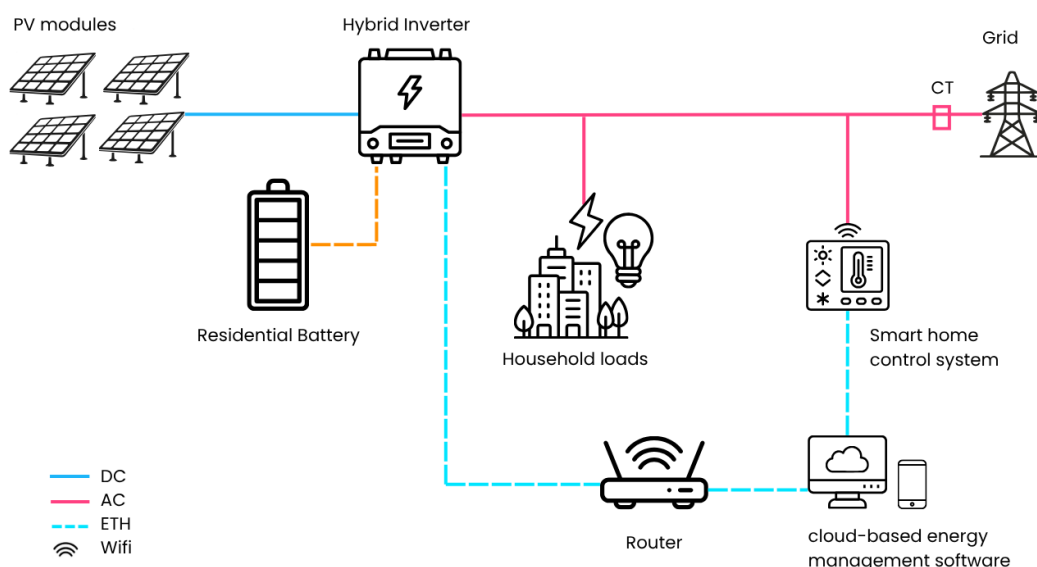


Figure 10: Residential BESS with a hybrid inverter, connected through the household router to a cloud-based energy management platform. At fleet scale, this cloud link is the systemic risk point.

Note on regulatory gap on residential BESS fleet aggregation:

Individual residential and C&I BESS units fall below critical infrastructure and are classified only under the CRA's default category. For nearly all residential installations and many C&I installations, the asset owner is not a regulated entity under NIS 2. However, vendor cloud platforms aggregating thousands of residential units can collectively influence grid frequency and market prices. The current regulatory framework only addresses the risk of aggregation for market participation and ignores connections related to O&M of installed assets.

The CSA 2.0 review shall consider whether VPP operators managing residential fleets above a certain aggregate capacity should face enhanced obligations.

3. Responsibility Mapping Across the Lifecycle & Actors

This section provides a mapping of cybersecurity responsibilities across actors and phases, distinguishing between primary accountability, shared obligations, and review/oversight roles. The matrix below is intended as a working baseline for procurement specifications, contractual frameworks, and regulatory guidance.

3.1 Responsibility Matrix

The following matrix maps key cybersecurity responsibility areas to value chain actors. The designations used in the matrix are defined as follows:

Responsibility Area	OEM / Manufacturer	System Integrator / EPC	Asset Owner / Operator	O&M Provider	Cloud / ICT Provider
Secure design & architecture	A/R	S	C	I	—
Hardware / Software BOM (HBOM/SBOM)	A/R	S	C	—	—
Firmware update management	A/R	S	C	—	—
Communication interface security	S	A/R	C	I	I
Access & identity management	S	S	A	R	S
Remote access controls (SRA)	S	S	A	R	S
Network monitoring & detection	—	S	A	R	S
Patch & vulnerability management	S	S	A	R	I
Incident response & reporting	I	—	A	R	S
Vulnerability disclosure	A/R	S	—	—	—
Decommissioning & data erasure	—	A/R	A/R	S	—
Supply chain vetting	S	A/R	A	R	—

Table 1: Who is accountable, responsible, supporting, consulted or informed for each cybersecurity task, by value-chain actor.

Legend:

- **A/R - Accountable and Responsible:** the actor holds ultimate accountability and carries out the activity. This is the named responsible party in contracts and regulatory filings.
- **A - Accountable:** the actor holds ultimate accountability for the outcome but delegates execution. Must be named in contracts and regulatory filings.
- **R - Responsible:** the actor carries out the activity under the accountability of another party.
- **S - Support:** the actor contributes to delivery and must coordinate with the Accountable party. Responsibility cannot be unilaterally discharged and must be formalised in contractual arrangements.
- **C - Consulted:** the actor provides input before decisions are finalised but does not hold an execution or accountability role.
- **I - Informed:** the actor is notified of outcomes without an active role in delivery or decision-making.
- **— :** no direct obligation for this actor under current frameworks, though obligations may arise indirectly via supply chain duties or contractual requirements from regulated clients.

Notes on the matrix:

Multi-vendor environments: Where multiple actors share a *Support* designation with no single *Accountable* party, a named lead must be contractually designated. Shared responsibility without a named accountable party is functionally equivalent to no accountability.

O&M outsourcing: NIS 2 Article 21 places ultimate accountability on the asset owner, but execution typically falls to the O&M provider under a separate contract. Patch timelines, access credential management, and incident liability must be explicitly assigned in O&M contracts, not assumed.

Assets outside NIS 2 scope: For residential and small commercial and industrial assets, the Asset Owner / Operator column may carry no regulatory obligation as *Accountability* defaults to the vendor. The proposed Cybersecurity Act revision and NCCS implementation should address this for aggregated fleets where collective grid impact is material.

3.2 Technology Responsibilities (CRA + CSA)

Technology-layer responsibilities cover the hardware, software, and system architecture components of a BESS deployment, including:

- BMS, EMS, PCS, and their embedded software
- Communication interfaces, protocols, and gateways
- Cloud and ICT infrastructure
- Firmware, configuration files, and cryptographic credentials

OEM Obligations	Under the Cyber Resilience Act, OEMs placing BESS components with digital elements on the EU market must implement security-by-design across the product lifecycle. This includes: maintaining a verified SBOM and HBOM; publishing and maintaining a vulnerability disclosure policy; providing a minimum of five years of security patches; and CE-marking products as CRA-compliant.
	These obligations apply from December 2027 for new products, with mandatory vulnerability reporting beginning September 2026.
	A critical gap exists in the current CRA classification: digital components of battery storage systems, including BMS, PCS, and EMS, are classified as “Default category products”, requiring only manufacturer self-assessment. Given their direct influence

	on grid operations, reclassification as “Critical” (Class I or II), with mandatory third-party conformity assessment, is more appropriate and should be pursued through the CRA delegated acts process.
System Integrator Obligations	System integrators bear responsibility for ensuring that individually compliant components from multiple OEMs interact securely when assembled. This requires: validating communication interfaces between BMS, EMS, PCS and other critical electrical components; establishing a system-level SBOM that aggregates component-level SBOMs; configuring secure defaults (closing unnecessary ports, disabling default credentials); and conducting integration-level security testing before handover to the asset owner.

3.3 Process Responsibilities (NIS 2 + NCCS)

Process-layer responsibilities govern the operational and organisational cybersecurity functions that sustain security throughout the asset's operational life. Key areas are addressed below.

Access Management (Including Remote Access)	Remote access is operationally necessary for BESS, OEM diagnostics, O&M monitoring, and aggregator platforms. However, uncontrolled remote access is the most common entry point for adversaries in OT environments. Responsible parties must implement: role-based access control (RBAC) with principle of least privilege; multi-factor authentication (MFA) for all remote sessions; session logging with audit trail retention; and regular access reviews with prompt revocation upon role changes. In outsourced O&M models, the asset owner retains ultimate accountability under NIS 2 but must contractually ensure the O&M provider meets these requirements. Energy Storage Europe opinion: The proposed approach to remote access and data security under the Cloud and AI Development Act (CADA) may also introduce considerations related to jurisdiction and location of control functions. These elements are closely linked to emerging cloud sovereignty requirements under EU digital frameworks, which may influence how remote control, monitoring and optimisation of BESS assets can be performed across borders. From an energy storage perspective, it is essential that such requirements are clearly defined and proportionate, to avoid unintended constraints on system operation, flexibility services and real-time grid interaction.
Patch & Firmware Update Management	Patch management for BESS is complicated by the multi-vendor environment and the operational constraints of a grid-connected asset (many BESS cannot be taken offline for patching without prior notification to the system operator). Responsibility must be clearly assigned in contracts: the OEM publishes patches and/or compatibility with underlying operating system patches; the asset owner or O&M provider schedules and applies them; and the system integrator validates that patches do not introduce integration issues. Testing patches in a staging environment before production deployment is strongly recommended.
Monitoring, Detection & Incident Response	NIS 2 Article 21 requires essential and important entities to have the capability to detect and respond to cyber incidents. Energy Storage Europe opinion: For BESS, this means: network monitoring across OT and IT environments with consideration of local network monitoring at critical plants; anomaly detection for unusual BMS or EMS communication patterns; a documented incident response plan that includes coordination with the system operator (TSO/DSO); and defined escalation paths. The incident response plan should be tested annually through tabletop exercises.

Vulnerability Disclosure	OEMs are required under the CRA to maintain a coordinated vulnerability disclosure policy and to report actively exploited vulnerabilities to ENISA within 24 hours. Asset owners and operators should require OEMs to provide disclosure policy documentation as part of procurement specifications, and should establish internal processes for receiving and acting on vulnerability disclosures from OEMs and national CERTs.
The Outsourcing Handover Risk	A recurring gap in current BESS deployments is the 'handover risk' in hybrid operational models: NIS 2 Article 21(2)(d) requires the asset owner to vet its supply chain, but the practical implementation of patches, access controls, and monitoring often falls to the O&M contractor. Energy Storage Europe opinion: Where contracts do not explicitly allocate responsibilities for patching and remote access, ambiguity can arise over who is accountable if an incident occurs during a patch window managed by the O&M provider. Contracts should therefore specify: which party applies patches; what approval is required from the asset owner; how incidents during O&M activities are classified and reported; and what liability applies if the O&M provider's remote access becomes the vector of a breach. <i>This will be further explained under the Challenges & Gaps chapter.</i>

4. Regulatory Mapping & Accountability

The European cybersecurity regulatory framework has transitioned from voluntary standards to a comprehensive, multi-layered ecosystem of binding legislation designed to secure every level of the digital value chain, from hardware components to cross-border operational flows. For grid-relevant components or functions as used in Battery Energy Storage Systems (BESS), this framework is anchored by five primary pillars: the NIS 2 Directive, the Cyber Resilience Act (CRA), the Network Code on Cybersecurity (NCCS), the proposed Cybersecurity Act 2.0, and the Critical Entities Resilience Directive (CER).

4.1 Primary Legislative Pillars and Interactions

The framework is built upon five primary legislative pillars that interact to provide horizontal, product-level, and sector-specific security.

- **The Organisational Pillar:**
 - **NIS 2 Directive (EU) 2022/2555:** This Directive sets the baseline for a high common level of cybersecurity across the Union (**Article 1**) at entities level. It classifies the energy sector as a "sector of high criticality" (**Annex I, Point 1**), bringing BESS operators under strict regulatory oversight.
 - **Critical Entities Resilience Directive (EU) 2022/2557:** While NIS2 focuses on cyber security, the CER includes resilience for critical entities for physical security, organisational continuity and provides the basis for defining critical infrastructure in Member States.
- **The Product Pillar: Cyber Resilience Act (CRA) Regulation (EU) 2024/2847:** While NIS 2 focuses on entities, the CRA sets horizontal cybersecurity requirements for "products with digital elements" (**Article 1**). This includes the hardware and software used in BESS, such as BMS, inverters/power conversion and control systems.
- **The Sector-Specific Pillar: Network Code on Cybersecurity (NCCS) Regulation (EU) 2024/1366:** This provides rules for cross-border electricity flows (**Article 1**). It complements NIS 2 by providing deeper, technical requirements for the electricity sub-sector. Compliance with NCCS may serve as evidence of compliance with NIS 2 (**NCCS Recital 15**).
- **The Governance Pillar: Proposed Cybersecurity Act 2 (CSA2):** This proposal intends to reform ENISA's mandate and introduce a "Trusted ICT Supply Chain Framework" (**Article 1**) to address ICT supply chain's increasing exposure to risks of a non-technical nature, including risks linked, but not limited, to the jurisdiction to which a supplier of certain components is subject.

4.2 Key Definitions Under the Framework

- **Critical Infrastructure:** An asset that is necessary for the provision of essential services. This is then defined explicitly in each member states implementing legislation.
- **Cybersecurity:** The activities necessary to protect network and information systems, their users, and affected persons (**NIS 2 Article 6(3)**; **CSA2.0 Article 2(1)**).
- **Incident:** An event compromising the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data or services (**NIS 2 Article 6(6)**).
- **High-Impact Entity:** An entity that carries out a process with a high electricity cybersecurity impact (**NCCS Article 3(24)**).
- **Critical-Impact Entity:** An entity carrying out a business process with a critical electricity cybersecurity impact (**NCCS Article 3(7)**).

- **High-Risk Supplier:** An entity an entity established in a third country posing cybersecurity concerns designated in accordance with Article 100, or controlled by such third country, by an entity established in such third country, or by a national of such third country; and an entity designated in accordance with Article 103(7) and entities controlled by that entity (proposed CSA 2.0 Article 2(39)). *This definition is drawn from the European Commission's legislative proposal for the revision of the Cybersecurity Act, which is currently in the ordinary legislative procedure.*¹

4.3 Applicability Matrix

The following matrix summarises how the principal EU cybersecurity frameworks apply to each actor in the BESS value chain. Direct coverage indicates the actor is a named subject of the regulation. Indirect coverage indicates obligations flow via supply chain duties, contractual requirements, or client mandates.

Entity	NIS2	NCCS	CRA	CSA 2.0 proposal	Comment
TSO / DSO	Essential entity under NIS2 (Annex I, electricity). Always in scope.	Always an NCCS entity for cross-border flows.	Only if they market digital products (rare).	Will interact with ENISA for coordinated crisis management (EU-CyCLONE)	Primary addressee of both NIS2 and NCCS.
Recommendation: TSOs and DSOs should cascade cybersecurity requirements to all contracted BESS asset owners and O&M providers via standard supply chain clauses, and should provide clear NCCS impact classification decisions within mandated timelines.					
Aggregator / VPP	Essential entity as electricity aggregator/market participant.	In scope if digital processes are classified high/critical impact.	Only if selling products with digital elements.	Can demonstrate compliance via "Cyber Posture" certification to ease audits	Usually NIS2-covered; NCCS depends on cross-border role.
Recommendation: VPP operators aggregating residential BESS fleets above a defined aggregate capacity threshold should be explicitly classified under NCCS regardless of individual unit size. ACER should issue guidance on the applicable threshold.					
Plant Operator	In scope only if it is the legal producer; otherwise via NIS2 supply-chain duties.	In scope only if designated NCCS entity; normally obligations flow via producer/TSO/DSO.	CRA only if it develops or markets products.	Legally barred from using "key assets" from High-Risk Suppliers	Treat as service provider implementing others obligations for utility-scale plants.
Recommendation: Where plant operators are not the legal producer, NIS2 supply-chain clauses must explicitly name the plant operator and define their obligations. Additionally, where they exercise direct operational control over BESS assets, they should be recognised as accountable entities under NIS2 Directive. Industry should develop standard contract templates for this handover.					

¹ This definition is drawn from the European Commission's legislative proposal for the revision of the Cybersecurity Act, which is currently in the ordinary legislative procedure.

Asset Owner	Essential entity as electricity producer, if size thresholds met including aggregated controllers (SCADA, DERMS).	NCCS entity where plants/IT are tagged high/critical impact, including aggregated controllers.	Not CRA operator unless selling own digital products.	Must account for equipment replacement costs if using components from designated High-Risk Suppliers.	Main responsibility holder for plant cybersecurity. For SPVs, the entity has no employees and is reliant on the parent investor.
Recommendation: Asset owners must maintain a named cybersecurity accountable person even where operations are fully outsourced. SPV structures should explicitly document their NIS2 compliance posture, including whether the paragraph 16 independence argument applies.					
Financial Investor / SPV	Exemption possible if SPV is independent (NIS2 paragraph 16). In scope when IT/OT systems are centralised across multiple SPVs, treated as linked enterprises.	No direct NCCS role; influence via governance of in-scope entities.	No CRA duties in pure investor role.	Must evaluate the jurisdictional and ownership profile of OEM suppliers as part of investment due diligence.	Centralised systems pose the greatest threat to grid stability but also bring SPVs into scope. True operational independence is required for exemption.
Recommendation: The European Commission should publish guidance on how NIS2 applies to SPV portfolio structures. Investors centralising IT/OT across multiple SPVs should be recognised as de facto system operators and brought into the scope of NIS2 Directive					
OEM / Manufacturer	Covered as important entity as manufacturer of electrical equipment. This is inadequate for inverter manufacturers and excludes companies with no EU legal entity.	Can be designated critical ICT provider for cross-border systems; otherwise affected via NCCS supply-chain rules.	Core CRA economic operator, but only in Default category. Must be reclassified as Critical to be adequate for grid-relevant components. Risk classification should prioritise verifiable ownership, control, or governance ties to jurisdictions of concern.	Subject to potential High-Risk Supplier designation under Article 100. Criteria for designation remain subject to the legislative process.	CRA is primary regime. NCCS may apply as critical ICT supplier or managed service provider depending on infrastructure classification.
Recommendation: The Commission shall use CRA delegated acts to reclassify grid- and system-critical components such as BMS, EMS, and PCS as Critical (Class I or II) products. Cybersecurity validation under the CRA should move from self-attestation to third party validation. ENISA should publish sector-specific security requirements. Additionally, OEMs providing BESS components with remote access capabilities or embedded control functions should be subject to enhanced operational accountability, beyond product compliance under the CRA. IEC 62443 should be used as a practical technical reference framework, in particular, IEC 62443-4-1 is relevant to secure product development lifecycle requirements, while IEC 62443-4-2 is relevant to technical security requirements for components such as BMS, EMS, PCS, SCADA, gateways. Supply Chain requirements under proposed CSA 2.0 need to provide clear guidance on applicability.					
Developer / EPC	Not a listed NIS2 entity; possibly covered indirectly via client's supply-chain obligations.	Not normally designated; possible NCCS duties passed down contractually.	CRA operator only if it sells its own digital products.	High-assurance evaluations must remain within the EEA to protect intellectual property under proposed provisions.	Focus on secure-by-design integration demanded by NIS2/NCCS clients.

Recommendation: Standard secure-by-design integration checklists and commissioning protocols shall be designed so that EPCs can adopt as contractual deliverables, reducing dependency on client-by-client specification.					
Installer / Contractor	Out of NIS2 scope as an entity type; obligations flow via NIS2-regulated customers technical specs.	Not an NCCS entity; must follow NCCS-driven installation and configuration requirements from clients.	CRA only if re-branding or substantially modifying products.	Staff may obtain certified Union-wide cybersecurity skills attestations under proposed provisions.	Classic supply-chain actor; compliance largely enforced via contracts.
Recommendation: Standard installation security specifications covering secure configuration baselines, credential management, and commissioning verification should be developed as industry guidance and included in all EPC and owner procurement contracts.					
O&M Provider (3rd party)	Directly in scope only if acting as managed ICT/OT service provider at NIS2 scale; otherwise via contracts.	Not usually designated; NCCS measures flow down from TSO/DSO/producer.	CRA duties only if it develops or markets digital products.	MSPs themselves cannot be controlled by a designated third country under proposed provisions.	Will only be directly covered if inverters and other relevant platforms are classified as critical ICT.
Recommendation: O&M contracts must explicitly assign patch application responsibility, define patch timelines, require MFA and session logging for all remote access, and specify liability for incidents occurring during O&M-managed sessions. Standard O&M cybersecurity annexes should be developed at industry level. Additionally, and as a general principle, O&M providers performing critical operational functions should be subject to minimum cybersecurity obligations aligned with managed service providers, even where not directly classified under NIS2.					
Fleet Monitoring / SCADA	In scope as cloud/data-centre/managed-service provider where medium or larger in size.	Typically designated critical ICT provider when supporting cross-border-relevant operations.	CRA applies to any SCADA/gateway software or hardware put on the market; not to pure SaaS backends.	Likely designated as a key asset, additional requirements for High-Risk Suppliers.	Will be considered a critical ICT provider under the NCCS.
Recommendation: Fleet monitoring providers should proactively seek NCCS critical ICT designation clarity from national authorities. SCADA software placed on the EU market must be CRA-compliant by December 2027; conformity assessment planning should begin now.					
Cloud Provider	Essential entity: cloud computing/data-centre service provider (Annex I).	Designated critical ICT provider where hosting NCCS entities critical systems.	CRA only if also selling software or devices as products; pure cloud is outside CRA.	Encouraged to adopt Union-based sovereign cloud offerings to reduce critical dependencies; subject to supply chain vetting obligations.	Will be considered a critical ICT provider under the NCCS.
Recommendation: Cloud providers hosting BESS EMS or fleet management platforms should be recognised as integral components of the control chain, not only infrastructure providers, and confirm critical ICT designation status with relevant NCCS authorities and ensure contractual cybersecurity obligations, including incident notification timelines, flow down to BESS asset owner clients.					

Directly covered

Indirectly covered

Action needed

Not applicable

Table 2: How NIS 2, NCCS, the CRA and the proposed CSA 2.0 apply to each value-chain actor: direct, indirect or no coverage, and where action is needed.

Note on regulatory implementation:

The European Commission proposed Cybersecurity Act 2.0 and its newly introduced chapter on Security of ICT Supply Chains has been mentioned in this paper, and as the proposal is currently in the legislative process, the above table may be subject to change.

The following timeline summarises the key milestones for BESS operators, OEMs, and policymakers in the current regulatory cycle:

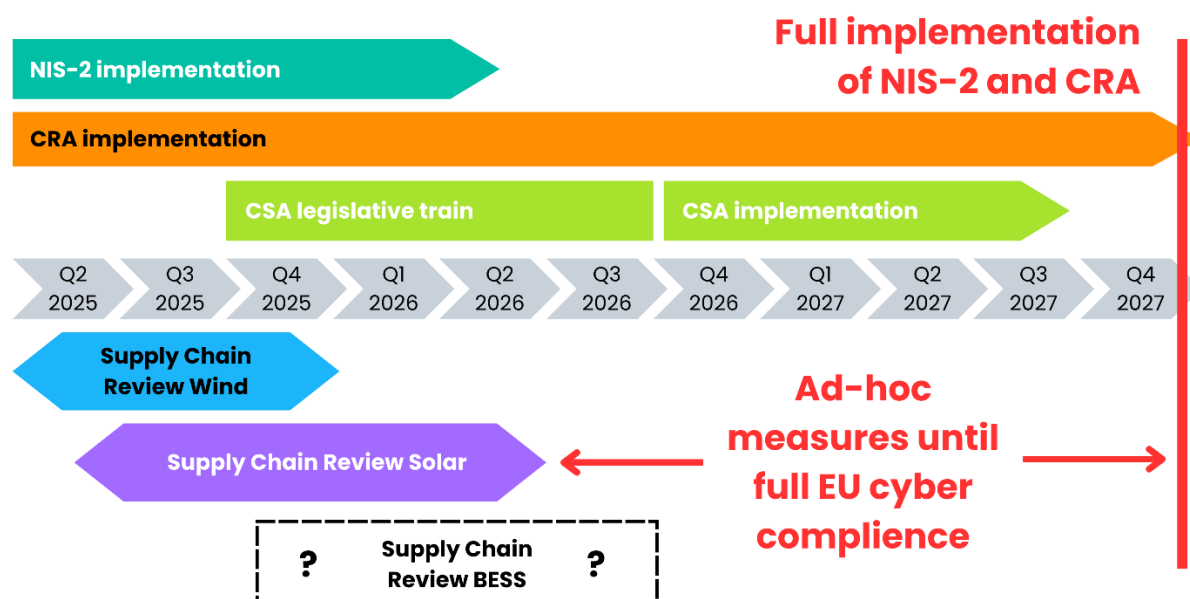


Figure 11: Key EU regulatory milestones for BESS, Q2 2025 to Q4 2027 (status September 2026). No BESS-specific supply chain review has been scheduled yet.

5. Challenges & Gaps

This chapter identifies where the existing EU cybersecurity framework, while broadly sound in design, creates practical gaps for battery storage. It focuses on four areas: underused coordination mechanisms; inconsistent implementation across Member States; unresolved accountability gaps; and emerging ICT supply chain risks, including limited transparency. Chapter 6 sets out recommendations to address these gaps.

5.1 Coordination Opportunities Within the Existing Framework

Two existing mechanisms are not yet fully exploited:

- Under Recital 15 of the Network Code on Cybersecurity, compliance with sector-specific electricity obligations may serve as evidence for Network and Information Security Directive compliance, reducing duplicative audits. This shall be formally operationalised through joint guidance from the EU Agency for Cybersecurity and the Agency for the Cooperation of Energy Regulators (ACER).
- Similarly, for battery storage components sold by manufacturers to regulated operators, the Cyber Resilience Act and the Network and Information Security Directive create complementary rather than conflicting obligations.

5.2 Harmonisation Failures and Their Consequences

The most acute harmonisation failure for battery storage is at NIS 2 implementation level. **NIS 2 obligations are not harmonised across the EU:** varied national transpositions create compliance complexity for pan-European operators and, in practice, create *de facto* exemptions for non-EU manufacturers with no EU legal entity. Member States also differ in their approaches to non-European technology providers, with some imposing additional technical requirements around data storage, data access, and data transfer. These **divergent approaches create a systemic mismatch in a grid that is deeply interdependent.**

At the **Network Code on Cybersecurity level, Distribution System Operators in different Member States impose varying technical requirements on battery storage systems connecting to their networks.** For utility-scale installations, this is manageable. For residential and commercial battery storage, it is not: manufacturers serving multiple national markets must engineer and certify market-specific system configurations, adding significant cost and delaying deployment across the Single Market.

This fragmentation is particularly acute for battery storage as BESS – like electric vehicles – are mass-produced to bring costs down and enable adoption. Software-based cybersecurity requirements have direct hardware implications, as they are embedded in firmware and power circuit boards manufactured on standardised lines. **Unharmonised requirements force costly modifications to the manufacturing process, leading to either market retraction, price increases, or cost-cutting (including on cybersecurity itself),** all of which are detrimental to European consumers.

5.3 Specific Gaps Requiring Urgent Resolution

Four accountability gaps in the current framework require immediate attention.

1. **Legacy assets:** Battery storage units placed on the market before the Cyber Resilience Act's December 2027 implementation date fall outside its product compliance requirements, but mandatory vulnerability reporting obligations begin in September 2026. Manufacturers of pre-regulation legacy assets have no clear obligation to report vulnerabilities in products already deployed. National authorities should urgently issue guidance on how vulnerability management obligations apply to the existing installed

base, and industry should proactively adopt voluntary disclosure practices in advance of mandatory requirements.

2. **Cyber risk management handover in outsourced operations:** The Network and Information Security Directive requires asset owners to vet their supply chain and implement the appropriate security controls. But in many battery storage projects, the security architecture design and practical implementation of security controls such as patches falls to a subcontractor operating under a separate contract. Subcontractors often do not have authority to direct or influence the design of other vendors sub systems or influence responsibilities of the asset owner such as: Business Continuity Management; incident response or reporting requirements. The asset owner is legally accountable, but the party responsible for managing security day to day may not be directly supervised by the owner. Standard contractual provisions, such as defined patch timelines, mandatory approval workflows, and incident liability clauses for contractor-managed remote access, should be developed as industry guidance and adopted as a baseline in all operations and maintenance contracts
3. **Treatment of special purpose vehicle ownership structures:** Where a battery storage asset is held by a legally independent special purpose vehicle with no employees, obligations under the Network and Information Security Directive may fall to the parent investor entity, which may lack operational control over the asset. Where information technology and operational technology systems are centralised across multiple such vehicles and the linked enterprise threshold is met, this brings the portfolio into scope. Guidance is needed from the European Commission on how these structures should be treated, and investors who centralise systems across multiple vehicles should proactively assess their exposure.
4. **Manufacturers with no European legal entity:** The Cyber Resilience Act applies to products placed on the European market regardless of where the manufacturer is incorporated, but enforcement against non-European manufacturers without an EU presence remains challenging. There is also a possible route under NIS 2 to classify certain non-EU OEMs directly as essential entities in their capacity as providers of digital services in the EU market - an interpretation that has not yet been formally tested but that deserves attention from the European Commission and the NIS Cooperation Group. In the meantime, the authorised representative mechanism established by the Cyber Resilience Act must be actively enforced rather than treated as a formality. Additionally, treatment of inverter and battery manufacturers, who maintain access of installed facilities through cloud infrastructure, as providers of cloud services or digital service providers would provide a legal mechanism to include vendors as essential entities and allow the appropriate national competent authority the right to audit vendors under standard NIS 2 audit schemes. This applies as well to EU legal entities of non-EU manufactures.

5.4 Transparency Around Emerging ITC Supply Chain Risk Management

In the draft CSA of the Commission, measures and processes around cyber security risks of non-technical nature are proposed. These are linked to the jurisdiction to which a supplier of (still to be defined) key ICT components are subject to and the supplier's proprietary control structure. For financial institutions channelling EU Commission funding, inverters used in solar PV, BESS and wind projects were identified as a key ICT component, for which a funding ban exists now. Within the scope of the draft CSA 2.0, the assessment of key ICT components is still ongoing as well as the scope of measures applicable.

While the CSA under discussion and its adoption only expected by 2027 the earliest, it is vital to provide the industry at the earliest possible time with transparency, details and clarification on process and timelines of bans of components from high-risk countries, to allow the storage industry to realign and restructure its supply chain strategies in line with the applicable legislation. Industry requires not only early disclosure of the direction of supply chain measures, but also a clear, component-based risk assessment that distinguishes between systems whose failure would cause immediate, system-wide disruption to critical infrastructure and components that present lower operational risk. Proportionate timelines, including a minimum response period for suppliers requested to provide information, are essential to ensure due process.

6. Recommendations

This chapter sets out the actions that follow from the mapping in Chapter 4 and the gaps identified in Chapter 5, organised by addressee so that each actor in the value chain can see what is being asked of it. Section 6.1 covers industry actors; and Section 6.2 covers EU institutions.

6.1 Recommendations for the Industry

6.1.1 Asset Owners and Operators

- Require verified HBOMs and SBOMs from all OEMs and system integrators as a standard procurement condition. Use SBOMs to run automated CVE scans before commissioning and at regular intervals during operation.
- Implement a defensible architecture from day one: ensure proper network segmentation between critical applications, balance-of-plant systems, and external systems; deploy monitored firewalls; and define a safe-state configuration that the system defaults to if communications are disrupted.
- Ensure continuous monitoring capabilities, including centralised logging, anomaly detection, and integration with SOC/SIEM platforms, to enable early detection of anomalous behaviour across both IT and OT environments.
- Establish secure remote access with role-based permissions, MFA, session logging, and dedicated engineering workstations. Prohibit shared accounts, require access reviews at least quarterly, and ensure no standing privileged vendor access. All OEM and third-party remote sessions should operate within owner-approved, time-limited windows, with full audit logging and owner-retained revocation rights at all times.
- Perform cyber risk assessments and develop cyber architecture early, then incorporate explicit cyber requirements into procurement contracts (going beyond "the plant shall be NIS 2 compliant").
- In all O&M contracts, define patch application responsibility and timelines, require MFA and session logging for remote access, and specify liability for incidents occurring during O&M-managed sessions. Where the O&M provider is not the legal producer or plant operator, name it explicitly in the contract's NIS 2 supply-chain clauses.
- Maintain a documented incident response plan that includes coordination with the TSO/DSO and meets NIS 2 reporting timelines (initial notification within 24 hours, detailed report within 72 hours).
- Maintain a comprehensive and continuously updated asset inventory covering all hardware, software, and communication interfaces across the BESS architecture.
- Maintain a named cybersecurity accountable person even where operations are fully outsourced. Where the asset is held through an SPV, document the entity's NIS 2 compliance posture, including whether the independence exemption under paragraph 16 applies; investors centralising IT/OT systems across multiple SPVs should proactively assess their exposure under the linked enterprise threshold.

6.1.2 OEMs and System Integrators

- Ensure that cyber responsibility and interfaces during system design and construction are clearly defined in contracts.
- Treat SBOM and HBOM production as a design-phase activity, not a post-deployment exercise. Retrospective SBOM generation costs between €1,000 and €20,000 per asset and frequently requires reverse engineering of third-party intellectual property.
- Implement security-by-design principles, including secure boot, signed firmware, hardened configurations, and removal of default credentials, so that core components are resilient from the outset.

- Establish and publish a coordinated vulnerability disclosure policy before the September 2026 CRA mandatory reporting deadline, including for products placed on the market before the CRA's December 2027 application date, and demonstrate active engagement with ethical disclosure processes ahead of that deadline.
- Design BESS systems so that loss of remote monitoring or communications does not affect safe operation; the system should default to a safe state, not an operationally dependent one.
- Commit to software support contracts that match the expected asset lifespan (15 to 20 years), and address obsolescence explicitly, including end-of-life plans for embedded operating systems and communication stacks that will lose vendor support mid-asset-life.
- Ensure interoperability and security testing across multi-vendor environments, validating that interactions between BMS, EMS, PCS, and external systems do not introduce systemic vulnerabilities.
- Where remote access or embedded control functions are provided, accept enhanced operational accountability beyond product compliance under the CRA.

6.1.3 EPCs and Installers

- Develop standard secure-by-design integration checklists and commissioning protocols that EPCs can adopt as contractual deliverables, reducing dependency on client-by-client specification.
- Develop standard installation security specifications, covering secure configuration baselines, credential management, and commissioning verification, as industry guidance for inclusion in all EPC and owner procurement contracts.

6.1.4 System Operators, Aggregators, and Service Providers

- TSOs and DSOs should cascade cybersecurity requirements to all contracted BESS asset owners and O&M providers via standard supply chain clauses, and should provide NCCS impact classification decisions within mandated timelines.
- VPP operators aggregating residential BESS fleets above a defined aggregate capacity threshold should treat themselves as in scope of NCCS ahead of formal guidance on that threshold (see 6.2.1).
- Fleet monitoring and SCADA providers should proactively seek NCCS critical ICT designation clarity from national authorities, and begin conformity assessment planning now for CRA compliance by December 2027.
- Cloud providers hosting BESS EMS or fleet management platforms should recognise themselves as integral components of the control chain, not only infrastructure providers, confirm their critical ICT designation status with the relevant NCCS authorities, and ensure contractual cybersecurity obligations, including incident notification timelines, flow down to BESS asset owner clients.

6.2 Policy Recommendations for the EU

- Harmonise NIS2 technical requirements at EU level through the CSA 2.0 process, keeping them risk-based and avoiding overly prescriptive technical requirements that could limit operational flexibility across diverse assets. Direct ENISA to publish minimum harmonised technical requirements for BESS DSO connectivity, eliminating market-specific engineering requirements for residential and C&I systems.
- Escalate CRA classification of grid-critical BESS components (PCS, EMS, BMS) from Default to Critical (Class I or II) through the delegated acts process. Self-assessment is not adequate for components that can directly affect grid frequency and voltage; require third-party verification. Direct ENISA to publish sector-specific security requirements for these components.
- Publish joint NIS 2 / NCCS implementation guidance clarifying where NCCS compliance satisfies NIS 2 supply chain vetting obligations, reducing audit duplication for asset owners.
- Reference industry cybersecurity standards such as ISO 27001 and IEC 62443 in EU-level BESS guidance as the preferred technical baseline for industrial control cybersecurity, particularly for secure development lifecycle, component security capabilities, network segmentation, access control, patch

management, and vulnerability handling. This would avoid duplicative national frameworks and support efficient conformity assessment, reduced compliance costs, and enhanced resilience across the Union.

- Issue urgent guidance on how vulnerability management obligations apply to the existing installed base of legacy assets placed on the market before the CRA's December 2027 implementation date, given that mandatory vulnerability reporting begins in September 2026; industry should adopt voluntary disclosure practices in the interim.
- Issue guidance on how NIS 2 applies to SPV portfolio structures, including the treatment of centralised IT/OT systems across multiple SPVs under the linked enterprise threshold.
- Issue guidance on the aggregate capacity threshold above which VPP operators aggregating residential BESS fleets should be classified under NCCS regardless of individual unit size.
- Actively enforce the CRA's authorised representative mechanism for manufacturers with no EU legal entity, rather than treating it as a formality, and examine the NIS 2 and cloud/digital service provider classification routes for non-EU OEMs described in Chapter 5.
- Recognise O&M providers performing critical operational functions as subject to minimum cybersecurity obligations aligned with managed service providers, even where not directly classified under NIS 2.
- Include CRA compliance and vulnerability disclosure commitments as conditions for public market and public procurement participation.

7. References and Sources

EU Legislative and Regulatory Instruments

- Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)
- Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). Available at: <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>
- Commission Delegated Regulation (EU) 2024/1366 establishing a network code on cybersecurity in the electricity sector (Network Code on Cybersecurity)
- Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act)
- European Commission, consultation on revising the EU Cybersecurity Act, April 2025. Available at: <https://digital-strategy.ec.europa.eu/en>
- European Commission proposal for a Regulation amending Regulation (EU) 2019/881 as regards managed security services (proposed Cybersecurity Act revision / CSA 2.0)
- Regulation (EU) 2024/1735 on establishing a framework of measures for strengthening Europe's net-zero technology manufacturing ecosystem (Net Zero Industry Act)
- European Commission proposal for a Regulation establishing a framework for the competitiveness of the European net-zero technology industry (proposed Industrial Accelerator Act)
- Delegated Regulation (EU) 2025/1463 specifying main specific components of net-zero technology final products under the NZIA
- Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive)
- Regulation (EU) 2023/1542 concerning batteries and waste batteries (Battery Regulation), including Digital Battery Passport provisions
- European Commission, "A Competitiveness Compass for the EU," COM(2025) 30 final, January 2025. Available at: https://commission.europa.eu/document/download/10017eb1-4722-4333-add2-e0ed18105a34_en

EU Institutional Documents and Communications

- European Commission and High Representative, Joint Communication on Strengthening EU Economic Security (2024)
- European Commission, "Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures," 2020. Available at: <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>
- ENISA, Threat Landscape 2025
- ENISA, Cyber Europe: Testing EU Cyber Preparedness in the Energy Sector
- ENISA, Guidelines on Supply Chain Cybersecurity
- NIS Cooperation Group, cybersecurity supply chain review for the solar sector (ongoing; interim findings referenced in Commission financing decisions, April 2026)

Technical Standards

- IEC 62443-4-1: Security for industrial automation and control systems, Secure product development lifecycle requirements
- IEC 62443-4-2: Security for industrial automation and control systems, technical security requirements for components
- IEC 62443-3-3: Security for industrial automation and control systems, System security requirements and security levels
- IEC 61850: Communication networks and systems for power utility automation
- ISO/IEC 27001: Information security management systems

Industry and Research Sources

- Idaho National Laboratory, "BESSIE: Battery and Energy Storage Supply Chain Analysis, Mitigation Deployment, and Tools," March 2024. Available at: https://inl.gov/content/uploads/2024/03/BESSIE_supply-chain-battery-report.pdf
- The Brattle Group and Dragos, "Cybersecurity and Battery Energy Storage Systems," 2025
- S&P Global Energy, "EU cuts funding to projects with Chinese power conversion systems," May 2026
- NERC, "IBR Controls Oscillation Events," September 2025. Available at: https://www.nerc.com/globalassets/programs/event-analysis/ll20250901_ibr_controls_oscillation_events.pdf
- European Commission trade data: in 2023, components from China accounted for approximately one third of EU imports of low-voltage boards and panels, including programmable logic controllers
- Australian Energy Market Operator (AEMO), "AESCSF Framework and Resources," 2025. Available at: <https://aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources>

Member State Regulatory References

- Germany: KRITIS-Dachgesetz and BSI Act implementing the CER Directive and NIS 2 Directive; applicable BESS thresholds under KRITIS (104 MW general; 36 MW for FCR-prequalified assets; 1 MW for black-start providers)
- Lithuania: national measures restricting Chinese remote access to energy storage, solar, and wind devices (2024)

This image shows a full page of white paper with horizontal blue or grey ruling lines. The lines are evenly spaced and run across the width of the page, providing a template for handwriting practice. There are no margins, text, or other markings on the page.

About the Energy Storage Europe:

Energy Storage Europe is the leading member-supported association representing organisations active across the entire energy storage value chain. The Association supports the deployment of energy storage to further the cost-effective transition to a resilient, carbon-neutral, and secure energy system. Together, Energy Storage Europe members have significant expertise across all major storage technologies and applications. This allows us to generate new ideas and policy recommendations that are essential to build a regulatory framework that is supportive of storage.

For more information, please visit www.energystorageeurope.eu

Disclaimer:

This content was elaborated by the Energy Storage Europe and reflects a consolidated view of its members from an energy storage point of view. Individual Energy Storage Europe members may adopt different positions on certain topics from their corporate standpoint.

Contact: Secretariat | info@energystorageeurope.eu



Avenue Adolphe Lacomblé 59/8
1030 Brussels | Belgium
www.energystorageeurope.eu



The Unified Voice
of Energy Storage